AXOS R21.x Turn-Up and Transport Guide

August 2021

#220-01193, Rev 13

Contents

.

About This Guide

This guide describes how to initially turn up, manage access, and configure network transport for Calix AXOS systems.

Intended audience

This document is intended for personnel responsible for turning up and managing carrier network systems and services. This document assumes that the user is familiar with using a command-line interface (CLI) over a standard telnet or console connection. Familiarity with datacom, telecom, and standards-based Ethernet technologies and conventions is recommended.

Document scope

Please note the following details regarding the scope of this document:

- This document provides configuration instructions via the command line interface (CLI). For configuration support via other interfaces, please see the related documentation or your Calix representative.
- This document assumes that the most recent software release has been installed. For the supported features for a given AXOS system and release, see the corresponding release notes or product planning guide.

Note: CLI commands may be visible in AXOS that are not necessarily applicable to every AXOS system or release version. To avoid unexpected results or error messages, do not execute inapplicable commands. For the supported features for a given AXOS system and release, see the corresponding product planning guide.

Related documentation

You can access Calix product documentation by logging into My Calix (*www.calix.com/my-calix* (*https://www.calix.com/mycalix*)) and browsing the My Calix Documentation Library.

.

Chapter 1

Getting Started with AXOS Systems

This chapter provides an overview of the Calix AXOS E-Series systems and Command-Line Interface (CLI), the turn-up process, and how to establish an initial connection to the system.

Note: For instructions on how to install the AXOS system hardware and connect physical network interfaces, see the appropriate Calix Installation Guide.

Topics covered

This chapter covers the following topics:

- Calix AXOS systems overviews
- Turn-up process
- Establishing an initial connection to the system
- CLI overview

Systems Overview

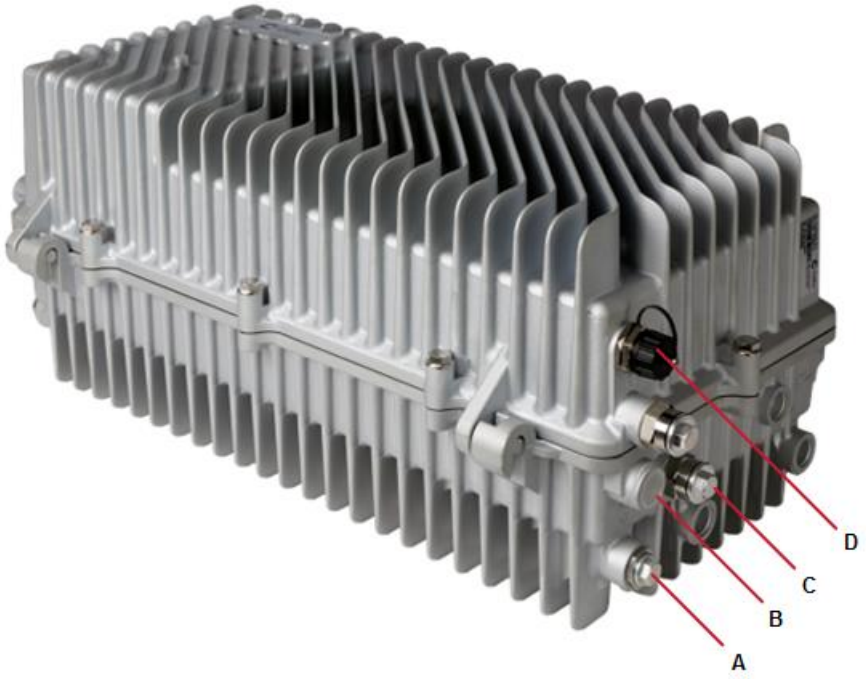
This section provides descriptions of the Calix AXOS systems. The systems share common operating software and some features, but differ in physical form factor, installation and powering options.

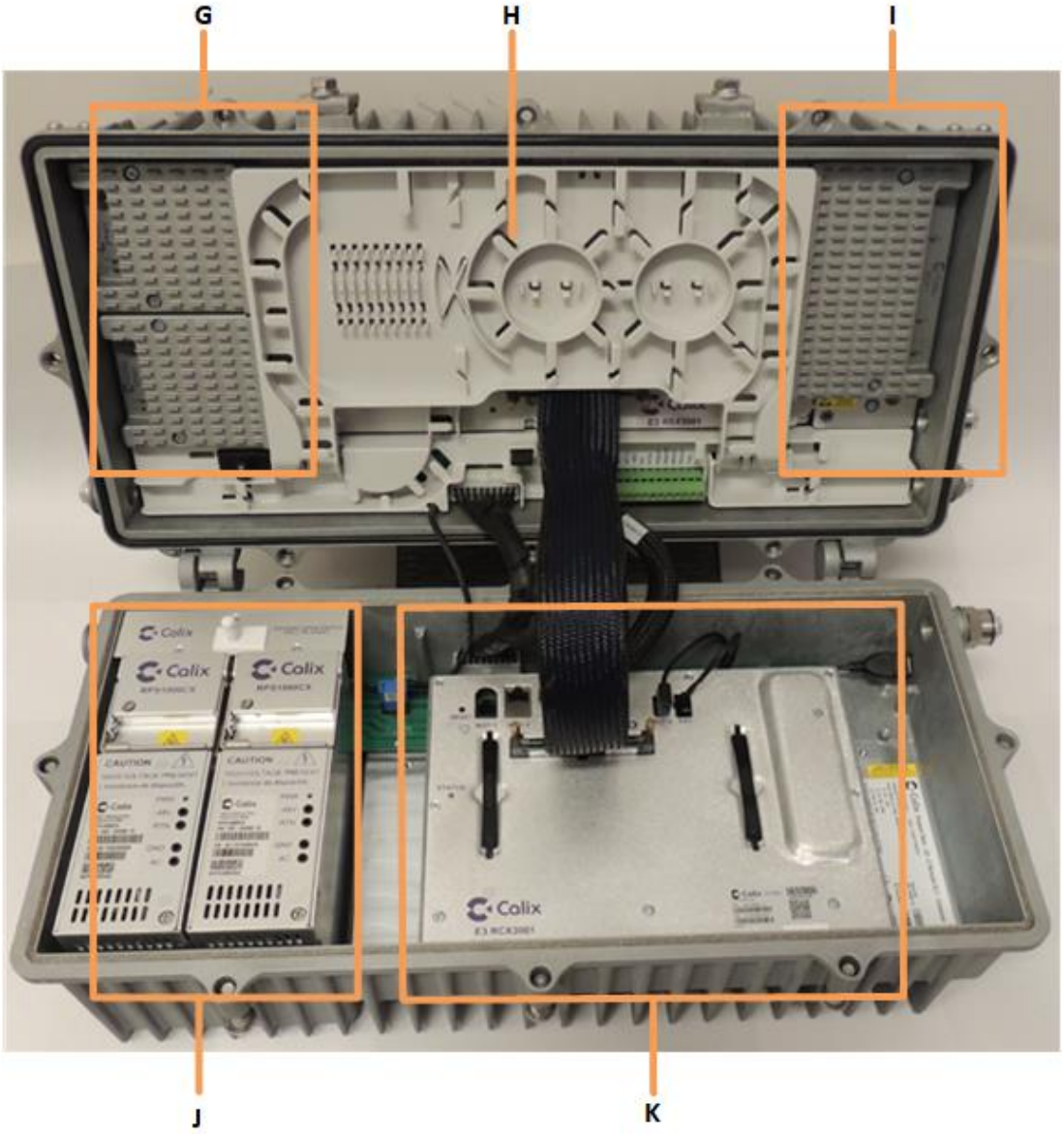
Note: For instructions on how to install the AXOS system hardware and connect physical network interfaces, refer to the appropriate installation guide.

E3-2 System Description

The Calix E3-2 is an environmentally-hardened, remote OLT that is designed for OSP installations (strand, pole, and pedestal), accepts power from a variety of sources, utilizes the AXOS architecture to support Layer 2 and 3 services, and supports multiple PON technologies. In addition, the modular design of the E3-2 allows for quick and reliable hardware configurations, upgrades, and repairs.

For additional product details, see the *Calix E3-2 Intelligent PON Node Product Datasheet*, available from the My Calix Documentation Library.





Dimensions

- Width: 22 inches
- Depth: 11.5 inches
- Height: 9.65 inches

External features

A	Coax power port (right side)
B	Fiber port (right side)
C	AC/DC/alarm wiring port
D	UBS port (capped)
E	Coax power port (left side) - not shown
F	Fiber port (left side) - not shown

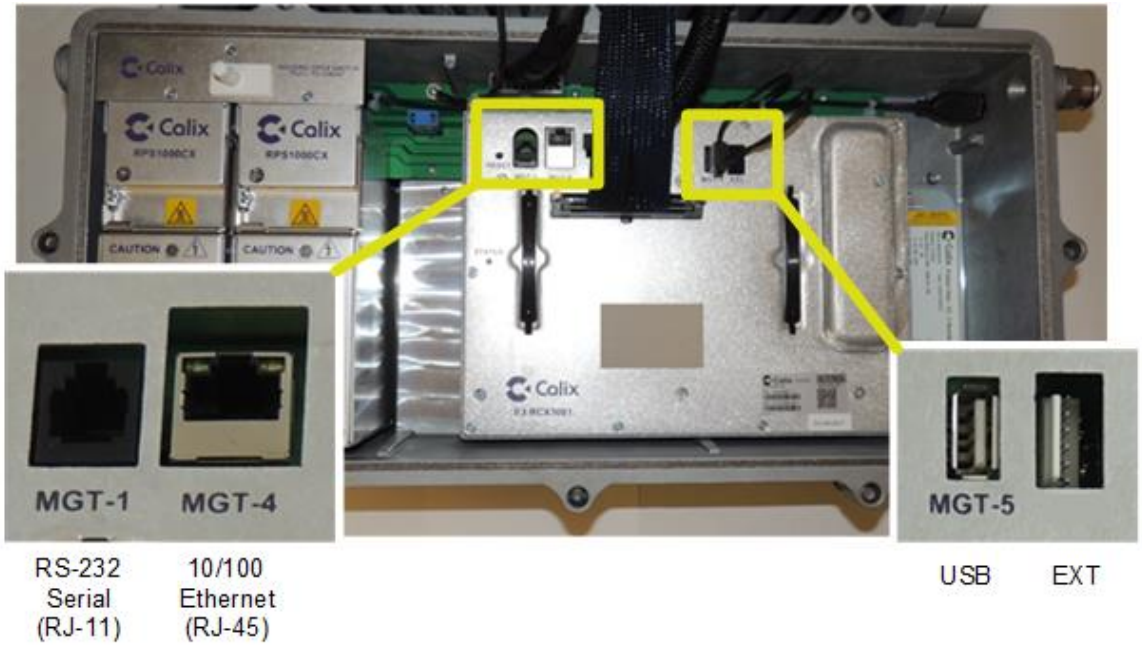
Internal features

G	PON modules with PON ports
H	Switch module (under fiber tray)
I	WAN module with 10GE WAN ports
J	Power supply modules, if required
K	Control module with craft ports, if applicable
	Upper half: Coax surge suppressor, coax power shunt Lower half: Lid switch (not shown), PROM card (blue) with system ID; Interconnection cables

Management ports

Applicable E3-2 control modules provide the following management ports:

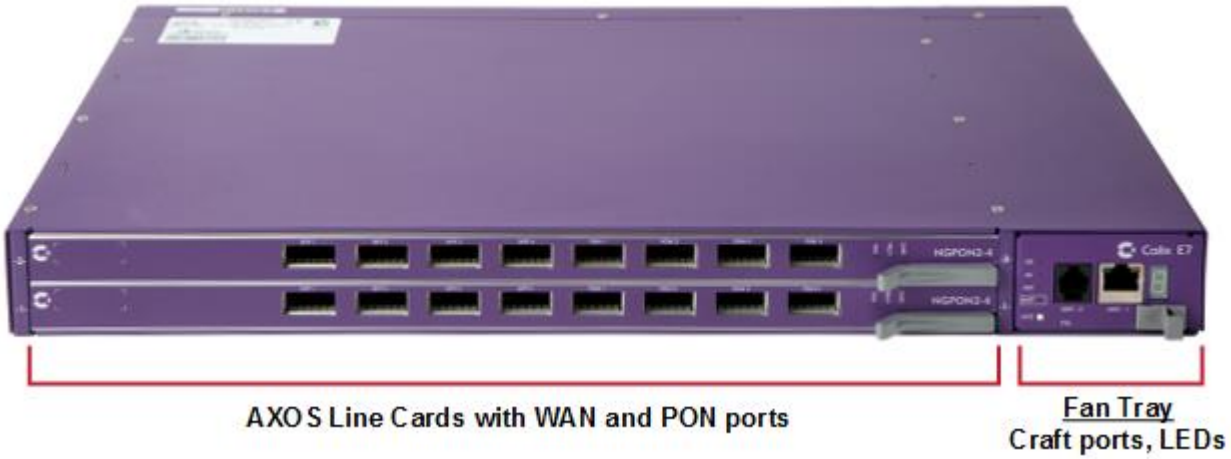
- MGT-1 (internal) RS-232 serial port for console connections to the CLI (RJ-11 connector, 115200 baud rate)
- MGT-4 (internal) Internal: Out-of-band 10/100 Ethernet management port (RJ-45 connector).
- MGT-5 (internal/external): USB management port, with connector cable to the external USB port.



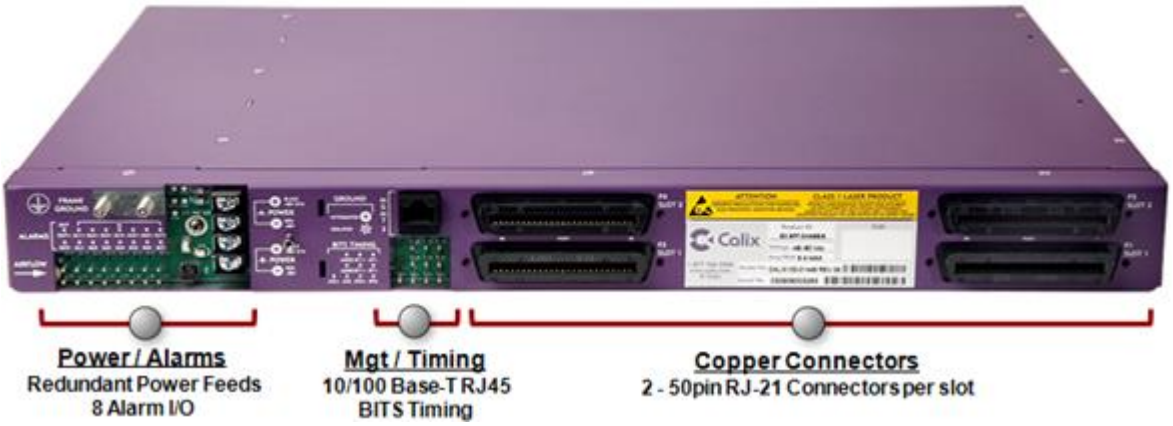
E7-2 System Description

The Calix AXOS E7-2 Intelligent Modular System is the industry's benchmark for a modular, small form factor, environmentally hardened access solution for service providers.

An E7-2 AXOS system consists of an E7-2 chassis with only AXOS line cards installed.



Front View of E7-2 Chassis with Two Line Cards



Rear View with Power, Alarm, Management, Timing and RF-21 Copper Connectors

E7-2 AXOS line cards

For information about the latest, supported E7-2 AXOS line cards, see the following resources:

Topic	Resources
Card descriptions	See the latest Calix E7-2 AXOS Product Planning Guide.
Deployment considerations	See the latest Calix E7-2 AXOS Product Planning Guide.
Hardware installation	See the E7-2 Installation Guide
Removal and replacement	**Software steps:** Prior to removal, save your configuration to an external server. After replacement, restore your configuration. For more details, see *Managing AXOS Configuration Files* (on page 345). **Physical removal and replacement steps:** See the E7-2 Installation Guide

Fan tray assembly

The FTA design includes four individual variable speed fans that maintain system cooling even with one fan failure. Airflow is from right to left (toward the line cards).

Calix E7-2 Fan Tray Assembly Front Panel

Each FTA is hot-swappable and can be quickly replaced by unlocking the sliding latch, removing the failed unit and sliding in the new FTA. Each FTA includes a field replaceable fan filter that slides in from the top of the FTA once it is removed from the E7-2 shelf.

Note: When the E7-2 is operated in a remote terminal that includes integrated cabinet filters, the FTA fan filter should be removed from the FTA to increase airflow within the E7-2.

System status indicators

The E7-2 system includes multiple visual status indicators located on the front of the E7-2 FTA. The FTA status indicators will remain dark until at least one card is inserted in the E7-2 shelf.

- Critical (CR) Alarm – RED LED indicates a critical alarm is present in the system
- Major (MJ) Alarm – RED LED indicates a major alarm is present in the system
- Minor (MN) Alarm – AMBER LED indicates a minor alarm is present in the system
- System Controller (MGT) – GREEN LED indicates E7-2 shelf has an active shelf controller
- 7-segment LCD display – not used in R1.0

An Alarm Cut-Off (ACO) button is also integrated on the front on the FTA.

System management ports

The E7-2 has the following ports available for device management:

- **MGT-1** located on the FTA front panel for local craft access to management user interfaces. The connector is 10/100 Base-T Ethernet (RJ-45).
- **MGT-2** can be configured within any VLAN on any E7-2 Ethernet port interface for an in-band management interface.
- **MGT-3** located on the E7-2 rear panel for permanently connecting to the network back office management systems. The connector is 10/100 Base-T Ethernet (RJ-45).
- **MGT-4** located on the FTA front panel for local craft management. RS-232 serial port for console connections to the CLI only. (RJ-11 connector, 115200 baud rate.)

Power inputs: The E7-2 is equipped with dual power inputs to support redundant –48VDC power feeds (A and B), switching between them when one source fails.

Alarm inputs and outputs: The E7-2 supports eight external alarm input/output (I/O) positions via wire-wrap pins located on the E7-2 rear panel. The eight external alarm positions include seven inputs and one output position.

BITS Timing: The E7-2 can be synchronized to a local traceable clock using the Building Integrated Timing Supply (BITS) composite clock timing wire-wrap pins located on the back of the E7-2 shelf. Up to 10 shelves may be connected serially. The BITS interface is designed to support both DS1 and E1 inputs. See T1/E1 PWE3 Service.

Operational LEDs: The E7-2 is equipped with the following LED operational indicators:

- **Line card LEDs** - Located at each card slot on the front panel to indicate when at least one port is active (green) and when a card is in standby (orange).
- **Port status LEDs** - Each GPON Optical Interface Module (OIM), GE-SFP, 10GE-XFP module sockets have a combined link status/activity LED below the socket.
  - Green LED (Ethernet ports) is solid green when a link is established and blinks at a variable speed to indicate traffic load.
  - Green LED (GPON ports) blinks steadily when the first ONT is ranging on a GPON port and remains lit when at least one ONT is in service.
  - Red LED indicates a module is inserted into a socket which is directed to the backplane (only x2 or x4).
- **Alarm LEDs** - Located on the fan module front panel; indicate critical, major, and minor alarms.

E7-2 dual line card operation

The E7-2 line cards are designed to operate at full port count and capability when deployed in a single-card system, and also operate as a protected pair when deployed in a dual-card system.

Line cards and system controller status

In dual-line card systems, one card is designated as the system controller which manages alarms, configuration, and performance monitoring. A "*" is shown next to the card label in the web interface and in the CLI show card command results. The other card is in a standby status.

E9-2 System Description

Calix provides two types of E9-2 Intelligent Edge systems:

- E9-2 ASM3001 systems
- E9-2 CLX3001 systems

Calix E9-2 ASM3001 systems

For access aggregation and edge routing applications, each E9-2 shelf is equipped with one or two Aggregation Service Manager (ASM3001) cards and operates as a standalone system.

Calix E9-2 CLX3001 systems

For L3/L2 FTTx access applications, a collection of E9-2 shelves comprises an OLT system, where one shelf is equipped with one or more control and aggregation (CLX3001) cards, and the remaining shelves—minimum of one, maximum of eight—are equipped with xPON access cards.

An E9-2 chassis becomes an aggregation shelf or an access shelf once a card of that type is inserted into the chassis. The E9-2 OLT system is a disaggregated collection of access shelves, with each access line card connecting externally to the aggregation shelf—forming a larger OLT system. With the aggregation card, the E9-2 collapses the functions of the traditional OLT, aggregation switch, and edge router with subscriber management into a single system. This disaggregated system uses data center high bandwidth interconnect technology to support scaling to a very high density, non-blocking capacity to enable service providers to converge mobile, business and residential services networks over a single unified network structure.

Overview of E9-2 Hardware

There are two types of Calix E9-2 Intelligent Edge systems:

- Calix E9-2 ASM3001 systems:
  - For access aggregation and edge routing applications, each E9-2 shelf is equipped with one or two Aggregation Service Manager (ASM3001) cards and operates as a standalone system.
- Calix E9-2 CLX3001 systems:
  - For L3/L2 FTTx access applications, a collection of E9-2 shelves comprises an OLT system, where one shelf is equipped with one or more control and aggregation (CLX3001) cards, and the remaining shelves—minimum of one, maximum of eight—are equipped with xPON access cards.
  - An E9-2 chassis becomes an aggregation shelf or an access shelf once a card of that type is inserted into the chassis. The E9-2 OLT system is a disaggregated collection of access shelves, with each access line card connecting externally to the aggregation shelf—forming a larger OLT system. With the aggregation card, the E9-2 collapses the functions of the traditional OLT, aggregation switch, and edge router with subscriber management into a single system. This disaggregated system uses data center high bandwidth interconnect technology to support scaling to a very high density, non-blocking capacity to enable service providers to converge mobile, business and residential services networks over a single unified network structure. A two-shelf OLT system is shown below, with one aggregation shelf (top) and one access shelf (bottom).

E9-2 front chassis view

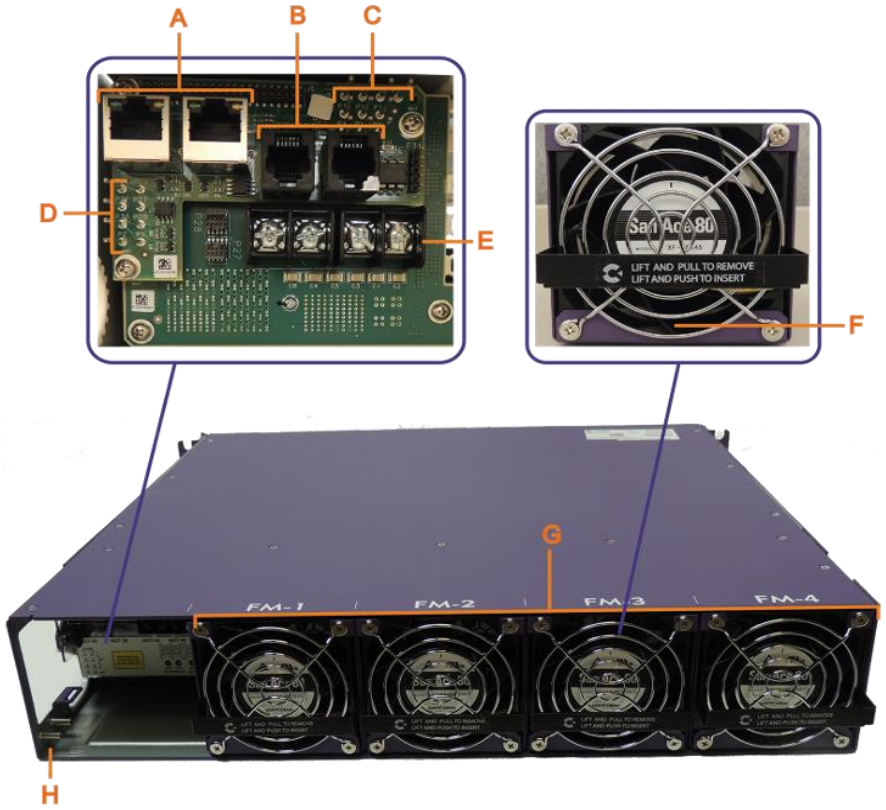
The Calix E9-2 shelf consists of a 2-slot 2RU chassis, with up to two aggregation or two access line cards installed into the front of the shelf:

- Slot 1 (bottom)
- Slot 2 (top)

Note: An E9 'blank' card plugs into either of the two universal slots and is used to maintain emissions and facilitate proper airflow in E9-2 systems with only one card. Whenever an E9-2 shelf operates with only one card, a blank card must be installed in the other slot.

E9-2 rear chassis view

The following components can be viewed from the rear panel of the E9-2 chassis:



A	**MGT-3A/MGT-3B**: (2) 10/100/1000 Ethernet management interface ports with RJ-45 connectors for a fixed out-of-band management connection
B	**MGT-4A/MGT-4B**: (2) RS-232 serial management interface ports with RJ-11F connectors to connect to a PC for a console management connection
C	BITS timing interfaces to support synchronization with an external clock source. **Note:** There is no BITS timing input capability on access line cards. Access line cards receive timing from the control and aggregation cards
D	Alarm I/O**:** (4) external alarm input/output wire wrap pins
E	-48 VDC and RTN power inputs (A/B)
F	(4) Fan module status LEDs, located behind the fan blades at the bottom of the module
G	FM-1 to FM-4: Fan modules that pull air from the front of the chassis and exhaust out the rear
H	Frame ground connection

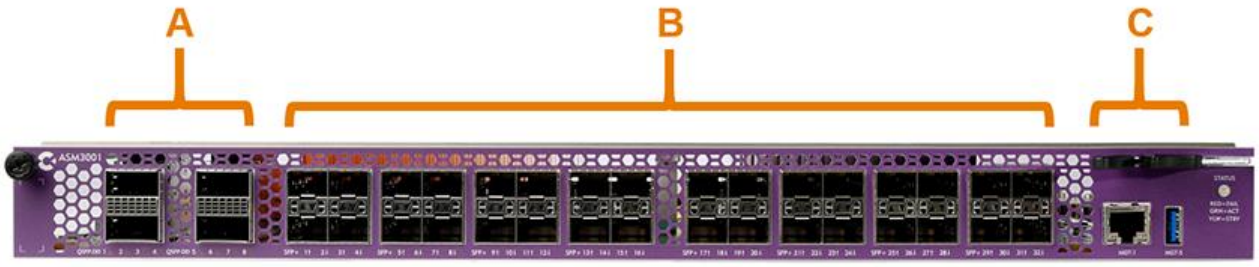
E9-2 aggregation cards

An E9-2 shelf supports up to two aggregation cards, which must be of the same type:

- For access aggregation applications where each E9-2 shelf is a standalone system, use the E9-2 aggregation service manager (ASM) card(s) in that shelf.
- For L3/L2 FTTx OLT applications, where each multi-shelf OLT system contains one aggregation shelf per node, use the E9-2 control & aggregation switch (CLX) card(s) in that shelf.

E9-2 aggregation service manager card (ASM3001)

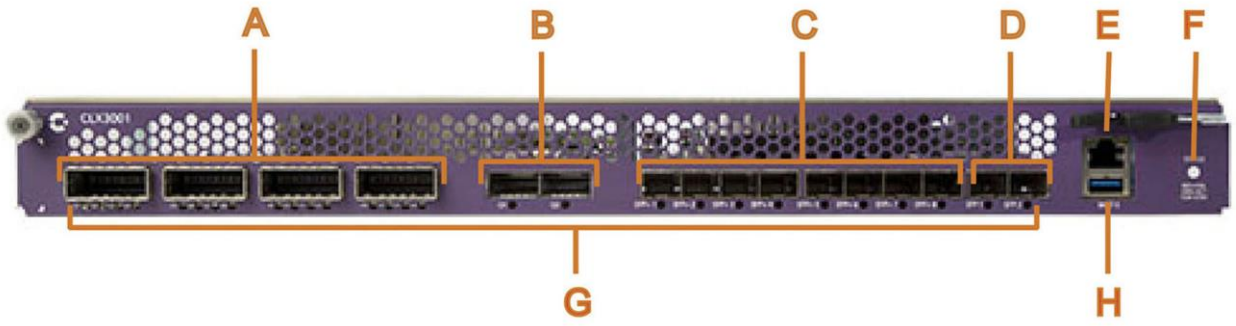
An E9-2 shelf supports up to two aggregation service manager cards. The following ports and components can be viewed from the faceplate of an ASM3001 card, for example:



A	**QSFP-DD:** (4) QSFP-DD sockets for housing up to 200GE modules or DAC cables per port for uplink connections
B	**SFP+**: (32) SFP+ 10GE ports for aggregation (support 10G/2.5G/1G Ethernet SFP+ modules)
C	**MGT-1**: (10/100/1000 Ethernet port, RJ-45 connector) Craft port for use in lab qualification, testing, configuration, and maintenance activities **MGT-5**: Ethernet management port with a USB 2.0 interface for local upgrade and rescue functions (future)

E9-2 control and aggregation switch card (CLX3001)

An E9-2 shelf supports up to two control and aggregation cards. The following components can be viewed from the faceplate of a CLX3001 aggregation card, for example:



A	**C-QSFP**: (4) CDFP ports, each containing (4) QSFP interfaces with CDFP copper connectors to support 4x100GE line rates for interconnecting to access line cards The E9-2 system uses CDFP–4x QSFP28 fan out cables to interconnect a control and aggregation card to access line cards.
B	**QSFP**: (2) QSFP-28 sockets for housing QSFP+ modules to support 100GE uplink connections
C	**SFP+**: (8) SFP 10GE uplink ports
D	**SFP**: (2) SFP 1GE uplink ports
E	**MGT-1**: (10/100/1000 Ethernet port, RJ-45 connector) Craft port for use in lab qualification, testing, configuration, and maintenance activities
F	Status LED (red/green/yellow) that shows the card's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information
G	Port status LEDs located below each C-QSFP/QSFP/SFP socket that show the given port's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information
H	**MGT-5**: Ethernet management port with a USB 2.0 interface for local upgrade and rescue functions (future)

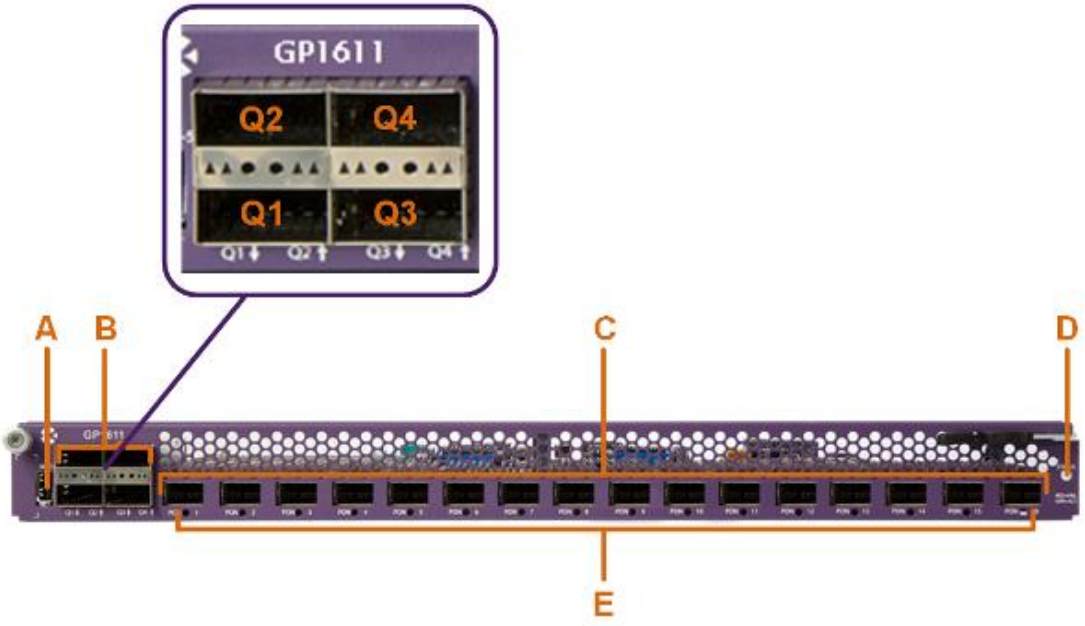
E9-2 fiber access line cards

For FTTx OLT applications, each E9-2 shelf supports up to two fiber access line cards, managed individually. Access line cards include 2.5G PON (GPON) and 10G PON (NG-PON2/XGS-PON) varieties, described below.

E9-2 GPON line cards (GP1611 and GP1612)

GP1611

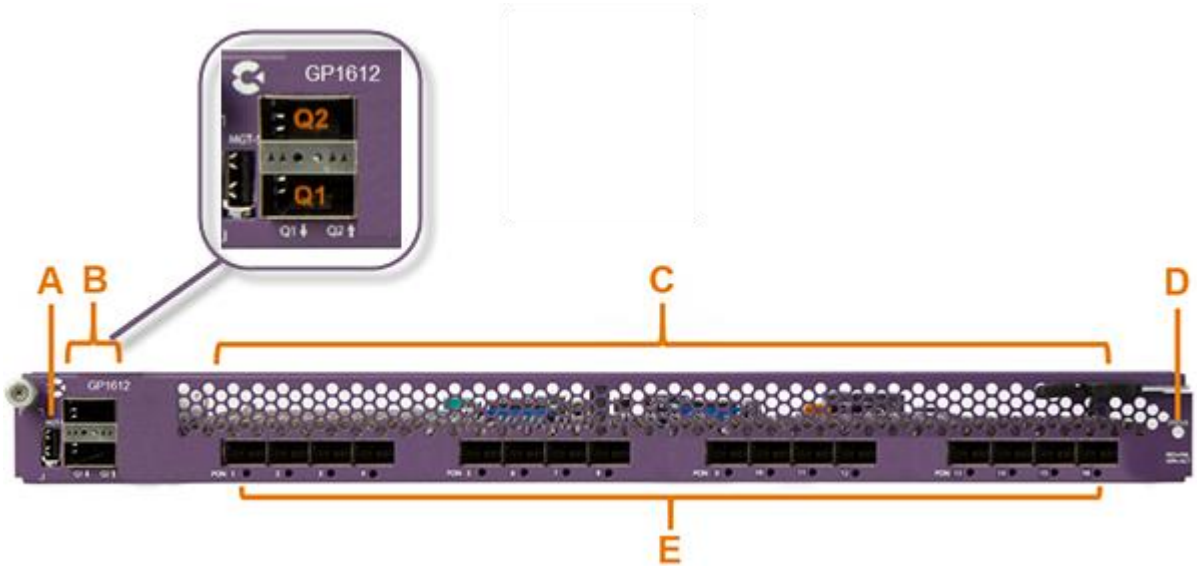
The following components can be viewed from the faceplate of a GP1611 card:



A	MGT-5: Ethernet management port with a USB 2.0 interface that connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access during turn-up and maintenance activities
B	Q1–Q4: QSFP-28 ports (two active, two standby) to support 4x10GE, 40GE or 100GE line rates for interconnecting to aggregation cards. 4x10GE connections support fan out cables; 40GE and 100GE connections support Direct Attach cables.
C	PON 1–PON 16: 16 SFP sockets for 2.5G/1.25G GPON access links.
D	Status LED (red/green) that shows the card's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information
E	Port status LEDs located below each XFP socket that show the given port's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information

GP1612 card

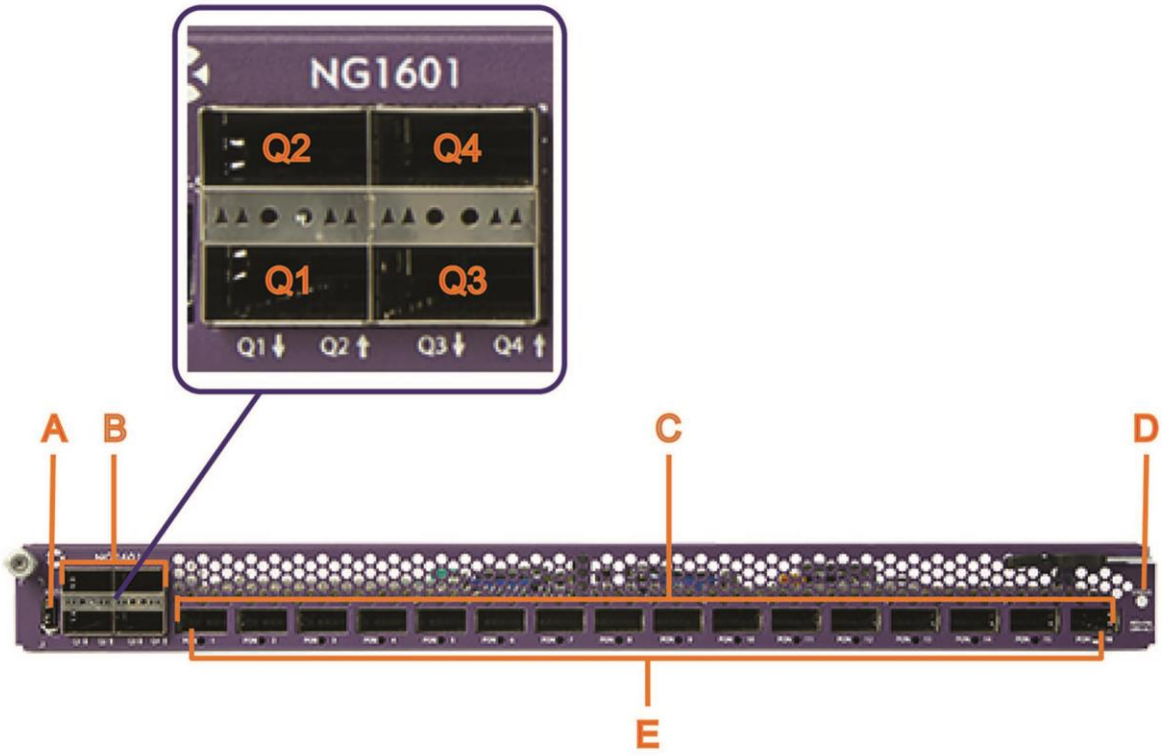
The GP1612 card operates identically to the GP1611 card while consuming 30% less power (and equipped with two 100GE QSFP ports instead of four).
The following components can be viewed from the faceplate of a GP1612 card:



A	MGT-5: Ethernet management port with a USB 2.0 interface that connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access during turn-up and maintenance activities
B	Q1–Q2: QSFP-28 ports (active, standby) for interconnecting to aggregation cards. Use QSFP Direct Attach cables to support 100GE or 40GE inter-connect links (ICLs).
C	PON 1–PON 16: 16 SFP sockets for 2.5G/1.25G GPON access links.
D	Status LED (red/green) that shows the card's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information
E	Port status LEDs located below each XFP socket that show the given port's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information

E9-2 10G PON line card (NG1601)

The E9-2 NG1601 10G PON access line card supports both NG-PON2 and XGS-PON technologies, depending on the type of optical modules are installed in the PON ports. The following components can be viewed from the faceplate of a NG1601 card:



A	MGT-5: Ethernet management port with a USB 2.0 interface that connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access during turn-up and maintenance activities
B	Q1–Q4: QSFP-28 ports (two active, two standby) to support 4x10GE, 40GE or 100GE line rates for interconnecting to aggregation cards. 4x10GE connections support fan out cables; 40GE and 100GE connections support Direct Attach cables.
C	PON 1–PON 16: XFP sockets housing NG-PON2 or XGS-PON optic modules to support 10G/10G or 10G/2.5G access links
D	Status LED (red/green) that shows the card's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information
E	Port status LEDs located below each XFP socket that show the given port's operational status; refer to *E9-2 LED Behavior* (on page 392) for more information

Air filter assembly

The E9-2 shelf supports an optional front-mounted air filter assembly. The filtration system allows for viewing of the card status LEDs and can be removed for card servicing.

Note: E9-2 systems that are installed in environments that comply with ISO 14644-1 Class 8 standards (accomplished through use of facility MERV-13 level air filtration or equivalent) do not require use of the Calix air filtration assembly. For other non-qualifying indoor environments, Calix strongly recommends using the air filtration assembly to protect the E9-2 electronics from airborne contaminants.

Note: Airflow direction is front to back, with cooling fan modules located at the rear of the shelf.

E9-2 High Availability

A system that is highly available operates continuously and reliably, providing services even in the presence of failures. To remain highly available, the AXOS systems use the following:

- Elimination of Single Points of Failures by providing redundancy within the system
- Link protection in crossover points that connect the redundant components together
- Fast detection of failures so services are restored quickly

Elimination of Single Points of Failures

Redundancy provided within the system ensures that failure of a single component (hardware, software or firmware) does not result in the failure of the entire system.

- **Aggregation shelf**

  The cards in the aggregation shelf serve as dual common controller cards supporting 1:1 equipment redundancy for a highly available system. The cards operate in an Active / Standby arrangement providing non-stop operation of the management applications and underlying control plane and data plane protocols. The AXOS applications and protocols operate in an active / standby arrangement such that any hardware or operating system failure causes an automatic switch to the standby controller yielding a highly available system. The E9-2 shelf backplane provides an interconnection between the CPU subsystems on aggregation cards for facilitating application state synchronization, database synchronization, and protocol synchronization.

  Related commands:

  ```
  redundancy auto-switchover <enable|disable [duration <n>]>
  show redundancy status
  ```

- **Wavelength mobility**

  After the initial activation and wavelength selection of NG-PON2 ONUs, wavelength mobility allows ONUs to transition from one wavelength to another on the PON as needed, in support of the following applications:

  - Shifting wavelengths to provide a hitless system upgrade
  - Equipment protection

  To support wavelength mobility, the NG-PON2 OLT and ONUs must be configured in advance; subsequently, ONU wavelength shifts can be initiated by automatic processes or intentional user commands.

Redundancy in Crossover Points

Protected connections between redundant components ensures a reliably available system.

The E9-2 has inter-chassis links (ICL) between the aggregation cards and the access line cards that operate in an Active/Standby LAG arrangement. Two links are members of the LAG from the active aggregation card and two links are members from the standby aggregation card. Four member-links are combined to form a single LAG to each line card.

Connections between aggregation cards and access line cards are physical connections using CDFP–4x QSFP28 fan out cables, with a 1:4 split.

Note: When a CDFP cable is pulled on a CLX3001 aggregation card, convergence times of >50 msec are observed (times are on the order of hundreds of milliseconds). This issue is not seen when a QSFP cable is pulled on an NG1601 access card. There is no workaround this is a hardware limitation.

Note: Calix recommends consistently using the interconnect pattern illustrated in the *E9-2 Installation Guide*; during startup, the aggregation card provides each line card with a shelf number which is derived from the physical port(s) used to connect the aggregation card to the line card.

Fast Detection of Failures Restores Services

Quickly detecting a failure and switching over to standby secondary components, the system ensures continuously available equipment.

High Availability (HA) Service Level Agreement (SLA) is typically measured in terms of a number of 9s. For example, an SLA level of six 9s (or 99.9999%) implies a total outage/downtime that adheres to the following constraints.

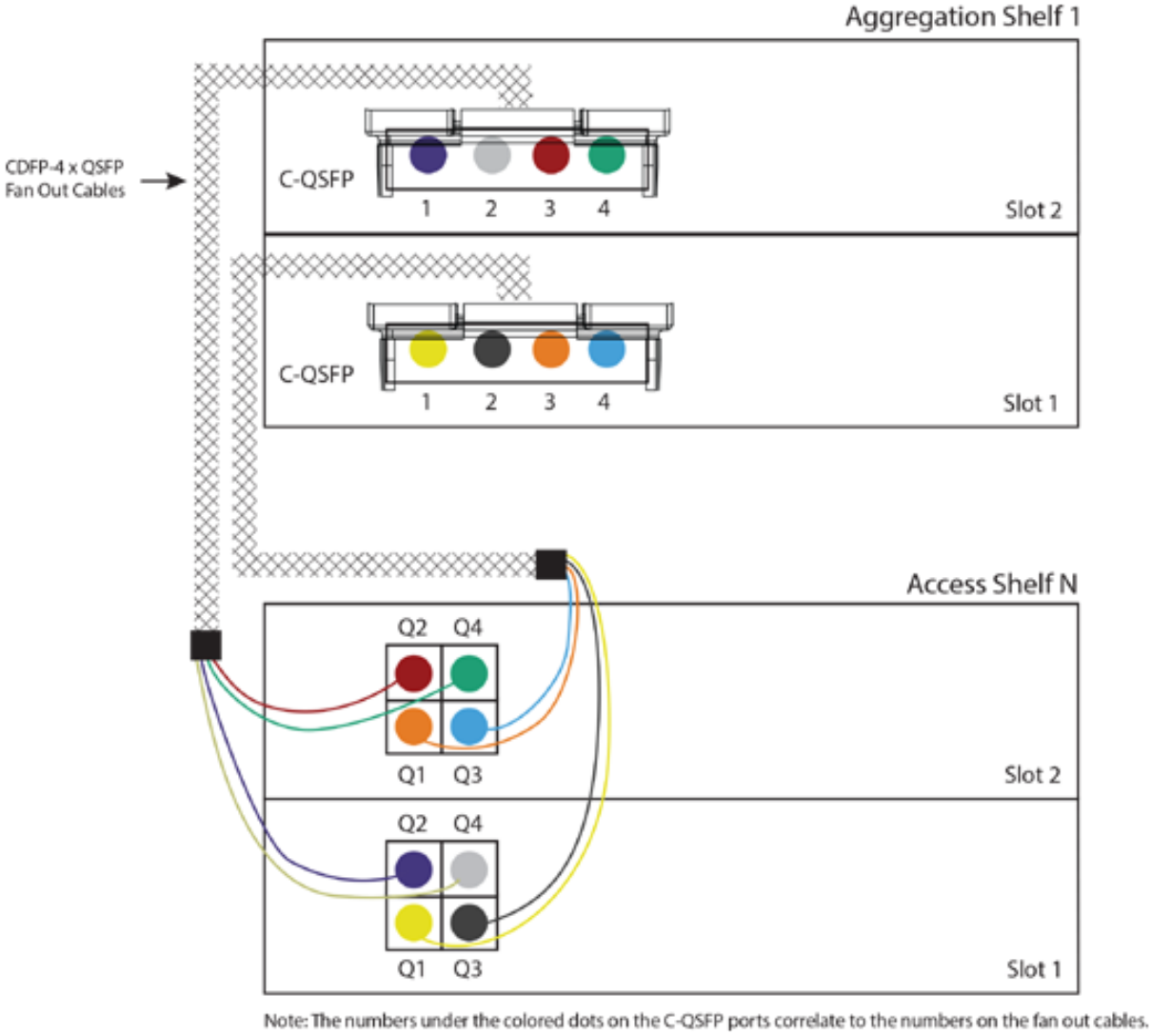
Downtime	Period
86.4 milliseconds	daily
604.8 milliseconds	weekly
2.59 seconds	monthly
32.5 seconds	yearly

E9-2 Inter Chassis Links- Active/Standby LAG

Note: This topic currently applies to 200G ICL configurations, such as used for 10G PON access cards.

The E9-2 uses Inter-Chassis Links (ICL) between the aggregation cards and the access line cards that operate in an Active/Standby LAG arrangement. Two links are members of the LAG from the Active aggregation card and two links are members from the Standby aggregation card. Four member-links are combined to form a single LAG to each line card. The aggregate capacity of the ICL to each line card is 200GE as only one Aggregation card is in the Active state at any given time.

Note: See the *Calix E9-2 Installation Guide* for information on interconnecting the E9-2 shelves.

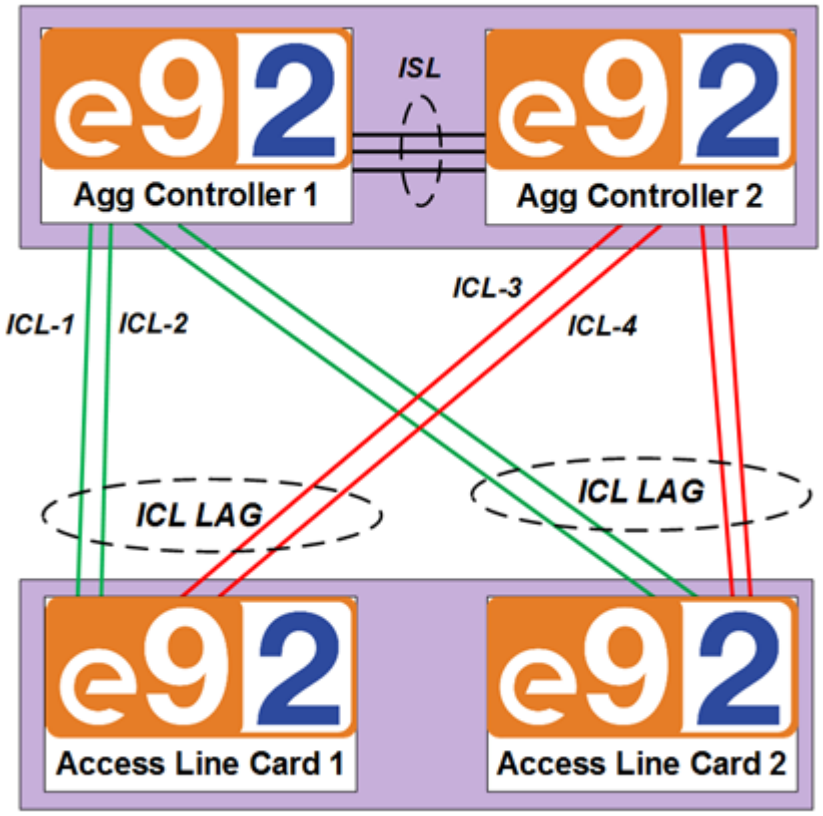


Note: The numbers under the colored dots on the C-QSFP ports correlate to the numbers on the fan out cables.

All ICLs on any access line card are in one ICL LAG interface. The ICL LAG interface consists of four 100 gig ports, with two ports homing in on one card running active and in the bundle with the other two ports as standby and not in the bundle. The port pairs are configured in discrete protection groups, 1 and 2. This affinity allows for the protection path to switch as a group in response to degradations/failures in member ports in one of the protection groups. The standby ICL LAG links carry no bearer traffic in normal operation (only OAM-CFM/CCM). Note that the E9-2 supports the ability to manually determine which ICL protection group to keep active, as described in *Configuring ICL LAG Switchover* (on page 263).

Note: If either of 2 links in the active protection group ICL go down, working links in the standby protection group ICL will forward traffic instead. By design, active and standby protection group ICLs cannot both forward traffic at the same time; as a result, if one link goes down in **both** the active and standby protection group ICLs, only the one remaining link in the standby protection group ICL will forward traffic, reducing the ICL capacity to 100G (even though a link in the formerly active protection group ICL is still up).

The following illustration shows ICLs 1-4 connected to access line card 1 as follows: ICL-1 and ICL-2 are active and ICL-3 and ICL-4 are standby. The two aggregation cards are connected by an Inter-switch link (ISL).



When installing or replacing access cards in an E9 system, consider the following configuration guidelines:

- LAG groups la25-la32 are used specifically for the downlinks from aggregation cards to the access line cards. (LAG interfaces la1 – la2 are used for uplinks)
- The aggregation card instantiates the system LAGs (la25-la32) with a role of ICL automatically upon correct connection and includes the appropriate aggregation card Ethernet ports as members of the appropriate LAG.
- The aggregation shelf can have up to 8 LAGs for the southbound ports with members coming from either aggregation card in shelf 1.
- Each access card instantiates only 1 LAG (slot-LAG la1) with a role of ICL automatically and includes the appropriate Ethernet ports as members of the slot-LAG.
- The access line cards can each have only one LAG with its members being only the 4 north facing ports
- LAG members on each access line card are limited to only the 4 north facing ports (q1 through q4):
    - Members can only be from the same card.
    - The LAG for each access card is uniquely identified by shelf/slot/la1.
- LAG groups expect physical ports of the same speed.

Note: See the *Calix E9-2 Installation Guide* for information on interconnecting the E9-2 shelves.

Turn-Up Process

This topic provides high-level steps for the initial turn-up of an AXOS system.

Note: At any time, you may skip to step 9 to save configuration changes.

1. Power-on and boot up the system.
2. Establish an initial management connection, as supported by your AXOS system:
   a. Connect to a local management port
   --OR--
   Connect via the default in-band management configuration
   b. Log into the CLI.

   Note: (E7-2/E9-2) After step 2, you may skip to step 8 and back to establish a permanent out-of-band management connection. For in-band management, going through the rest of these steps in order is recommended.
3. Upgrade the system software, if required. For details, see the *Calix AXOS Upgrade Guide*.
   - For systems that boot up with an operational software version: Calix recommends checking for and upgrading to the latest production software release that is available for your system.
   - For systems that boot up with the factory default image (FDI): In order to be operational, these systems must be upgraded to a production software release after boot up is complete and before putting the system into service. FDI-related alarms will be present until an upgrade to a production software release has occurred. For more details, see the *Calix Quick Tip (AXOS QT-21-0021 Factory Default Image for AXOS Systems: What You Need To Know)*.
4. Configure network transport (for example, Layer 2 or Layer 3 uplink interfaces)
5. Configure basic system settings as needed.
6. Configure user authentication and authorization settings as needed.
7. (Optional, E9-2 CLX only) Confirm the forward-table mode that should be used for your deployment. See *Configuring the Forward-Table Mode* (on page 262).

   Note: If changing from the default (mode-1) to mode-2, you must reload the system.
8. Configure the system for remote management.
9. Save your configuration.

After the initial turn-up outlined above, you may establish remote management of the system and configure services.

Connecting to a Local Management Port

This topic describes how to connect to a local management port, to establish local or temporary out-of-band management of the system for initial turn-up activities.

Note: For remote management, configuring in-band management and permanent out-of-band management are covered elsewhere in this guide.

For the location of each management port (per system), see the table below:

Management Port	E3-2 Location (1)	E7-2 Location	E9-2 Location (2)
*RJ-45 Ethernet (MGT-1)	RJ-45 port inside the case. • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1/1/1 • interface craft 1/2/1 • For local/temporary management access.
RJ-45 Ethernet (MGT-3)	N/A	RJ-45 port on the rear panel • interface craft 2 • For a permanent out-of-band connection.	RJ-45 ports on the rear panel, labeled MGT-3A and MGT-3B. • interface craft 1/1/2 • interface craft 1/2/2 • For a permanent out-of-band connection • For use with interface system-craft
*RS-232 Serial (MGT-4)	RJ-11 port inside the case • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 port on the front panel • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 ports on the rear panel, labeled MGT-4A and MGT-4B • Always enabled with fixed connection settings. • For local/temporary management access.
*USB (MGT-5)	External • interface wifi wlan1 • Requires a compatible, user-supplied USB Wi-Fi adapter. • For local/temporary management access.	N/A	N/A

Note: Ports marked with an * are typically considered for local/temporary management access.

Other notes:

(1) If supported by the installed E3-2 control module.

(2) Only E9-2 aggregation shelf locations are shown in this table.

(3) E9-2 access shelf locations:

- RJ-45 Ethernet (MGT-3A and MGT-3B) on the rear panel of access shelves
- interface craft x/1/1 and interface craft x/2/1, where x is greater than 1
- For local/temporary management access

Related topics:

- *Configuring the RJ-45 (MGT-1) Ethernet Management Port* (on page 338)
- *Configuring the RJ-45 (MGT-3) Ethernet Management Port* (on page 342)
- *Configuring the RS-232 Serial (MGT-4) Management Port* (on page 342)
- *Configuring the USB (MGT-5) Ethernet Management Port* (on page 343)

Connecting Via the RJ-45 Ethernet Port (MGT-1)

This topic describes how to connect your PC to the RJ-45 Ethernet management port for local access, using either a dynamically (DHCP) or statically assigned IP address for communication.

Management Port	E3-2 Location (1)	E7-2 Location	E9-2 Location (2)
RJ-45 Ethernet (MGT-1)	RJ-45 port inside the case. • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1/1/1 • interface craft 1/2/1 • For local/temporary management access.

(1) If supported by the installed E3-2 control module.

(2) Only E9-2 aggregation shelf locations are shown in this table.

(3) E9-2 access shelf locations:

- RJ-45 Ethernet (MGT-3A and MGT-3B) on the rear panel of access shelves
- interface craft x/1/1 and interface craft x/2/1, where x is greater than 1
- For local/temporary management access

Note: For E9-2 systems, you must connect to the *active* aggregation card (status LED lit green).

The procedures in this topic provide examples for a Windows 7 operating system; adjust for your operating system as needed.

To configure your PC to communicate using DHCP

Note: The Ethernet management port and its internal DHCP server are enabled by default.

1. From the Start menu, click **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.
2. Click the **Properties** button.

   The Local Area Connection Properties window displays.
3. Under, "This connection uses the following items:," select **Internet Protocol Version 4 (TCP/IPv4)** from the list.
4. Click the **Properties** button.

   The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
5. On the General tab, verify that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
6. Click **OK**, and close all dialog boxes.
7. Connect your PC to the Ethernet management port with a 'straight-through' Ethernet patch cable with RJ-45 connectors on both ends.

To configure your PC to communicate using a static IPv4 address

1. From the Start menu, click **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.
2. Click the **Properties** button.

   The Local Area Connection Properties window displays.
3. Under, "This connection uses the following items:," select **Internet Protocol Version 4 (TCP/IPv4)** from the list.
4. Click the **Properties** button.

   The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
5. On the General tab, do the following:
   a. Click the **Use the following IP address** option.
   b. In the IP address box, type **192.168.1.2**
   c. In the Subnet mask box, type **255.255.255.0**.
   d. Leave the remaining boxes blank.
6. Click **OK**, and close all dialog boxes.
7. Connect your PC to the Ethernet management port with a 'straight-through' Ethernet patch cable with RJ-45 connectors on both ends.

To log in

After configuring your PC and connecting it to the Ethernet management port, you can log into the CLI.

Connecting Via the RS-232 Serial Port (MGT-4)

This topic describes how connect your PC to the RS-232 management port and establish a local console connection.

Management Port	E3-2 Location [1]	E7-2 Location	E9-2 Location [2]
RS-232 Serial (MGT-4)	RJ-11 port inside the case • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 port on the front panel • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 ports on the rear panel, labeled MGT-4A and MGT-4B • Always enabled with fixed connection settings. • For local/temporary management access.

(1) If supported by the installed E3-2 control module.

(2) Only E9-2 aggregation shelf locations are shown in this table.

Note: For E9-2 systems, you must connect to the *active* aggregation card (status LED lit green).

To establish a local console connection

Note: This procedure assumes that you have installed a VT100 terminal emulation program on your PC (such as HyperTerminal or Procomm Plus).

1. Connect your PC to the RS-232 serial port with an appropriate RS-232 console cable (DB-9F to RJ-11M). Refer to the installation guide for instructions.
2. Launch a VT100 terminal emulation program on your PC, and configure the program to match the following default port characteristics: 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.

   For example, launch a HyperTerminal session as follows:

   a. On the Start menu, click **All Programs** > **Accessories** > **Communications** > **HyperTerminal**.

   b. In the Connection Description dialog box > Name field, type a name for the session and then click **OK**.

   c. In the Connect To dialog box > Connect Using list, select the PC COM port connected to the serial cable. For example, click **COM1**.

   d. In the COM# Properties dialog box, on the Port Settings tab, do the following:

   - In the Bits per Second list, click **115200**.
   - In the Data Bits list, click **8**.
   - In the Parity list, click **None**.
   - In the Stop Bits list, click **1**.
   - In the Flow Control list, click **None**.

Note: The communication settings of your PC COM port must match the settings on the serial port.

e. Click **OK** to connect.

3. In the console window, press the **Enter** key to initiate the console session.
4. When prompted, enter the user name and password to log into the CLI. For example:
   - User name: **sysadmin** (default)
   - Password: **sysadmin** (default)
5. At the prompt, enter **cli**.

Connecting Via the USB Ethernet Port (MGT-5) (E3-2 only)

The topic describes how to connect your PC or mobile device to the USB Ethernet management port.

Management Port	E3-2 Location (1)	E7-2 Location	E9-2 Location
USB (MGT-5)	External • interface wifi wlan1 • Requires a compatible, user-supplied USB Wi-Fi adapter. • For local/temporary management access.	N/A	N/A

(1) If supported by the installed E3-2 control module.

Considerations

- The USB interface supports access via a Wi-Fi-enabled PC or mobile device (smartphone or tablet); supported operating systems include Android, iOS and Windows.
- A compatible, user-supplied USB Wi-Fi adapter is required. For requirements, see the installation guide.
- Refer to the product label for the following factory default information:
  - Service Set Identifier (SSID): CalixCraft-XXXX, where XXXX is the last four hex digits of the system MAC address
  - SSID passphrase: Calix_XXXX, where XXXX is the last four digits of the product serial number

To establish a Wi-Fi connection

1. Connect your Wi-Fi adapter to the USB interface.
2. From your PC or mobile device, display the available wireless networks (SSIDs).

   For example (laptop, Windows 7):

   a. Move the wireless switch on your laptop to the ON position.

   b. From your laptop, select **Start** > **Control Panel** > **Windows Mobility Center**.

   c. Turn the wireless network on, and then close the window.

   d. From the Control Panel, select **Network and Sharing Center** > **Connect to Network**.

      A list of available wireless networks displays. If the SSID does not display (ssid-broadcast parameter = DISABLED), you can still connect manually.

3. Select the SSID (for example, CalixCraft_0006).

   Note: Refer to Considerations above for more information.

4. Enter the SSID passphrase (for example, Calix_8400).

   Note: Depending on the OS of your device, the passphrase may also be referred to as a security key or password.

To log in

After establishing a Wi-Fi connection through the USB management port, you can log into the system. Be sure to disconnect the Wi-Fi adapter from the system when you are done.

Logging into the CLI

Calix AXOS systems support an embedded Command Line Interface (CLI) for system management access via local or remote TCP/IP connections and local console connections. Please refer to *CLI Overview* (on page 48) for information about how to use the CLI.

Considerations

- You can access the CLI using one of the following methods:
  - **Secure Shell (SSH) connection:** You can establish an SSH (port 22) connection using the IP address of the:
    - Front RJ-45 craft port: 192.168.1.1 (default for craft 1, craft 1/1/1, and craft 1/2/1)
    - (E3-2 only) USB Ethernet management port: 169.254.42.1 (default for wlan 1
    - Out-of-band management interface: user-configured address
    - In-band management interface: user-configured address
  - **Telnet connection:** After enabling Telnet on the system, you can establish a Telnet connection (port 23) using the IP address of the:
    - Front RJ-45 craft port: 192.168.1.1 (default for craft 1, craft 1/1/1, and craft 1/2/1)
    - Out-of-band management interface: user-configured address
    - In-band management interface: user-configured address

  Note: Telnet does not provide a secure connection.

  - **Serial connection:** Via the RS-232 serial management port
- Login usernames and passwords are case sensitive.
- The system supports up to eight simultaneous CLI sessions. When eight sessions are active, and a user with permissions logs in, the session of an active user with the lowest permissions is terminated.
- Immediately after the system boots up, logins are not accepted for a brief period of time. If your login is not accepted, try again in a few minutes.
- If the first login attempt fails, a backspace keystroke used during the second and third prompt to login may turn into the Ctrl-H (^H) character depending on the terminal type used. This also causes such login attempts to fail.
- After logging in, the system may not accept commands for up to 60 seconds.
- Once you have logged in, you may change the default CLI session timeout as follows:
  - Calix-1(config)# cli session-timeout <0-255>

  Note: Entering 0 prevents CLI sessions from timing out.

Procedures

To establish a SSH connection from a PC or mobile device

1. Ensure that a SSH client program has been installed (for example, SecureCRT or puTTY).
2. Launch the SSH client program.
3. Using the IP address of the management port as the host IP address, begin an SSH session. For example:

   For example: **192.168.1.1** (default for craft 1, craft 1/1/1, or craft 1/2/1)
4. When prompted, enter the user name and password to log into the CLI. For example:
   - User name: **sysadmin** (default)
   - Password: **sysadmin** (default)

To establish a Telnet connection from a PC

1. Enable Telnet for the system:
   a. Log in via SSH (as described above) and enter the following command at the config level:

      Calix-1(config)# cli telnet enable

   b. Log out of the SSH session.
2. Ensure that a Telnet client program has been installed.
3. Launch the Telnet client program.
4. At the Telnet command prompt, type **o** (open host) followed by a space and the host IP address, and then press **Enter**.

   For example: **o 192.168.1.1** (default for craft 1, craft 1/1/1, or craft 1/2/1)
5. When prompted, enter the user name and password to log into the CLI. For example:
   - User name: **sysadmin** (default)
   - Password: **sysadmin** (default)

To establish a serial connection from a PC

See Connecting Via the RS-232 Serial Port.

CLI Overview

Calix AXOS systems support an embedded Command Line Interface (CLI) for system management access via local or remote TCP/IP connections and local console connections.

Command modes

The CLI command modes support specific sets of commands. The table below lists the command modes, access method, and associated CLI prompt.

Mode	Access Method	Prompt	Exit Method
Operational	Log in.	**`Calix-1#`**	Enter the **exit** command to end the CLI session.
Main configuration	From the Operational mode, enter the **configure** command.	**`Calix-1(config)#`**	Enter the **exit** command or **end** command (Ctrl+ Z) to return to the Operational mode.

The main configuration mode is the highest level of configuration mode. From the main configuration mode, you can enter a variety of sub-configuration modes to make changes to the running configuration. For example, the table below shows the interface configuration mode.

Mode	Access Method	Prompt	Exit Method
Interface configuration	From the main configuration mode, enter the applicable interface command: **interface restricted-ip-host 1**	**`Calix-1(config-restricted-ip-host-1)#`**	Enter the **exit** command to move one level up. Enter the **top** command to move to the highest configuration mode level. Enter the **end** command or use the Ctrl+Z key combination to return to the Operational mode.

Note that a configuration command may be issued from any mode if it is a valid command. However, the help (either tab or "?") is context sensitive and will only show the sub-commands present under that mode.

The 'do' form of an Operational mode command

From any configuration mode, you can issue Operational mode commands by using the **do** form of the command. For example, enter **do show cli** from the *interface ethernet X* configuration mode, entering the following complete command:

```
Calix-1(config-craft-1)# do show cli
```

Note: From the main configuration mode, you can enter a partial do form of a command followed by the tab key to complete the command name. From all sub-configuration modes, you must enter the complete do form of the command. There is no help or command expansion available for do commands in the sub-configuration modes.

The 'no' form of a command

Most configuration commands have a **no** form that is used to delete the configuration or return a command to its default settings. For example, enter **no interface craft 1** to reset craft 1 to default settings.

To determine whether a configuration command has a **no** form, enter a question mark at the prompt or following the command or keyword as shown below:

```
Calix-1(config)# interface craft 1
Calix-1(config-craft-1)# ?
Description: Craft Port
Possible completions:
  description   Craft Port description (255 characters maximum)
  ip            craft interface IP Address and Netmask
  shutdown      craft port administration state
  ---
  exit          Exit from current mode
  no           Negate a command or set its defaults
  top           Exit to top level and optionally run command
  <cr>
```

CLI Help

The CLI includes interactive Help. You may request help at any point in the command-line by entering a question mark (?) to list possible completions (syntax options), as described in the table below.

At the system prompt, enter ...	To ...	Example
?	List all available commands.	**Calix-1# ?** **Possible completions:** **accept Accept config** **clear Clear object data** **...**
partial command<**tab key**>	Expands a partial command name.	**Calix-1(config)# upg<tab> upgrade**
*partial command***?**	List commands that begin with the character string.	**Calix-1# se?** **Possible completions:** **send Send message to terminal of one or all users** **session Session settings for autonomous notifications**
command **?**[1]	List syntax options (possible completions) associated with a command.	**Calix-1(config)# terminal ?** **Possible completions:** **<generic/xterm/vt100/ansi/linux>** **screen-length Configure screen length** **screen-width Configure screen width**
command + keyword **?**[1]	List syntax options (possible completions) associated with a keyword.	**Calix-1# start vca ?** **Possible completions:** **join Join and snoop a multi-cast channel** **snoop Snoop a multi-cast channel**

[1] Command requires a space between the command and the question mark.

Note: A carriage return <cr> symbol indicates that you may press the **Enter** key to execute the command, without adding any syntax.

Displaying User Configured Options to Complete a Command

When completing a command, entering the TAB key and the question mark are sometimes both required to see all the available options for command completion. The tab key shows a list of configured values vs a ? key, which shows a list of possible CLI commands.

For example, to issue the command **clear meg** {*meg-name*} **mep** {*mep-id*} **statistics**, the tab and question mark keys can be used as follows:

- When the command "clear meg" is issued with a question mark, the following information appears:

```
node# clear meg ?
Description: Clear Maintenance Entity Group Information
```

- However, when the command "clear meg" is issued with a tab, a list of previously configured MEG names is displayed:

```
node# clear meg  (tab)
Possible completions:
  new_meg1  new_meg2  new_meg3  pMEG
```

- In the next step, issuing a question mark displays that "mep" or "mip" are the two possible parameters for the command:

```
node# clear meg new_meg1 ?
Description: Clear Maintenance Entity Group Information
Possible completions:
  mep   Clear Maintenance End Point Information
  mip   Display Maintenance Intermediate Point Information
```

- In the next step, issuing a question mark will not display any specific information, as the only available options are user configured:

```
node# clear meg new_meg1 mep ?
Description: Clear Maintenance End Point Information
```

- Instead, issue the tab key to display the previously configured MEP IDs (1 and 5):

```
node# clear meg new_meg1 mep (tab)
Possible completions:
1 5
```

- Issue the question mark to display the remaining options to complete the command:

```
node# clear meg new_meg1 mep 1 ?
Description: Clear Maintenance End Point Information
Possible completions:
delay-measurement-bin Clear MEP delay measurement statistics bin
delay-measurement-session Delay measurement session
loss-measurement-bin Clear MEP loss measurement statistics bin
loss-measurement-session Loss measurement session
statistics Clear MEP statistics
node# clear meg new_meg1 mep 1 statistics
```

Editing command-line entries

To navigate on the command line, use the following keystrokes:

- The ← and → arrows allow editing in the current line.
- The Ctrl+A key combination moves the cursor to the beginning of the line.
- The Ctrl+E key combination or the **End** key moves the cursor to the end of the line.
- The Ctrl+B key combination moves the cursor back a space.
- The Ctrl+F key combination moves the cursor forward a space.

To delete text, use the following keystrokes:

- The Ctrl+U key combination deletes all text on the current line.
- The Ctrl+K key combination deletes text from the cursor to the end of the line.
- The Ctrl+W key combination deletes the word to the left of the cursor.
- The **Delete** or **Backspace** key deletes the character to the left of the cursor.

To recall commands, use the following keystrokes:

- The Ctrl+P key combination recalls the previous command.
- The Ctrl+N key combination accesses the next command.
- The ↑ and ↓ arrows recall previous and/or next commands.

Output Modifiers

For commands that generate a lengthy output, you may use a modifier so that the output displays only the information that you want to see. Type the command followed by the pipe symbol (|) and desired output modifier. For example, enter the command **show alarm | count** to display only the number of lines in the alarm output. To determine whether a command supports output modifiers, enter a question mark following the command or keyword.

The CLI supports the following output modifiers:

- **append** *filename* or *.bash_history*—Append the output text to a file.
- **begin** *regular expression*—Begin the output with the first line in which a match of the regular expression is found and all lines that follow.
- **count**—Count the number of lines in the output.
- **exclude** *regular expression*—Exclude all lines in which a match of the regular expression is found.
- **include** *regular expression*—Include only lines in which a match of the regular expression is found.
- **linnum**—Enumerate lines in the output.
- **more**—Paginate the output.
- **nomore**—Suppress the pagination.
- **save** *filename, .bash_history,* or *overwrite*—Save the output text to a file.
- **until** *regular expression*—End the output with the first line in which a match of the regular expression is found.

Note: The --More-- prompt displays for output that extends beyond the visible screen. To continue the output, press the **Return** key to scroll down one line or press the **space bar** to display the next full screen of output. To discontinue the output and return to the system prompt, use the Ctrl-C key combination.

Command syntax guidelines

Note the following command syntax guidelines:

- [] Square brackets enclose an optional parameter, or enclose a list of two or more optional values separated by pipe bars, where one (and only one) of these values may be included in the CLI command string.
- <> Angle brackets enclose a required value.
- {|} Braces enclose a list of two or more required values separated by pipe bars, where one or more of these values (if supported) may be included in the CLI command string.
- For commands that have optional parameters, you can specify them in any order or omit any that are unnecessary.
- When entering a name string that includes a special character (space, tab, question mark [?], pipe bar [|], etc.), begin and end the name with double quotes.
- If you enter a command incorrectly—for example, a command name that does not exist—the message "Invalid input detected at '^' marker" displays. The caret (^) indicates where the (first) error is located.
- If you do not enter all of the keywords or values required by the command, the message "syntax error: incomplete path" displays.

Chapter 2

Configuring Network-Facing Layer 2 Interfaces (Layer 2 Uplinks)

This chapter describes how to configure network-facing Layer 2 interfaces (Layer 2 uplinks) for AXOS systems.

Configuring a Layer 2 Single-Port Uplink

This topic describes how to configure a Layer 2 single-port uplink.

Configuration guidelines

- Assumptions:
  - All required network equipment and devices are installed, powered on, and functioning properly
  - All required profiles are created, such as a transport service profile (TSP)

Related topics

- *Creating and Modifying Transport Service Profiles* (on page 292)
- *Configuring Ethernet Parameters* (on page 297)

Configuration process

1. Navigate to an Ethernet interface.
2. Ensure that switchport is enabled.
3. Ensure that the role is set to INNI.
4. Select a transport service profile (TSP).

   Note: If SYSTEM_TSP is already applied to an interface, you may keep it (and modify it as needed); alternatively, you may remove it and apply a newly created TSP.
5. Configure additional parameters as required.
6. Ensure the interface is administratively enabled.

Configuration example

```
configure

interface ethernet 1/1/x1
switchport enabled
role inni
!!example of removing SYSTEM_TSP and applying a new TSP
no transport-service-profile SYSTEM_TSP
transport-service-profile TSP1
no shutdown
top
```

Configuring a Layer 2 LAG Uplink

This topic describes how to configure a Layer 2 LAG uplink.

Configuration guidelines

- Assumptions:
  - All required network equipment and devices are installed, powered on, and functioning properly.
  - All required profiles are created, such as a transport service profile (TSP).
- Configuration rules:
  - You must configure the LAG on both sides of the link.
  - You must set the interfaces on either side of the link to the same speed.
- **Configuration options:**
  - To configure an **active-active (A/A) LAG**:
    - Set the max ports (max-port) value to >= the number of ports in the LAG. For example, if 2 member ports are in the LAG, set max-port to 2 or greater.
    - Operation: When a failure occurs, the available bandwidth is reduced by the amount of bandwidth carried over the failed port.
  - To configure an **active-standby (A/S) LAG**:
    - Set the max ports (max-port) value to < the number of ports in the LAG. For example, if 2 member ports are in the LAG, set max-port to 1.
    - Enable LACP (lacp-mode = "active" or "passive," but not "none").
    - Operation:
      - Member ports exchange LACPDUs to communicate aggregation information.
      - Members automatically detect link failures and dynamically manage port protection.
      - The lacp-port-priority designates standby ports positioned to come online when an active port fails, effective if the current AXOS system is controlling the LAG.

Note: The LACP system priority (lacp actor-system-priority) + LACP system MAC (show lacp actor-system) is compared with that of the other system (on the other side of the link) to determine which system controls the LAG. The the system with the lower value controls the LAG.

- To configure **same-card LAG**, add member ports from one card
- To configure **cross-card LAG**, add member ports from two cards (E9-2 and E7-2 dual-card systems only)

- Related commands for cross-card LAG:

```
[CLI operational mode]
redundancy auto-switchover
redundancy force-switchover
redundancy switchover
show card
show redundancy
show switchover status
```

Related topics

- *Creating and Modifying Transport Service Profiles* (on page 292)
- *Configuring LAG Interface Parameters* (on page 311)
- *Configuring Ethernet Parameters* (on page 297)

Configuration process

1. Create a switched LAG group:
   a. Enable the switchport.
   b. Set the role to INNI.
   c. Select a transport service profile (TSP).
   d. Set the max-port value as required:
      - For active-active LAG [LAG with all active ports], accept the default value.
      - For active-standby LAG [LAG with active and standby port(s)], select a value less than the number of ports that will be added to the group. (For example, if only 2 ports will be added to the group, set max-port = 1 so that the excess port can be standby.)
   e. Select the lacp-mode as required:
      - For static LAG, accept the default lacp-mode of "none"
      - For dynamic LAG, set the lacp-mode to "active" (recommended) or "passive"

   Note: Dynamic LAG is required for active-standby configurations.

   f. Configure additional parameters as required.
   g. Enable the interface.

2. Assign Ethernet interfaces to the LAG as member ports:
   a. Navigate to an Ethernet interface.
   b. Set the interface role to "lag" and system-lag to the lag name (for example, "la1").
   c. (For active-standby LAG) Set the lacp-port-priority differently to designate standby ports.
   d. Configure additional parameters as required.
   e. Ensure the interface is administratively enabled.
   f. Repeat for other interfaces.
3. (Optional) Check the LACP system priority & MAC address to compare with the other system (on the other side of the link) to ensure the correct system is controlling the LAG; modify the system priority, if needed. For an example, see the following steps a, b, c:
   a. Check the partner system's MAC and priority value:

```
[operational mode]
show interface lag <lag name> lacp
...
  partner
    ...
    system-id       <some MAC value> !! received partners system-mac
    system-priority <some priority value, such as 32768> !! received
partners system-priority
```

   b. Check the AXOS system's MAC and priority value:

```
[operational mode]
show lacp actor-system !!to see the system mac address
show lacp actor-system-priority !!to see the system priority value
```

   c. Change the AXOS system's priority value, if needed:

```
[configuration mode]
lacp actor-system-priority 20000 !!lower the value from the default
32768
```

Configuration examples

Active-Active LAG

```
configure

!!creating the LAG group
interface lag la1
switchport enabled
role inni
transport-service-profile TSP1 !!pre-created TSP
!!using default max-port value, max value of the system (e.g., 8)
no shutdown
top

!!adding two member ports
interface ethernet 1/1/x1
role lag
system-lag la1
no shutdown
top

interface ethernet 1/1/x2 !! or 1/2/x1 for cross-card LAG
role lag
system-lag la1
no shutdown
top
```

Active-Standby LAG

```
configure

!!creating the LAG group
interface lag la1
switchport enabled
role inni
transport-service-profile TSP1 !!pre-created TSP
max-port 1
lacp-mode active
no shutdown
top

!!adding two member ports
interface ethernet 1/1/x1
role lag
system-lag la1
lacp-port-priority 28672
no shutdown
top

interface ethernet 1/1/x2 !! or 1/2/x1 for cross-card LAG
role lag
system-lag la1
lacp-port-priority 32768
no shutdown
top
```

Configuring an G.8032v2 Ring for Uplink/Transport

This topic describes how to configure the uplink for a G.8032v2 ring.

The G.8032v2 Ethernet ring protocol provides protection switching on ring topologies, while preventing loops by blocking Ethernet data frames on one link. The Calix implementation of the G.8032v2 is compliant with the ITU G.8032/Y.1344 standard (dated 2/2012).

Each Ethernet ring consists of multiple nodes, with each node connected to adjacent nodes in the ring, using two independent links that could be LAGs. A port for a ring link is called a ring port. The G.8032v2 ring protection switching architecture provides loop avoidance by guaranteeing that, at any time, traffic flows on all but one of the ring links. This link is configured as the Ring Protection Link (RPL).

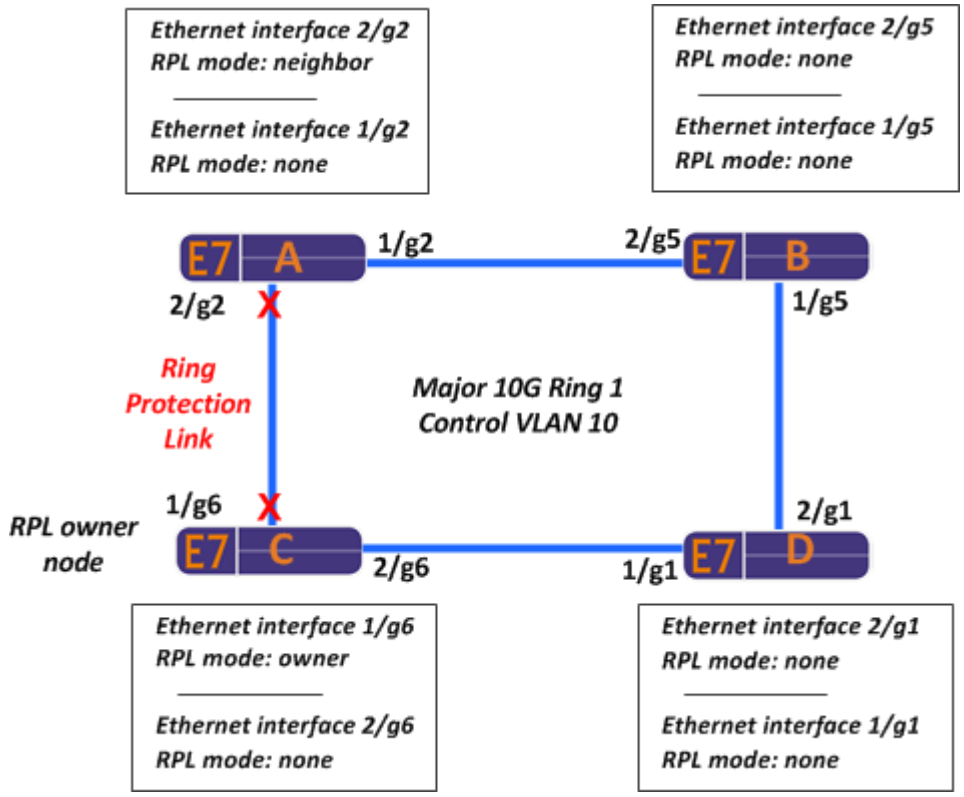
The G.8032v2 protocol allows for links of different speeds. For example, a mix of GE, 2.5G, and 10GE line rates in a single ring are permitted. However, the recommended practice is to configure the same rate for both ring ports on a node.

The nodes in a G.8032v2 ring are identified as follows:

- **RPL owner node**—the node with the designated Ring Protection Link (RPL) port that is responsible for blocking Ethernet data frames at one end of the RPL to prevent loops from occurring.
- **RPL neighbor node**—the node adjacent to the RPL owner node where the connecting port is optionally designated as the RPL Neighbor port that is responsible for blocking its end of the RPL.

Note: All other nodes in the ring are identified as RPL Mode "none".

The following graphic shows an *example* of a simple four node main 10GE ring that is referenced in the procedure below.



A control VLAN assigned to the G.8032v2 ring instance passes Ring Automatic Protection Switching (R-APS) packets between all nodes on the ring. The R-APS channel carries control messages for managing the blocking state of the ring.

Fault monitoring

You may configure maintenance group end points (MEPs) on the individual ring ports for Continuity Check Message (CCM) monitoring (as defined in ITU Y.1731). MEPs represented on ring ports monitor each ring link. At a specified interval, MEPs send CCM protocol data unit (PDU) messages to check continuity on the ring.

Link failures

The RPL owner node may detect a signal failure condition and initiate a ring switch due to the following situations:

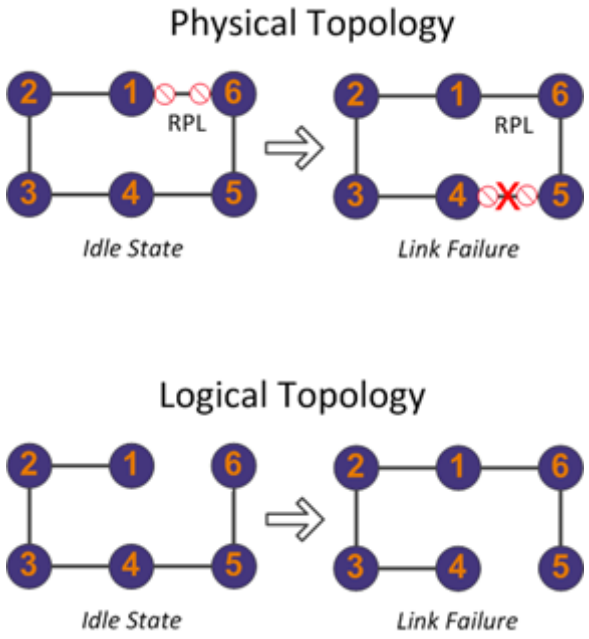
- A fiber cut
- Failure to receive consecutive timely or valid CCMs from MEPs
- Receipt of a Signal Fail (SF) message from any node on the ring

To initiate a ring switch, the RPL owner node unblocks the RPL owner port, forwards R-APS messages on the control VLAN, and flushes MAC addresses from its forwarding database (FDB). All nodes then unblock any blocking ports and perform a FDB flush, and learn the new ring topology.

The implementation of G.8032v2 works for both unidirectional failure and multiple link failure scenarios in a ring topology.

Ring nodes may be in one of the following states:

- **OOS** – Ring protocol is administratively down.
- **Idle** – Normal operation with no faults present on any ring node. The RPL is blocking.
- **Protection** – Ring is in protection switched state due to signal failure (SF) condition asserted at one or more ring nodes.
- **Manual Switch** – Ring is in manual switch state because a Manual Switch request has been set by the operator at a ring node.
- **Forced Switch** – Ring is in forced switch state because a Force Switch request has been set by the operator at a ring node.
- **Pending** – There is no SF condition or switch condition present on the ring and the RPL owner node is in the process of reverting the ring to the Idle state.



Configuration guidelines

Follow these guidelines when configuring an Ethernet transport ring with G.8032v2:

- One logical ring instance is supported per physical ring.
- One G.8032v2 physical ring supports up to 32 units.
  - Each E7 card consists of one unit; an E7 chassis containing two cards counts as two units.
  - Each CLX3001 aggregation shelf consists of one unit.
- Each E9-2 OLT system supports up to 16 G.8032v2 instance using 6 dual CLX cards (2x 100G ports and 8x 10G ports each).
- The E9-2 supports G.8032v2 to interconnect with other:
  - E9-2s or routers using 100GE or 10GE interfaces on the CLX3001 card.
  - E7-2s/E9-2s using 10GE interfaces on the CLX3001 card, and allows a mix of E7-2 AXOS and E7-2 EXA nodes.
- The E9-2/E7-2 support interlocked major rings; sub-rings are not supported.
- E9-2 supports L2 triple play traffic over G.8032v2 rings, including DHCP, PPPoE, and multicast traffic.
- (E7-2/E3-2 only) You can map a ring instance to any pair of GE or 10GE Ethernet ports in the ring.
- You can map a ring instance to LAG interfaces where the members of each LAG interface are on the same card.
- E9-2 ring LAGs:
  - To support G.8032v2 rings using > 10G interfaces, a ring LAG is required (for example, a 20G LAG ring consists of two 10GE interfaces on a single ring).
  - The maximum member count is eight.
  - Do not support CCM.
- (E7-2/E3-2 only) You can mix GE, 2.5GE, and 10GE line rate in a ring to allow for migrating from a GE ring to a 10GE ring.
- (E9-2 only) For VLANs in the ELINE mode, G.8032v2 rings do not support switch mode = CROSS-CONNECT.
- Configure the revertive/non-revertive mode at the RPL owner node. Note that as the RPL owner node controls the revert behavior, it does not matter what the revert configuration is at other nodes.
- Disable/Enable ring on nodes without owner/neighbor will not form into loop. (All nodes' ring ports are unblocked)

- Some devices do not send to the multicast address as calculated by using the Ring ID but send to the G.8032 Version 1 default MAC of 01-19-A7-00-00-01. Calix strictly adheres to the standard and will send the R-APS packets for each Ring ID to the multicast address 01-19-A7-00-00-[Ring ID]. If the addresses do not match, the G.8032 protocol will fail as messages are not properly interpreted by RPL owner and neighbor for each Ring ID. The destination address may be configurable on the 3rd party equipment as a workaround. Calix is *not* configurable.
- Adding SOAM (CFM) to an existing ring is service affecting.
- For E9-2 SOAM configurations on a G.8032v2 ring:
  - MEGs bound by the same ring ports should use the same level; note that the system does not prevent you from configuring different levels.
  - The 'ccm-protection auto' CLI command supports automatic internal creation of the MEG/MEPs, however the 'show meg' command does not display the created objects.

Procedures

To create a G.8032v2 ring (via SMx)

1. From the menu bar, click **Network**.
2. In the list of devices, click the name of the device to use. You might need to navigate to a region to find your device.
3. Click the **Ring** tab.
4. Click the **Network Ring Configuration** tab.
5. In the G8032 Ring table, click **Create G8032 Ring**.
6. In the Create G8032 Ring window, do the following:
   a. Select the node(s) to configure.

      The node specific parameter fields display.

   b. Reference the *G.8032 ring parameters* (on page 319) to configure, as required.

   c. Click **Submit** to save your changes.

To create a G.8032v2 ring (via CLI)

1. In the CLI configuration mode, enter the starting point command "g8032-ring" and enter a unique index number for the ring instance.

   ```
   g8032-ring <instance-id>
   ```

2. Reference the *G.8032 ring parameters* (on page 319) to configure, as required.

Examples

Assumptions:

- A TSP with service VLANs is applied to all ring interfaces.
  - (E3-2 only) All VLANs must be created on each node of the ring and be associated with the ring interfaces (via the applied TSP) of each node.
  - (E9-2/E7-2 only) All VLANs serving or passing through a node must be associated with the ring interfaces (via the applied TSP) of the node. However, only VLANs serving a given node must be created on the node.

Tip: (E9-2/E7-2 only) If a VLAN is only "passing through" a node, it does not have to be created on the node; it only has to be defined in the TSP used by the node.

Example with port x5 as ring interface and CCM:

```
configure

# Create ring
g8032-ring 1
control-vlan 2000
admin-state enable

# Create MEG and add down MEP to MEG
meg 22
remote-mep 1
mep 2
direction down
continuity-check enable

# Attach MEG to ring interface
interface ethernet 1/1/x5
no shutdown
role inni
g8032-ring 1
ccm-protection mep 22 2
```

Example with ports x1 and x2 as ring interfaces:

```
configure

g8032-ring 1
admin-state enable
description "One open standard ring"
control-vlan 500
ring-id 75
non-revertive disable
wait-to-restore-time 5
top

interface ethernet 1/1/x1
switchport enabled
role inni
g8032-ring 1 rpl-mode owner
top

interface ethernet 1/1/x2
switchport enabled
role inni
g8032-ring 1 rpl-mode none
top
```

CFM example (E3-2 only):

```
configure

g8032-ring 1
maintenance-entity-level 1
top

meg N1_to_N2
auto-discover disable
ccm-interval 10ms
level 1
mode y1731
mep 501
direction down
continuity-check enable
remote-mep 502
top

meg N1_to_N3
mep 501
direction down
continuity-check enable
remote-mep 503
top

interface 1/1/x1
description "Link to N2"
g8032-ring 1
top

interface 1/1/x2
description "Link to N3"
g8032-ring 1
```

Linked Re-Configuration example (E7-2 only)

This example assumes the G.8032v2 ring is configured on a single card system as described in the above example, and then a second card is added to the shelf and the system is reconfigured so each card has a designated G.8032v2 port.

Example with changing ring port 1/1/x2 to 1/2/x1 as ring interface:

```
configure

interface ethernet 1/1/x2
no g8032-ring 1
switchport enabled
top

interface ethernet 1/2/x1
switchport enabled
role inni
g8032-ring 1 rpl-mode none
top
```

CFM example:

```
configure

interface 1/1/x2
no g8032-ring 1

interface 1/2/x1
description "Link to N3"
g8032-ring 1
```

Configuring an ERPS Ring for Uplink/Transport

This topic describes how to configure the uplink for an ERPS ring.

Configuration guidelines

Follow these guidelines when configuring an Ethernet transport ring with ERPS.

- AXOS products support up to 16 ERPS rings.
- Each ERPS domain must have the following:
  - A unique domain name assigned to all nodes in the domain.
  - A unique control VLAN ID designated on each ring node.
  - One node designated as the controller node and the remaining nodes designated as transit nodes.
- A primary and secondary port must be designated on the controller node.
- A primary and secondary port must also be designated on the transit nodes.
- The secondary on the transit had to be facing a primary port on the controller node (and vice versa).
- A single node can be the Controller Node for all, some, or none of the ERPS domains on the system.
- Each Ethernet interface can only have one ERPS domain associated with it.
- E9-2 interconnects with other E7-2/E9-2 nodes using ERPS protocol over 10GE interfaces on the CLX3001 card; E7-2 AXOS and E7-2 EXA can be mixed within an ERPS ring.
- For E9-2:
  - ERPS over LAG is not supported.
  - For VLANs in the ELINE mode, ERPS rings do not support switch mode = CROSS-CONNECT.
- (E7-2 only) In E7-2 shelfs with two cards, traffic between rings is passed over the backplane between the two E7-2 cards.
- For the ERPS Control VLAN, use a VLAN ID that is NOT used for any services on the network.
- The ERPS ring Control VLAN is limited to passing the ERPS control PDUs.
- All node ports in an ERPS ring must be the same speed (for example, all 10GE).
- If you delete an ERPS domain from a node without first disabling the ports configured with the ERPS domain, a forwarding loop may potentially be introduced to the system. Calix recommends disabling the Ethernet ports containing the ERPS domain before deleting the ERPS domain from the system.
- To change any attributes on an ERPS domain, it must be disabled.

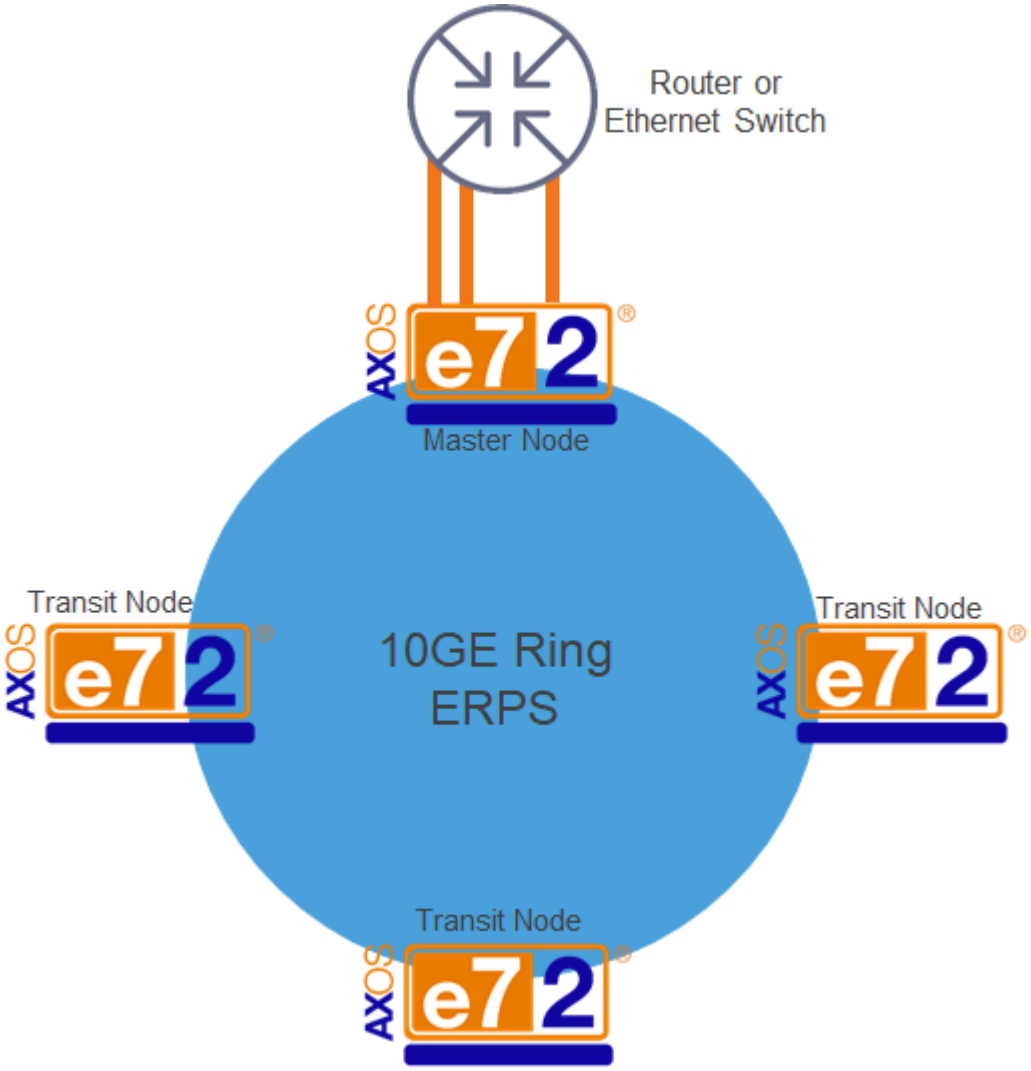
- (E7-2 only) If an E7-2 shelf with a single card is configured in an ERPS ring, the designated ERPS ports for that node will reside on the single card. However, if a second card is subsequently installed in the E7-2 shelf, one ERPS link for the node must be relocated to the second card and reconfigured such that each card has a designated ERPS port. See the "Re-Configuration Example" located at the end of this topic.
- An ERPS ring can support up to 32 units:
  - Each E7 card consists of one unit; an E7 chassis containing two cards counts as two units.
  - Each E9-2 aggregation shelf consists of one unit.
- A "chain of ERPS rings" should be limited to no more than 3 interconnected rings.
- Only modify the reserved VLAN of the system during a maintenance window, as the action is service affecting to the ERPS ring.
- (E3-2 only) All VLANs must be created on each node of the ERPS ring and be associated with the ERPS domain membership (via the applied TSP) of each node.
- (E7-2 only) All VLANs serving or passing through a node must be associated with the ERPS domain membership (via the applied TSP) of the node. However, only VLANs serving a given node must be created on the node.

  Tip: (E7-2 only) If a VLAN is only "passing through" a node, it does not have to be created on the node; it only has to be defined in the TSP used by the node.

- VLANs can be members of multiple ERPS rings. Traffic switched between rings and network designs must be reviewed to ensure forwarding loops are not introduced.
- The node periodically verifies that the ERPS control VLAN is still present in the forwarding table of the switch component. If the VLAN is not present in the hardware, an alarm is raised.
- A Health message is transmitted on the Controller Node primary interface at an interval of 1-10 seconds (user defined). If the Controller Node does not receive 3 consecutive Health messages on the secondary interface, it will generate an alarm, but does not automatically start forward traffic on the normally blocked secondary port.
- A Recovery message is sent from the Controller Node at an interval of 1-10 seconds (user defined) after a fault is detected on the ring to determine when the ring has recovered. The Controller Node must receive 6 consecutive Recovery messages to declare the ring as recovered, initiating a switchback.
- The total time for a ring to revert when the ring has recovered:

  6 RECOVERY tries * RECOVERY message frequency

The following image shows an example of an ERPS ring.



Configuration example

Example with ports x1 and x2 as ring interfaces:

```
configure

erps-ring 1
admin-state enable
description "One ring to rule them all"
control-vlan 500
health-time 5
recovery-time 1
role controller
topology-monitor enable
top

interface ethernet 1/1/x1
no shutdown
switchport enabled
role inni
erps-ring 1 role primary
transport-service-profile RING_VLANS
top

interface ethernet 1/1/x2
!! E9-2 example: 1/2/x1
no shutdown
switchport enabled
role inni
erps-ring 1 role secondary
transport-service-profile RING_VLANS
```

Re-Configuration example (E7-2 only)

This example assumes the ERPS ring is configured on a single card system as described in the above example, and then a second card is added to the shelf and the system is reconfigured so each card has a designated ERPS port.

1. Disconnect the ERPS link from a port and remove the port from the ring.
2. Connect ERPS link to a port on the second card.

Example with changing ring port 1/1/x2 to 1/2/x1 as ring interface:

```
configure

interface ethernet 1/1/x2
no erps-ring 1
no transport-service-profile RING_VLANS
top

interface ethernet 1/2/x1
no shutdown
role inni
erps-ring 1 role secondary
transport-service-profile RING_VLANS
top
```

Configuring the Uplink with RSTP

Note: This topic only applies to E3-2 and E7-2 systems.

This topic describes how to configure an uplink with RSTP.

Procedure

1. Configure an RSTP domain with parameter values as required for application:

```
rstp-domain <name>
!!parameter values as required
top
```

2. Add interfaces to the RSTP domain, editing the default RSTP interface parameters as required.

```
interface ethernet 1/1/x1
role inni
rstp domain <name>
!!RSTP interface parameters
!!rstp priorty ...
!!rstp cost ...
!!rstp topology ...
!!rstp topology-guard ...
transport-service-profile <TSP name>
no shutdown
top

!!repeat for additional interfaces
```

3. (Optional) To configure an RSTP node protection pair associated with an ERPS ring, use the RSTP domain "erps-ring" and "ring-role" parameters on the pair of nodes. For example, for nodes A and B:
   - RSTP domain on node A: **`erps-ring 1 ring-role primary`**
   - RSTP domain on node B: **`erps-ring 1 ring-role Secondary`**

Parameters

You can configure the following parameters for an RSTP domain:

Parameter	Description
rstp-domain <name>	A unique name for the RSTP domain, consisting of a string of 1–15 letters.
bridge-priority	Sets the root bridge. The bridge with the highest priority (lowest numeric value) becomes the RSTP root bridge. If all bridges have the same priority, the bridge with the lowest MAC address becomes the root bridge. Valid values: • 0 - 61440, in increments of 4096. (default = 32768) The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines hello-time, max-age-time and forward-delay-time.
erps-ring	Identifies the ERPS ring when associating with an ERPS ring. Valid value: • Name of a pre-configured ERPS ring.
forward-delay-time	The maximum time (in seconds) a bridge waits before changing states. This delay is required because every bridge must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. Valid values: • 4–30; (default = 20) As a general rule: 2 * (Forward Delay - 1) ≥ Max Age ≥ 2 * (Hello Time + 1)
hello-time	The time interval in seconds between BPDU configuration message generations by the root bridge. Valid values: • 1 • 2 (default)
max-age-time	The maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All bridge ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out RSTP information (provided in the last BPDU) becomes the designated port for the attached network. If it is a root port, a new root port is selected from among the bridge ports attached to the network. Valid values: • 6–40; (default = 20)
ring-role	When associating with an ERPS ring, and thus a partner RSTP domain, identify the role as primary (forwarding - active) or secondary (blocking). Valid values: • primary (default) • secondary

Chapter 3

Configuring Network-Facing Layer 3 Interfaces (Layer 3 Uplinks)

Note: This chapter only applies to the E3-2/E9-2.

This chapter describes how to configure network-facing Layer 3 interfaces (Layer 3 uplinks) for AXOS systems.

Layer 3 interfaces have Layer 3 (IP) interfaces associated with the AXOS system router.

Important: Prior to configuring a Layer 3 interface, you must ensure that security features, such as a control plane policy, have been configured. **After** configuring a Layer 3 interface, to establish connectivity with upstream routers, you must configure the AXOS system router for the required routing protocols.

Topics covered

- Configuring a Layer 3 single-port uplink (E3-2)
- Configuring a Layer 3 LAG uplink (E3-2)
- Configuring a Layer 3 LAG uplink (E9-2)

Configuring QoS for Control Plane Traffic (E9-2)

This topic describes how to configure QoS settings for control plane traffic, and is organized as follows:

- Overview | Configuration guidelines | Configuration process

Overview

E9-2 CLX systems allow you to configure QoS settings for control plane traffic (per application) originating from the E9-2 and egressing the network-facing (WAN) interface.

Configuration guidelines

- This functionality applies to control plane traffic originating from the E9-2 and egressing the network-facing (WAN) interface.
- This functionality must be enabled at a global level.
- Configurable QoS settings are PCP and DSCP, if applicable:
  - All applications have a PCP value (0-7)
  - IP-related applications also have DSCP value [DSCP PHB or hex value (0x00-0x3F) or decimal value (0-63)]
- When a DSCP map is configured on the 'For-Me' CoPP, note the following behavior depending on the global host application QoS admin state:
  - DISABLED: For packets egressing the CPU, the PCP values will be set by the DSCP map (mapped to PCP values based on the packet's DSCP value).
  - ENABLED: For packets egressing the CPU, if any PCP values are set by the host application QoS functionality, such values will override the PCP values specified by the DSCP map.
- Related CLI commands (config mode):
  - **`host application-qos admin-state {ENABLED|DISABLED}`** (default = DISABLED)
  - **`host application-qos <application name> dscp <dscp value> pcp <pcp value>`**

- Defaults values per application:

arp pcp 3	diameter dscp BE-CS0	ntp dscp EF
icmp dscp BE-CS0	diameter pcp 0	ntp pcp 4
icmp pcp 0	dhcp-v4 dscp CS6	dns dscp BE-CS0
bgp dscp CS6	dhcp-v4 pcp 3	dns pcp 0
bgp pcp 0	dhcp-v6 dscp CS6	ftp dscp BE-CS0
ospf dscp CS6	dhcp-v6 pcp 3	ftp pcp 0
ospf pcp 0	tacas dscp BE-CS0	tftp dscp BE-CS0
isis pcp 0	tacas pcp 0	tftp pcp 0
rip dscp BE-CS0	ssh dscp BE-CS0	syslog dscp BE-CS0
rip pcp 0	ssh pcp 0	syslog pcp 3
ldp dscp CS6	netconf dscp CS1	ipdr dscp BE-CS0
ldp pcp 0	netconf pcp 2	ipdr pcp 0
pim dscp CS6	snmp dscp BE-CS0	ipfix dscp BE-CS0
pim pcp 0	snmp pcp 0	ipfix pcp 0
igmp dscp CS3	http dscp BE-CS0	gnmi dscp BE-CS0
igmp pcp 0	http pcp 0	gnmi pcp 0
radius dscp BE-CS0	https dscp CS6	
radius pcp 0	https pcp 6	

Configuration process

1. Enable this functionality at the global level:

   ```
   host application-qos admin-state ENABLED
   ```

2. Configure the QoS settings (PCP and/or DSCP, if applicable) for an application. For example, to change the PCP value of BGP traffic from 0 (default) to 6, enter the following:

   ```
   host application-qos bgp pcp 6
   ```

3. Repeat Step 2 for as many applications as required.

Configuring a Layer 3 Single-Port Uplink (switchport disabled)

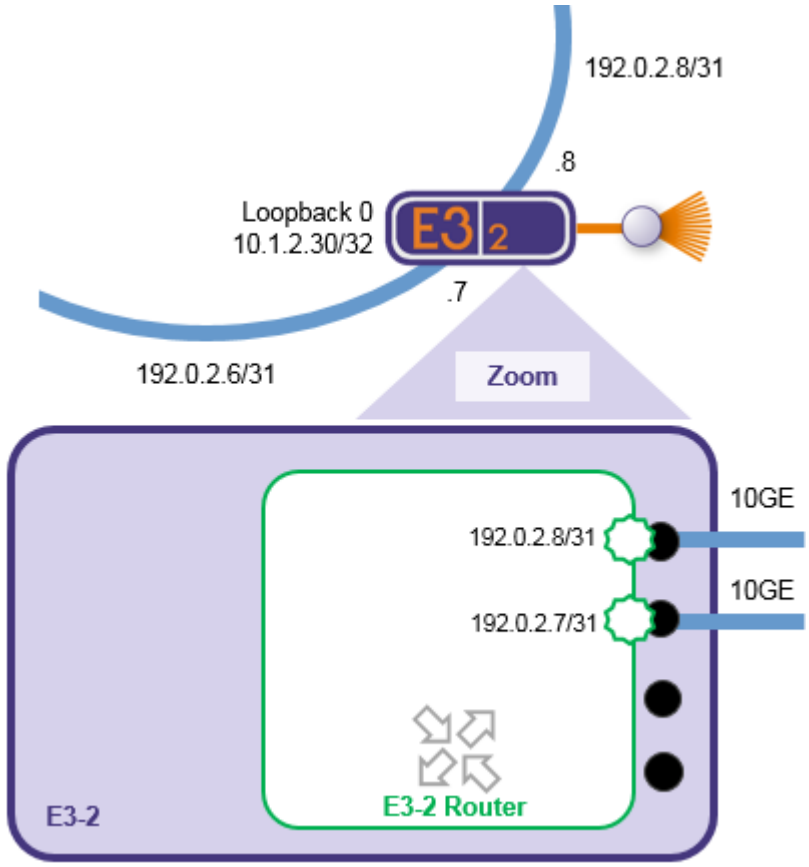
This topic describes how to configure the following single-port uplink for Layer 3 deployments:

- Ethernet interface in Layer 3, routed mode (switchport disabled), where IP interfaces are directly configured on the interface.

One such uplink per node can be used in a point-to-point topology. Two such uplinks per node can be used to include the node in a physical ring topology, where multiple nodes form a ring with upstream aggregation routers via 10GE links.

Configuration guidelines

- (Physical ring topology) Per node, two out of four 10GE routed WAN interfaces must be enabled for use.
- (Physical ring topology) Each participating 10GE interface must be configured with an IP address that is consistent with the network assigned per link.
    - For example, if using an IPv4 /31 network per link (to conserve public IP addresses), for the third node in the ring:
        - 10GE WAN interface 1/1/x1 = 192.0.2.8/31
        - 10GE WAN interface 1/1/x2 = 192.0.2.7/31



- For example, if using an IPv6 /127 network per link (to conserve public IP addresses), for the third node in the ring:
  - 10GE WAN interface 1/1/x1 = 2001:DB8:3::1/127
  - 10GE WAN interface 1/1/x2 = 2001:DB8:4::0/127

- (Physical ring topology) Each node constitutes a Layer 3 hop.
- Assumptions:
  - All required profiles are created:
    - DSCP map profile (optional)

Note: In Layer 3 applications, a DSCP map on a WAN Ethernet interface may be used for determining downstream packet priority. If a DSCP map is not applied, packets map to priority value 0.

    - IP access control list (optional)
  - Security features, such as a control plane policy, have been configured.

Configuration process

1. Navigate to an ethernet interface.
2. Disable the switchport.
3. Assign an IP address to the interface.
4. Configure additional parameters as required. For example:
   - (Optional) DSCP map profile: dscp-map <profile name>
   - (Optional) IP access control list: access-group {ipv4-acl | ipv6-acl} <profile name>
   - (Optional) Reverse path forwarding (RPF): ip-unicast-rpf {loose | strict}
5. Ensure that the interface is administratively enabled.

After the uplink configuration, to establish connectivity with upstream routers, you should configure the system router for the required routing protocols.

Example

```
configure

interface ethernet 1/1/x1
switchport disabled
ip address 192.0.2.8/31
ipv6 address 2001:DB8:3:1/127
no shutdown
top

interface ethernet 1/1/x2
switchport disabled
ip address 192.0.2.7/31
ipv6 address 2001:DB8:4::0/127
no shutdown
top
```

Related topics

- *Configuring Ethernet Parameters on the Uplink* (on page 297)

Configuring a Layer 3 LAG Uplink (switchport disabled)

This topic describes how to configure the following LAG uplink common for E3-2 Layer 3 deployments:

- LAG in Layer 3, routed mode (switchport disabled), where IP interfaces are directly configured on the LAG.

Configuration guidelines

- The switchport on the LAG interface should be disabled, and the switchport on the Ethernet interfaces should be enabled (default); only then can you configure Ethernet ports to be in the LAG.
- You can configure the LAG to have more members than the Max Port value, where the lacp-port-priority designates standby ports positioned to come online when an active port fails.
- Assumptions:
  - All required profiles are created:
    - DSCP map profile (optional)

Note: In Layer 3 applications, a DSCP map on a WAN Ethernet interface may be used for determining downstream packet priority. If a DSCP map is not applied, packets map to priority value 0.

    - IP access control list (optional)
  - Security features, such as a control plane policy, have been configured.

Configuration process

1. Create a routed LAG group
   a. Disable the switchport.
   b. Assign an IP address.
   c. Configure additional parameters as required. For example:
      - (Optional) DSCP map profile: **`dscp-map <profile name>`**
      - (Optional) IP access control list: **`access-group {ipv4-acl | ipv6-acl} <profile name>`**
      - (Optional) Reverse path forwarding (RPF): **`ip unicast-rpf {loose | strict}`**
   d. Ensure that the group is administratively enabled.

2. Assign Ethernet interfaces to the LAG.
   a. Navigate to an Ethernet interface.
   b. Set the interface role to "lag" and group to the lag name (for example, "la1").
   c. Configure additional parameters as required.
   d. Ensure the group is administratively enabled.

After the uplink configuration, to establish connectivity with upstream routers, you should configure the system router for the required routing protocols.

Example (static LAG):

```
configure

!!step 1
interface lag la1
switchport disabled
ip address 1.1.1.2/24
no shutdown
top

!!step 2
interface ethernet 1/1/x1
role lag
system-lag la1
no shutdown
top
```

Related topics

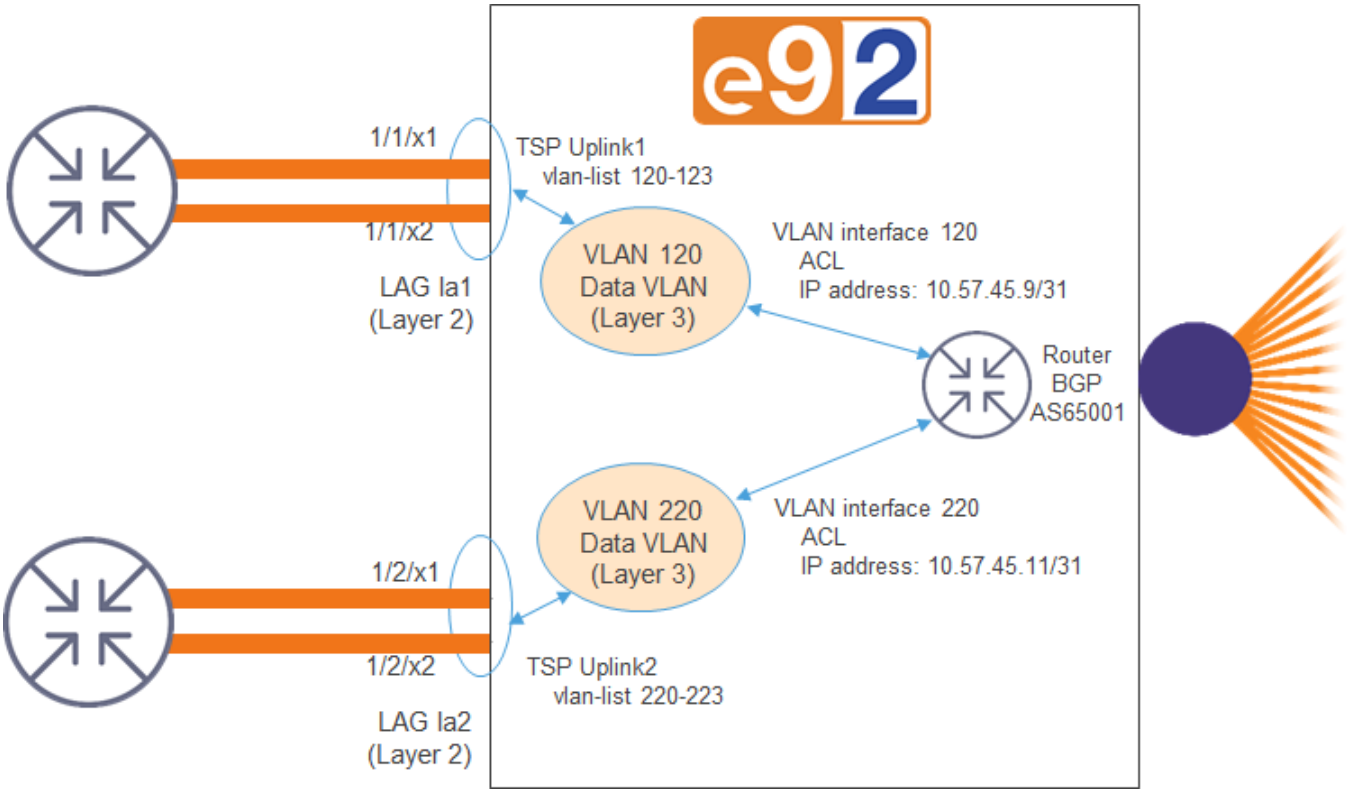
- *Configuring LAG Interface Parameters* (on page 311)
- *Configuring Ethernet Parameters on the Uplink* (on page 297)

Configuring a Layer 3 LAG Uplink (switchport enabled)

This topic describes how to configure the following LAG uplink common for E9-2 Layer 3 deployments:

- Dual LAG uplink—two LAGs links to two upstream routers
  - LAG 1 with members on the active aggregation card
  - LAG 2 with members on the standby aggregation card
- LAGs in Layer 2, switched mode (switchport enabled), where IP interfaces are not directly configured on the LAGs
- Layer 3 VLANs associated with the LAGs (via TSPs)
- IP interfaces configured on the Layer 3 VLAN interfaces

This configuration is depicted in the following diagram:



Configuration process

1. Prior to the configuration, confirm that security features, such as a control plane policy, have been configured.
2. Configure IP prefix lists for local interfaces (static management interfaces and the DHCP pool). An IP prefix list defines one or more IPv4 addresses and subnets to match against. IP prefix lists used for uplink LAG interfaces are used as match criteria for routing; the local interfaces are added to the routing table via the IP prefix lists.
3. Configure an IPv4 Access Control List (ACL) that references the IP prefix list. An ACL denies or permits traffic.
4. Create two sets of Layer 3 VLANs (one set per LAG), with each set comprised of a unique VLAN for each service
5. Per VLAN, create a VLAN interface, applying the previously configured ACL and defining an IP address
6. Create two transport service profiles (TSPs), one for each LAG with the corresponding set of VLANs added
7. Configure two LAG interfaces; per LAG:
   a. Confirm that switchport is enabled
   b. Apply the corresponding TSP
   c. Configure additional parameters as required
   d. Enable the interface
8. Configure LAG members (Ethernet interfaces)
   - First group of member ports on the active aggregation card and assigned to the first LAG
   - Second group of member ports on the standby aggregation card and assigned to the second LAG
9. After the uplink configuration, to establish connectivity with upstream routers, you should configure the system router for the required routing protocols.

Configuration example

```
!!assumptions: prefix lists and ACLs already created
```

!!vlans on first LAG

```
vlan 120
 description "Data VLAN"
 l3-service  ENABLED
!
vlan 121
 description "SIP VLAN"
 l3-service  ENABLED
!
vlan 122
 description "Multicast Video VLAN"
 l3-service  ENABLED
!
vlan 123
 description "Unicast Video VLAN"
 l3-service  ENABLED
!
```

!!vlans on second LAG

```
vlan 220
 description "Data VLAN"
 l3-service  ENABLED
!
vlan 221
 description "SIP VLAN"
 l3-service  ENABLED
!
vlan 222
 description "Multicast Video VLAN"
 l3-service  ENABLED
!
vlan 223
 description "Unicast Video VLAN"
 l3-service  ENABLED
!
```

!!interface vlans

```
interface vlan 120
 ip address 107.150.6.1/24
 no shutdown
!
interface vlan 121
 ip vrf forwarding voice
  ip address 107.151.0.1/30
 !
 no shutdown
!
interface vlan 122
 ip address 107.150.0.1/24
 ip pim 1
 !
 no shutdown
!
interface vlan 123
 ip vrf forwarding unicastvideo
  ip address 107.150.1.1/24
 !
 no shutdown
!
interface vlan 220
 ip address 107.150.7.1/24
 no shutdown
!
interface vlan 221
 ip vrf forwarding voice
  ip address 107.150.3.1/24
 !
 no shutdown
!
interface vlan 222
 ip address 107.150.4.1/31
 ip pim 1
 !
 no shutdown
!
interface vlan 223
 ip vrf forwarding unicastvideo
  ip address 107.150.5.1/24
 !
 no shutdown
!
```

!!transport-service-profiles

```
transport-service-profile uplink_lag3
 vlan-list 120-123
!
transport-service-profile uplink_lag4
 vlan-list 220-223
!
```

!!LAG interfaces

```
interface lag la3
 hash-method               enhanced
 lacp-mode                 active
 role                      inni
 transport-service-profile uplink_lag3
 no shutdown
!
interface lag la4
 hash-method               enhanced
 lacp-mode                 active
 role                      inni
 transport-service-profile uplink_lag4
 no shutdown
!
```

!!LAG members

```
interface ethernet 1/1/x2
 no shutdown
 role       lag
 system-lag la3
!
!!more LAG member ports may be added

interface ethernet 1/2/x1
 no shutdown
 role       lag
 system-lag la4
!
!!more LAG member ports may be added
```


.

.

Chapter 4

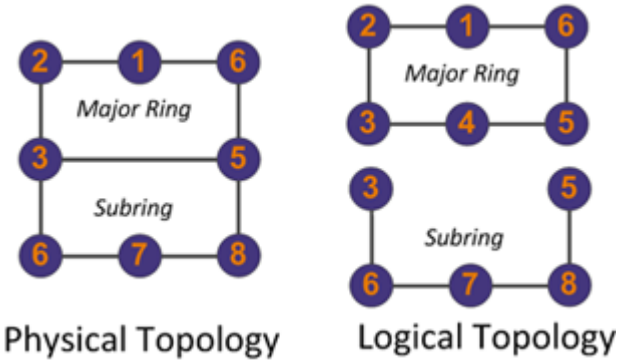
Configuring Access-Facing Layer 2 Interfaces (Layer 2 Downlinks)

This chapter describes how to how to configure access-facing Layer 2 interfaces (Layer 2 downlinks) for AXOS systems.

Configuring Subtended Rings

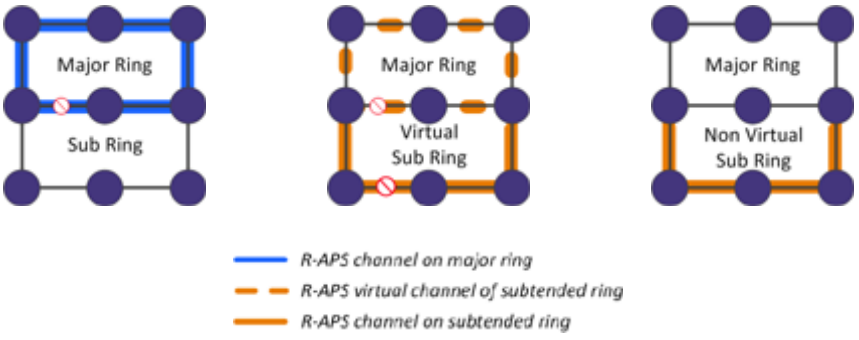
The E7-2 supports the configuration of subtended rings (sub-rings) off major G.8032v2 or ERPS rings. Each major and sub-ring has its own ring instance ID and control VLAN ID. All links of a major ring are controlled by the major ring instance. The sub-ring is not a closed ring and does not share control of any links with the major ring. The nodes that house major rings and sub-rings, are called interconnection nodes.

Note: The maximum amount of sub-rings that can be attached to a major ring is 5.



Two types of subtended rings can be configured off of a major ring:

- Virtual Sub-ring: This type of sub-ring configures the control VLAN for the sub-ring on all ring ports of the major ring. G.8032v2 R-APS messages for the sub-ring pass across the shared link or around the main ring, depending on where the RPL owner port is located. The shared link is controlled by the major ring instance. R-APS messages for the Virtual sub-ring instance are encapsulated and transmitted over a virtual channel on the major ring (if the link ports are unblocked).
- Non-Virtual Sub-ring: This type of sub-ring isolates R-APS messages pertaining to the sub-ring instance to the interconnect nodes and the nodes that are part of the sub ring. The R-APS channel on the sub-ring is terminated at the interconnection nodes. The sub-ring control VLAN is not built on any of the main ring interfaces.



-

- Each ring instance (major or sub-ring) has its own unique Ring ID (ring instance ID) and control VLAN ID.
- A sub-ring must connect to a major ring to avoid inherent confusion of ownership for a shared link between them. Configuration attempts to connect a sub-ring to a sub-ring will be rejected.
- Transport Service profiles:
  - Major ring interfaces:
    - The non-virtual sub-ring control VLAN is not added to the TSP on nodes in the major ring.
    - The virtual sub-ring control VLAN must be added to the TSP on all nodes in the major ring, except for the interconnection node where the sub-ring joins the major ring. The sub-ring's control VLAN is not required in the TSP on these nodes, as they are configured with the sub-ring instance (which contains the control VLAN). Note that if there is an intermediate node on the main ring between two interconnecting nodes, it is only participating in the major ring and has no sub-ring configuration. The TSP on the intermediate node interfaces must contain the sub-ring's control VLAN.
  - Sub-ring interfaces: The TSP on subtended ring interfaces contains the service and management VLANs for the subtended ring but not the control VLAN. R-APS messages for the major ring will not traverse the sub-ring, so do not add the major ring's control VLAN to the TSP on sub-ring nodes.
- RPL owner nodes:
  - Any node in the major ring may be the RPL owner.
  - Since the shared link is owned by the major ring instance, associated ring ports cannot be set as RPL owner for the sub-ring instance.
- Ethernet CFM (MEG/MEP) may be configured on any link in a major ring. Ethernet CFM may be configured on any link in a sub-ring except the interconnect link, as this MEG/MEP would be owned/configured on the major ring instance).
- If a node in a non-virtual sub-ring is accidentally configured with a major ring instance, one of the ports will show a “Failure of Protocol — Time-out (FOP-TO)” alarm, indicating a timeout due to misconfiguration.
- Confirm the major ring has enough bandwidth to carry the sub-ring traffic.

Configuring a G.8032 Sub-Ring off a Major Ring

This topic contains the steps involved in configuring a G.8032 sub-ring off a major ring.

Note: These steps assume that you have already configured a single major 10G G.8032v2 ring.

Configuration steps

Perform the following steps to configure a sub-ring on an E7-2 system.

1. Configure the sub-ring-non virtual or sub-ring-virtual on the sub-ring.

   Example:

```
E7-2(config)# g8032-ring 5
E7(config-g8032-ring-5)# ring-type
[major-ring,sub-ring-non-virtual,sub-ring-virtual] (major-ring):
sub-ring-virtual
E7(config-g8032-ring-5)# show f
g8032-ring 5
 ring-type sub-ring-virtual
!
```

2. Configure the control-vlan and admin-state.

   Example

```
E7-2(config-g8032-ring-2)# control-vlan 888
E7-2(config-g8032-ring-2)# admin-state enable
```

3. Configure the 'propagate-topology-change' option to propagate the topology change from the sub-ring to the major-ring.

   Example:

```
E7-2 (config-g8032-ring-1)# propagate-topology-change enable
E7-2 (config-g8032-ring-1)# show f
g8032-ring 1
 control-vlan              123
 propagate-topology-change enable
 wait-to-restore-time      1
 admin-state               enable
!
E7-2(config-g8032-ring-1)#
```

4. Configure the inter-connect mode when port binding the ring.

   Example:

```
E7-2# show running-config interface ethernet 1/2/x7
interface ethernet 1/2/x7
 no shutdown
 role                      inni
 transport-service-profile jl
 g8032-ring 1
 !
 g8032-ring 2
  rpl-mode inter-connect
 !
!
```

5. Configure the sub-ring port.

   Example:

```
E7-2# show running-config interface ethernet 1/2/x4
interface ethernet 1/2/x4
 no shutdown
 role inni
 transport-service-profile jl
 g8032-ring 2
 !
!
```

6. Use the "**show g8032-ring<id> configuration**" and "**show g8032-ring<id> status**" commands to view your changes.

   Example:

```
E7-2# show g8032-ring 2 configuration
configuration
 ring-instance-id          2
 admin-state               enable
 ring-type                 sub-ring-non-virtual   ---sub-ring type
 control-vlan              888
 maintenance-entity-level  1
 non-revertive             disable
 ring-id                   1
 propagate-topology-change enable
 monitor-fop-to            enable
 guard-time                500
 hold-off-time             0
 wait-to-block-time        5500
 wait-to-restore-time      5
```

```
 port-0-configuration
  shelf                          1
  slot                           2
  port-id                        x4
  rpl-mode                       none
  inter-connect-ring-instance-id none
  mep                            not-set
 port-1-configuration
  shelf                          1
  slot                           2
  port-id                        x7
  rpl-mode                       inter-connect   ---inter-connect
mode
  inter-connect-ring-instance-id 1
  mep                            not-set


E7-2# show g8032-ring 2 status
status
 ring-instance-id              2
 admin-state                   enable
 ring-type                     sub-ring-non-virtual   ---sub-ring
 configuration-state           resolved
 node-rpl-mode                 none
 protocol-state                state-a-idle
 protocol-version              2
 bridge-mac                    00:02:5d:bb:2d:54
 time-to-revert                n/a
 port-0-status
  shelf        1
  slot         2
  port-id      x4
  port-mac     00:02:5d:fd:d4:8f
  status       "port-up|rpl|blocked"
  fwd-state    blocking
  rpl-mode     none
  fop-to-alarm clear
 port-1-status
  shelf        1
  slot         2
  port-id      x7
  port-mac     00:02:5d:fd:d4:92
  status       port-up
  fwd-state    forwarding
  rpl-mode     inter-connect               ---inter-connect mode
  fop-to-alarm clear
```

```
configuration-unresolved-alarm clear
configuration-simplex-alarm    clear
isolated-node-alarm            clear
local-signal-fail-alarm        clear
local-manual-switch-alarm      clear
local-forced-switch-alarm      clear
remote-signal-fail-alarm       clear
remote-manual-switch-alarm     clear
remote-forced-switch-alarm     clear
fop-pm-alarm                   clear
```

Configuring INNI Links for Aggregation

This topic describes how to configure access-facing Layer-2 links for aggregation applications.

Assumptions

The following assumptions constitute the starting point for the provisioning process and examples in this topic:

- All required network equipment and devices are installed, powered on, and functioning properly.
- A network-facing Layer 2 interface (Layer 2 WAN uplink) is configured along with a transport service profile (TSP).

Provisioning process

The following high-level process steps begin after the assumptions listed above:

1. Ensure that all the VLANs being aggregated on the port are provisioned on the node.
2. Edit the transport service profile (TSP) to include all of VLANs being aggregated.
3. Apply the TSP to the aggregation port:
   a. Navigate to the desired Ethernet port
   b. Set the Ethernet port parameters as required, and with the following key setting:
      - role = inni
   c. Apply the TSP.

Example

```
config

!!Step 1.
vlan 101
top
!! create additional VLANs as needed

!!Step 2.
transport-service-profile TSP_L2-Aggregation
vlan-list 101
!! add additional VLANs as needed
top

!!Step 3.
!!Aggregation on one port (GE port example)
interface ethernet 1/2/g1
no shutdown
role inni
transport-service-profile TSP_L2-Aggregation
top
```

Configuring INNI Links for Aggregation with S+C+MAC Switching (E7-2)

This topic describes how to configure access-facing Layer-2 INNI links for aggregation applications with S+C+MAC switching.

This topics is organized as follows:

- Overview | Configuration guidelines | Configuration process

Overview

Using S+C+MAC switching on INNI links to subtended access shelves eliminates unnecessary broadcast flooding and allows the network to scale without traffic impacts.

Example application:

- 10GE-12 line cards subtending a stack of GPON8r2 cards

Configuration guidelines

- Supported AXOS systems: E7-2
- Supported port roles: INNI
- Supported VLAN modes: 1:1 and E-LINE
- Supported interfaces: Ring, LAG, and single-port configurations
- S+C+MAC switching is provisioned via a "Double Tag TSP" (DTTSP)

  Note: The term DTTSP refers to the following: On a given interface, a "transport-service" object with a "cvlan-list"

- A DTTSP is provisioned directly on an interface; it is not a reusable profile
- A DTTSP may coexist with a TSP
- The same S-Tag may be used with a DTTSP and TSP on a different interface

Provisioning process

Example

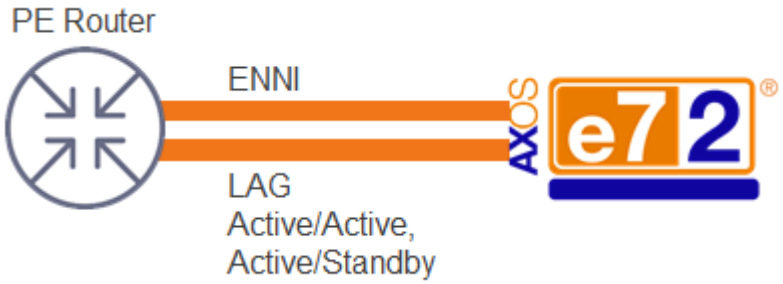
```
!!TSP for coexistence example
E7-2 (config)# transport-service-profile uplink
E7-2 (config-transport-service-profile-uplink)# vlan-list 100

!!Example INNI interface
E7-2 (config)# interface lag la3
E7-2 (config-lag-la3)# role inni
E7-2 (config-lag-la3)# transport-service-profile uplink !!coexisting
TSP
E7-2 (config-lag-la3)# transport-service 200 !!DTTSP part 1
E7-2 (config-transport-service-200)# cvlan-list 10-30 !!DTTSP part 2
```

Configuring ENNI Links

This topic describes how to configure access-facing Layer-2 ENNI links.

ENNI interfaces support tag actions to add, replace, or remove one or more VLAN tags. RSTP and LAG networking protocols are supported. ENNI interfaces are used primarily for connections at administrative boundaries where service VLANs are aligned/changed. ENNI interfaces will also be used for downlinked access devices, where tag action manipulations may be needed.

The following image shows an ENNI LAG downlink.



Configuration guidelines

- Assumptions:
  - All required network equipment and devices are installed, powered on, and functioning properly.
  - All required profiles are created.

Configuration process

For a given interface, follow the steps below:

1. Set the role to ENNI
2. Add a pre-configured Layer 2 service VLAN to the interface
3. Set the match-vlan value
4. (Optional) Set the remove-vlan option
5. (Optional) Set ingress metering
6. (Optional) Select an ingress pcp-map profile to modify incoming PCP values

CLI example

Example provisioning of an E-NNI interface (with remove-vlan)

```
no shutdown
role enni
vlan 302
match-vlan 30 remove-vlan

!!ingress tag actions: match on vlan 30, change tag to vlan 302
!!egress tag actions: change tag from vlan 302 to vlan 30
```

Example provisioning of an E-NNI interface (without remove-vlan)

```
no shutdown
role enni
vlan 303
match-vlan 30

!!ingress tag actions: match on vlan 30, add vlan 303 as the new
outer tag
!!egress tag actions: remove the outer vlan 303
```

Example provisioning of an E-NNI interface (with ingress metering and pcp-map)

```
no shutdown
role enni
vlan 302
match-vlan 30 remove-vlan
ingress pcp-map pcpmap1 !! pre-created pcp-map profile
ingress meter eir <value>
ingress meter ebs-bytes <value>
ingress meter ebs-nxmtu <value>
```

Configuring UNI Links

This topic describes how to configure access-facing Layer-2 UNI links for Ethernet business or residential services.

UNI links for Ethernet residential services

See the *Calix AXOS-R20.x Active Ethernet Services Guide*.

UNI links for Ethernet business services

Assumptions

The following assumptions constitute the starting point for the provisioning process and examples in this topic:

- All required network equipment and devices are installed, powered on, and functioning properly.
- A network-facing Layer 2 interface (Layer 2 WAN uplink) is configured along with a transport service profile (TSP)

Provisioning process

The following high-level process steps begin after the assumptions listed above:

1. Create a unique Layer 2 service VLAN for each subscriber with the following key settings:
   - l3-service = DISABLED (default)
   - mode = ELINE
   - mac-learning = ENABLED (default)
2. Edit the transport service profile (TSP) to add all of the new service VLANs.
3. Create an Ethernet class map with the following key settings:
   - One flow
   - Match rule to match untagged packets or any packet
4. Create an Ethernet policy map with the following key settings:
   - Reference to the class map created above
   - Add the relevant rate shaping information (Ingress Meter, Egress Shaper)
   - Optional: Class-map level tag actions
     - set-stag-pcp = 3

5. Add service to subscribers:

a. Navigate to the desired Ethernet port

b. Set the Ethernet port parameters as required, and with the following key setting:

- role = uni

c. Add the service VLAN

d. Under the service VLAN, add the policy map created above

e. Repeat Steps 5a to 5d for other subscribers, using a different service VLAN for each subscriber.

Example

```
config

vlan 101
mode ELINE
top
!! create additional VLANs as needed

transport-service-profile TSP_L2-Business
vlan-list 101
!! add additional VLANs as needed
top

class-map ethernet untag
flow 1
rule 1 match untagged !!or rule 1 match any
top

policy-map untag
class-map-ethernet untag
    egress shaper
      maximum 100000
    !
    ingress meter-mef
      cir 100000
    !
set-stag-pcp 3 !!optional
top
```

```
!!for one subscriber
interface ethernet 1/2/x1
no shutdown
role uni
vlan 101
policy-map untag
top

!!for another subscriber
interface ethernet 1/2/x2
no shutdown
role uni
vlan 102
policy-map untag
top
```

Chapter 5

Configuring Link Security via 802.1x

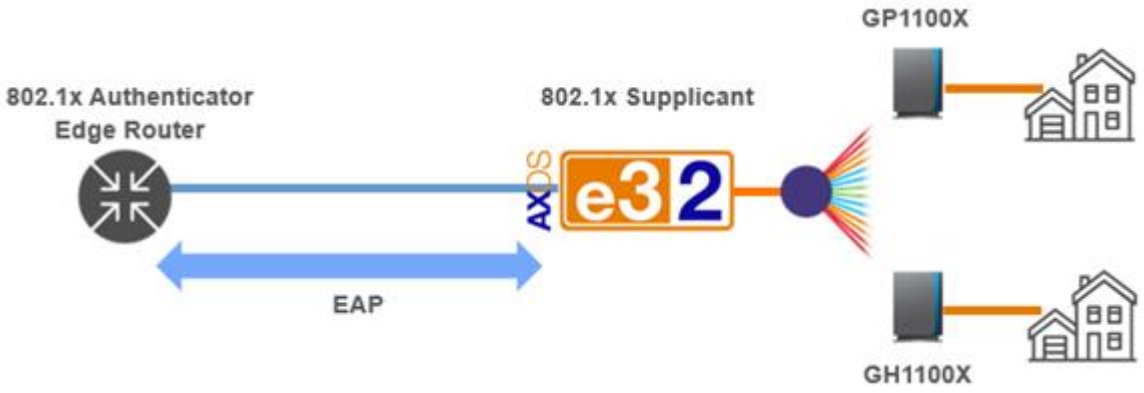
This chapter describes how to configure link security on the E3-2 with 802.1x Supplicant Support and is organized as follows:

- Overview
- Configuration Guidelines
- Configuration Process
- Parameters

Overview

IEEE 802.1x defines a port-based network access authentication mechanism for point-to-point devices on untrusted interfaces attempting to connect to a network. On an 802.1x enabled port, an untrusted device must be authenticated prior to accessing the network. 802.1x uses the Extensible Authentication Protocol (EAP) protocol that is based on encapsulating EAP packets within the data-link layer frame to provide access control mechanisms for devices interconnected by 802 LANs, known as EAP over LAN (EAPOL).

The 802.1x protocol can be used to authenticate E3-2 uplinks to provide a secure transmission of data between the E3-2 and the upstream edge router as shown in the diagram below.



802.1x authentication involves three roles:

- **Supplicant** - untrusted device that is requesting network access and is interfacing with an authenticator running EAPOL.
- **Authenticator** - a network device that provides a data link between the client and the network and can allow or block network traffic between the two. The authenticator is the upstream router that is peering on the data link with the supplicant on a given physical port. It relays EAP credentials between the supplicant and authenticating server.
- **Authentication Server** - receives and responds to requests for network access, validating the identity of the supplicant and informing the authenticator to either allow or deny access.

Configuration Guidelines

- The E3-2 acts as the supplicant and is connected to the upstream edge router via a 10GE interface (either a single 10GE interface or a LAG).
- The E3-2 uses MD5 for username and password authentication on each individual member of the LAG group, not the LAG interface itself.
- Considerations if Zero Touch Provisioning (ZTP) is used:

The E3-2 config file must include the username and password for the 802.1x supplicant.

The 802.1x authenticator (upstream edge router) is manually pre-provisioned for 802.1x supplicant support on the links connected to the E3-2; however, the authenticator function is disabled until after the E3-2 has successfully downloaded a config file.

The Upstream edge router pre-provisioning includes pre-authentication ACLs that allow DHCP and TFTP traffic to pass through before the port connected to the E3-2 is unauthorized.

- If 802.1x supplicant support is enabled and in an authenticated state, and the dot1x username or password is changed through in-band management, a reauthentication of the supplicant occurs. A 60 second delay timer is triggered when either the username or the password is changed. The reauthentication attempt begins when the delay timer expires.

Due to the pending reauthentication, be sure to change BOTH the username and password if needed WITHIN 60 seconds so that traffic on the link is not interrupted, and so that in-band management control is not lost (if configured on the link).

Related CLI commands (Oper mode):

- **`clear interface ethernet 1/1/x1 dot1x supplicant statistics`**
- **`show interface ethernet 1/1/x1 dot1x supplicant state`**
- **`show interface ethernet 1/1/x1 dot1x supplicant statistics`**

Configuration Process

Zero-Touch Provisioning (ZTP) option

802.1x supplicant support on the E3-2 can be incorporated into the Zero Touch Provisioning (ZTP) process as follows:

1. Disable the authenticator function in the upstream edge router until after the E3-2 has successfully downloaded the config file.
2. Boot up the E3-2 with the factory configuration that uses ZTP to get an IP address and download a config file that contains the username and password for the 802.1x supplicant.
3. Enable the authenticator function on the upstream edge router.
4. The E3-2 applies the config file and the authentication process with the edge router begins using the username and password contained in the config file.
5. The authentication server validates the identity of the E3-2, the authenticator sets the port to authenticated and allows all traffic to flow.

Manual Provisioning Option

802.1x supplicant support on the E3-2 can also be manually configured using the following CLI steps:

1. Enable the 802.1x supplicant on the interface.
2. Configure the username for EAP authentication.
3. Configure the password for EAP authentication.

Parameters

The parameters for manually provisioning 802.1x supplicant support are described below.

Parameter	Description
state	Enable or disable dot1x supplicant support on the up-link port. Valid values: • Enabled • Disabled Example: • E3-2# config interface ethernet-1/1/x1 dot1x supplicant state {enabled |disabled}
username	Configure the username for authentication. Valid values: • <string> Example: • E3-2# config interface ethernet-1/1/x1 dot1x supplicant username <string>
password •	Configure the password cipher string for authentication. Valid values: • <string> Example: • E3-2# config interface ethernet-1/1/x1 dot1x supplicant password <string> •

.

Chapter 6

Application Security

This chapter describes application security features that minimize exposure to denial-of-service attacks by suppressing unwanted or malicious traffic, including:

- Unicast reverse path forwarding
- L3 control plane policy
- Trap control plane policy

Configuring Unicast Reverse Path Forwarding (E9-2)

Unicast reverse path forwarding (uRPF) helps to reduce the effect of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. When you configure unicast RPF on an interface, it checks the unicast source address of each packet that arrives ingress on the interface. Packets that pass the check are forwarded. Packets that fail the check are dropped.

uRPF operates in two modes:

- In **strict mode**, uRPF checks each incoming packet against the routing table, and if the incoming interface is not the best reverse path, the packet is discarded.
- In **loose mode**, uRPF checks each incoming packet against the routing table, and the packet is dropped only if the source address is not reachable via any interface.

Configuration guidelines

- uRFP modes are supported on the aggregation card:
  - WAN interfaces (identified as g1–g2, q1–q2, x1–x8), applied at the interface level
  - Subscriber interfaces (identified as c1–c16), applied at the global level

  Note: Refer to *E9-2 port to CLI interface mapping* (on page 380) for more information on interface names.
- The uRPF feature is enabled globally by default; uRPF must be enabled globally before you can configure a uRPF mode on any interface (WAN or subscriber).
- uRFP is disabled by default on all interfaces until you configure a uRPF mode.
- Before disabling uRPF globally, first disable uRPF on all interfaces.
- A change to the global uRPF setting requires a system reload to take effect.

Parameters

You can configure the following parameters for uRPF globally:

Parameter	Description	Valid Options
ip-unicast-rpf	Globally enables or disables the uRPF feature, allowing you to configure uRPF on all interfaces.	enable (default) disable
subscriber	Globally configures strict or loose mode for all subscriber interfaces. **Note**: You cannot configure the uRPF mode on individual subscriber interfaces.	loose strict

You can configure the following parameter for uRPF on a WAN interface:

Parameter	Description	Valid Options
ip-unicast-rpf	Configures loose or strict mode RPF on the specified WAN interface.	loose strict

Procedures

To configure uRPF on a WAN interface

1. Verify that the uRPF feature is enabled globally.

```
Calix-1# show running-config ip-unicast-rpf | details
ip-unicast-rpf enable
```

2. Select a WAN interface. For example:

```
Calix-1(config)# interface ethernet 1/1/g1
```

3. Configure a uRPF mode on the interface.

```
Calix-1(config-ethernet-1/1/g1)# ip-unicast-rpf {loose|strict}
```

To configure uRPF on all subscriber interfaces

1. Verify that the uRPF feature is enabled globally.

```
Calix-1# show running-config ip-unicast-rpf | details
ip-unicast-rpf enable
```

2. Configure a uRPF mode on all subscriber interfaces.

```
Calix-1(config)# ip-unicast-rpf subscriber {loose|strict}
```

To change the global uRPF setting

1. Disable uRPF on all interfaces using the 'no' command, if needed. For example:

```
Calix-1(config)# no interface ethernet 1/1/g1 ip-unicast-rpf loose
Calix-1(config)# no ip-unicast-rpf subscriber loose
```

2. Disable or enable uRPF globally.

```
Calix-1(config)# ip-unicast-rpf {disable|enable}
```

3. Save the running configuration as the current startup configuration.

```
Calix-1# copy running-config startup-config
```

4. Reload the active aggregation card. For example:

```
Calix-1# reload 1/1
```

Control Plane Policies

A control plane policy (CoPP) provides a convenient way to prevent unwanted or malicious traffic from using CPU resources. You can apply a CoPP to packets that reach the CPU for processing by a Layer 3 (L3) forwarding decision or by a trap exception event, including:

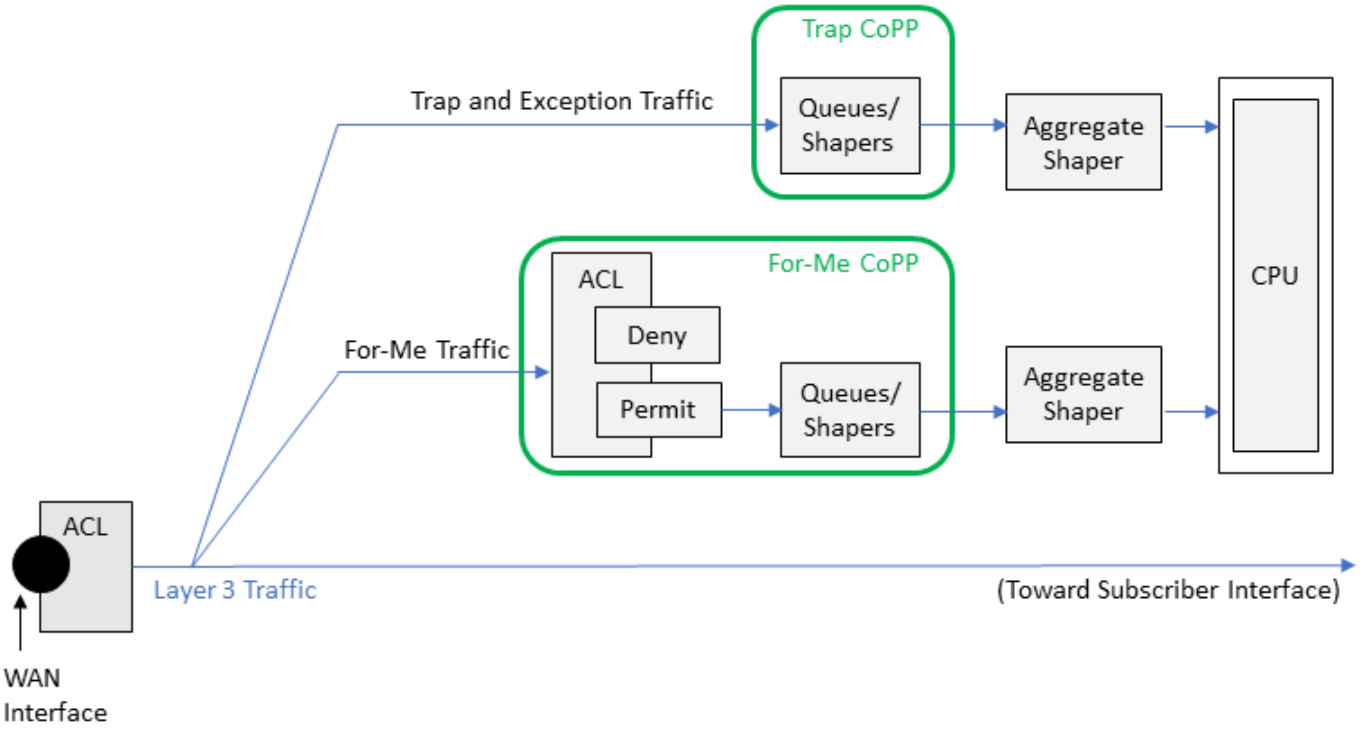
- For-Me traffic (or 'self destined'): L3 packets destined for a local IP address of the host CPU. For example, traffic destined to any of the following L3 interfaces:
  - Loopback interface IP address
  - VLAN interface IP address
  - WAN Ethernet port IP address
  - (E9-2) Multibind interface IP address
- Exception traffic: L3 packets routed to the host CPU, but not specifically addressed to a local IP address of the system. This traffic is the result of a default entry in the routing table for a subnet with the CPU port as a destination. This is typically traffic for which the system has a configured subnet, where the MAC address of the specified host is not yet known. Packets that would normally be routed may also be exceptioned to the local CPU for processing (for example packets TTL has expired). Exception traffic is directed to an internally managed queue that is limited to a fairly low rate, and intentionally separated from any other queue so that a flood of this type of traffic will not compete with other important functions in the device (such as the ability to manage it).
- Trap traffic: Packets of a specific type with well-defined attributes that are trapped to the host CPU to snoop, or otherwise pulled into the CPU for processing. Trap traffic includes: DHCPv4, DHCPv6, ARP, NDP, OSPF, IGMP, and any broadcast/multicast packets from L3 interfaces or L3 VLANs.

AXOS systems support a For-Me set of CoS queues (CoSQs) and a trap set of CoSQs for control plane traffic, each with a default CoSQ–to–CoS type mapping and default bandwidth policies. To modify these CoSQ sets, you can configure the following CoPPs:

- (E3-2/E9-2 CLX/E9-2 ASM only) **L3 For-Me CoPP**: Filters and modifies individual CoSQ mappings of For-Me traffic via an access control list (ACL), and manages bandwidth policies for permitted traffic via a CoSQ profile. The For-Me CoPP is configured at the system level.
- **Trap CoPP**: Manages bandwidth policies for trapped packets to the host CPU via a CoSQ profile. The Trap CoPP is configured at the card slot level; each slot can support the same set of defined CoSQs.

Note: On AXOS platforms that do not support L3 forwarding (for example, E7-2), all packets to the host CPU are supported by trap exception events.

This can be visualized in the diagram below, which depicts traffic in the downstream direction for an E9-2 CLX. For all other AXOS systems, there is a single aggregate shaper.



Configuring a L3 For-Me CoPP

This topic describes how to configure a *CoPP* (on page 117) at the system level that applies to L3 For-Me traffic only.

You can configure a For-Me CoPP policy to adjust one or more CoSQ entries to override system defaults. Using an ACL, this policy modifies CoSQ mappings and denies/permits incoming traffic and then queues and shapes the permitted traffic based on a CoSQ profile.

Guidelines

- When a CoSQ profile is applied on a For-Me CoPP with no ACL, the default CoSQ mapping is based on PCP only:
  - E3-2 and E9-2 ASM systems use an internal dedicated scheduler with 8 queues. Incoming For-Me packets are queued into one of the 8 queues based on the packet's PCP value (applying a CoSQ profile on a For-Me CoPP with no ACL has no effect).
  - E9-2 CLX systems use 8 of the 48 CoSQs (1, 7, 13, 19, 25, 31, 37, and 43) by scaling the packets PCP value into the respective CoSQ using an algorithm (PCP * 6+1). These CoSQs are reserved for system use and must have appropriate bandwidth settings.
- For E3-2/E9-2 ASM with no CoPP ACL and for E9-2 CLX3001, For-Me traffic may be filtered by ACLs on individual L3 interfaces.
- For transit traffic (not destined for the CPU), you can continue to configure ACLs on L3 interfaces as appropriate.
- E7-2 does not support the For-Me CoPP; all packets to the host CPU are supported by trap exception events.
- Trap traffic (snooped DHCPv4/v6, ARPs, etc.) is not affected by the For-Me CoPP.

Provisioning process

Perform the following high-level steps to configure a L3 For-Me CoPP:

Step 1 *Create a CoSQ Profile* (on page 131) for up to 48 CoSQs with the desired bandwidth attributes for each CoSQ.

Example:

```
cos cosq-profile COSQ-CONTROL_PLANE
 cosq-entry 1
  bandwidth maximum 128
  queue-depth    20000
  discard-policy TAIL-DROP
  .
  .
  .
 cosq-entry 43
  bandwidth maximum 10000
  queue-depth    20000
  discard-policy TAIL-DROP
 !
!
```

Step 2 (Optional) *Create a CoPP ACL* (on page 135) to specify deny and permit matches, as well as CoSQs (defined in the CoSQ profile) for permitted traffic.

Example:

```
access-list ipv4 COPPv4
 description "Control Plane Filter IPv4"
 rule 10 description LIMIT-10M-DST-DHCP
 rule 10 match protocol UDP source-port-range 68 destination-port-
range 67-68
 rule 10 action permit cpu-cosq 28 count
 .
 .
 .
 rule 255 description DENY-ALL
 rule 255 match any
 rule 255 action deny count
!
```

Step 3 (E9-2 CLX only: Optional) *Create a DSCP Map* (on page 282) to define DSCP to PCP mappings set on the E9-2 control plane traffic.

Example:

```
dscp-map CoPP dscp CS6 7
```

Note: See *Creating a DSCP Map* (on page 282) for information on how a DSCP map interacts with the *host application QoS* (on page 78) functionality.

Step 4 Configure the CoPP by applying the ACL, CoSQ profile, and DSCP map (if created) to the control plane.

Example:

```
control-plane access-group ipv4-acl COPPv4
control-plane cosq COSQ-CONTROL_PLANE
control-plane dscp-map COPP
```

CoSQ ID to CoS type mapping

CoS queues map to the following CoS types (defined by 802.1Q standard).

Note: Do not configure reserved CoS queues.

CoS Queues	CoS Type	Traffic Type	Description
1*, 2, 3, 4, 5, 6	BK	Background Traffic (lowest)	Bulk transfers and other activities permitted on the network which should not impact the use of the network by other users and applications.
7*, 8, 9, 11, 10, 12	BE	Best Effort	Default use by unprioritized applications.
13*, 14, 15, 17, 18	EE	Excellent Effort	Best-effort type services delivery for important customers.
16, 19*, 20, 21, 23, 24	CA	Critical Application	Characterized by having a guaranteed minimum bandwidth as the primary QoS requirement, and subject to some form of admission control (for example, bandwidth reservation per flow) to ensure that one system or application does not consume bandwidth at the expense of others.
25*, 26, 27, 29, 30	VI	Video	Characterized by less than 100 ms delay, or other applications with low latency as the primary QoS requirement.
31*, 32, 33, 35, 36	VO	Voice	Characterized by less than 10 ms delay for maximum jitter (one way transmission through the LAN infrastructure of a single campus).
37*, 38, 40, 41, 42	IC	Internetwork Control	In large networks comprising separate administrative domains, there is typically a requirement to distinguish traffic supporting the network as a concatenation of those domains from the Network Control of the immediate domain.
43#, 44, 45, 46, 47, 48	NC	Network Control	Characterized by a guaranteed delivery requirement to support configuration or maintenance of the network infrastructure (for example, LACP).

* These CoSQs have a higher BW and queue depth by default and are reserved for system use when no ACL is applied to the CoPP.

Note: CoSQs not listed in the table above (22, 28, 34, 39) are reserved for Calix internal use.

E9-2 CLX: CoSQ Defaults

Note: To display the CoSQ default values for any AXOS platform, issue the **`show control-plane qos cosq`** CLI command with no CoSQ profile configured against the For-Me CoPP.

CoSQ	Minimum Bandwidth	Maximum Bandwidth	Queue Depth
1	2000	20000	199872
2	500	500	99840
3	500	500	99840
4	500	500	99840
5	500	500	99840
6	500	500	99840
7	2000	20000	199872
8	500	500	99840
9	500	500	99840
10	500	500	99840
11	500	500	99840
12	500	500	99840
13	2000	20000	199872
14	500	500	99840
15	500	500	99840
16	500	500	99840
17	500	500	99840
18	500	500	99840
19	2000	20000	199872
20	500	500	99840
21	500	500	99840
22	500	500	99840
23	500	500	99840
24	500	500	99840
25	2000	20000	199872
26	500	500	99840
27	500	500	99840
28	500	500	99840
29	500	500	99840
30	500	500	99840
31	2000	20000	199872
32	500	500	99840
33	500	500	99840
34	500	500	99840
35	500	500	99840

CoSQ	Minimum Bandwidth	Maximum Bandwidth	Queue Depth
36	500	500	99840
37	2000	20000	199872
38	500	500	99840
39	500	500	99840
40	500	500	99840
41	500	500	99840
42	500	500	99840
43	2000	20000	199872
44	500	500	99840
45	500	500	99840
46	500	500	99840
47	500	500	99840
48	500	500	99840

E9-2 ASM: CoSQ Defaults

CoSQ	Minimum Bandwidth	Maximum Bandwidth	Queue Depth
1 . . . 48	0	4294967295	unlimited

E3-2: CoSQ Defaults

CoSQ	Minimum Bandwidth	Maximum Bandwidth	Queue Depth
1 . . . 64	0	4294967295	unlimited

.

Configuring a Trap CoPP

This topic describes how to configure a *CoPP* (on page 117) at the card slot level that applies to trap traffic.

AXOS cards have internal default CoSQ profiles configured on all trap CoSQs. You can configure a Trap CoPP on a card slot to override default bandwidth policy settings of one or more CoSQ entries (via a CoSQ profile) for packets that are trapped on a given card; default CoSQ–to–CoSQ type mappings cannot be overridden. For example, the configured services in conjunction with the scale of a given card may require that you modify bandwidth and queue depths for a trap CoSQ to accommodate increased packet trap rates.

Guidelines

- You can configure a trap CoPP to override a specific CoSQ entry; overriding all default CoSQ entries is not required.
- Each card can support the same set of defined CoSQs.
- CoSQs in use depend on the functionality supported by the given card; traps that support L3 interfaces/features are predominantly on the CLX3001 card and traps that support L2 features are predominantly on access cards.
- The assigned internal default CoSQ profile differs by card.

Active mappings for trap classifiers are based on the platform and configured services, and only these packets are trapped (i.e., trap classifiers are only active when the protocol is turned on). For example, the L2 Discovery trap is installed when ICL links are configured to support VLAN stitching between aggregation and line cards. Use the **`show control-plane-trap <shelf/slot> cosq-active`** CLI command to display active mappings.

Provisioning process

Perform the following high-level steps to configure a Trap CoPP:

Step 1 Create a CoSQ Profile for up to 48 CoSQs with the desired bandwidth attributes for each CoSQ.

Example:

```
cos cosq-profile COSQ-TRAP-1
 cosq-group-scheduling-type WRR
 cosq-entry 1
  bandwidth maximum 504
  bandwidth minimum 504
  weight         1
  queue-depth    100048
  discard-policy TAIL-DROP
  !
!
```

Step 2 To configure the trap CoPP, apply the CoSQ profile to the control plane on a card slot.

Example:

```
slot 1/1 control-plane-trap cosq COSQ-TRAP-1
```

Protocol to CoSQ mapping (non-configurable)

To view a systems current protocol to CoSQ mapping use the **`show control-plane-trap <shelf/slot> cosq-mapping`** CLI command. Mappings will change as new protocols/functionality are added.

CoSQ ID	Protocol	Definition
6	MONITOR[1]	Active during tcpdump
7	PROXY_ARP	Installed when MFF enabled on VLAN
7	POLICY_GROUP_RULE[2]	
8	PROXY_ICMPv6	Installed when DHCPv6 enabled on VLAN
9	RELAY_DHCPv6	Installed when DHCPv6 enabled on VLAN
10	RELAY_DHCPv4	Installed when DHCP enabled on VLAN
14	ARP	Installed to support IP interfaces
16	PPPOE	Installed when PPPoE enabled on VLAN
17	IPV4_XCAST (unicast, broadcast, multicast)	Installed when IPv4 interfaces created
18	IPV6_XCAST (unicast, broadcast, multicast)	Installed when IPv6 interfaces created
19	802.1X	Installed when 802.1X (dot1x) enabled on interface

CoSQ ID	Protocol	Definition
21	DHCP	Installed to support BNG services
22	ICMPV4	Not currently installed
23	NDP	Not currently installed
23	ICMPV6	Installed to support BNG services
24	SOAM	Installed when Service OAM configured
25	VCA[1]	Installed when Video Channel Analyzer is running
28	PROXY_IGMP	Installed when IGMP enabled on VLAN
29	IGMP, PIM	Installed when IGMP, PIM enabled on IP interface
33	IPV4_IBMGNT	Installed when VLAN interface created or Host interface (L3-Service disabled on VLAN)
34	IPV4-RIF	Not currently installed
35	IPV6_IBMGNT	Installed when VLAN interface created or Host interface (L3-Service disabled on VLAN)
36	IPV6_RIF	Not currently active
37	LLDP	Installed when LLDP is configured
38	LOAM	Installed when LOAM (802.3ah) is configured
39	SYNCE	Installed when SYNC-E is configured
39	LACP	Installed when LACP is configured on a LAG
39	VRRP	Installed when VRRP is configured
40	PTP	Installed when PTP is configured
41	L2_DISCOVERY	Installed to support VLAN stitching between aggregation and line cards
42	ICL_APS	Installed when Ethernet role is ICL
43	EAPS	Installed when G.8032 is configured
43	ERPS	Installed when ERPS is configured
43	RSTP	Installed when RSTP is configured
44	ISIS	Installed when ISIS is configured
44	LDP	Installed when LDP is configured
45	OSPF	Installed when OSPF is configured
45	RIP	Installed when RIP is configured
45	BGP	Currently not installed even if BGP enabled
46	MPLS	Installed when MPLS is configured

[1] E9-2 CLX card only

[2] ASM and access cards only

E9-2 CLX: Trap CoSQ Defaults

Note: To display the trap CoSQ default values for any AXOS card, issue the **`show control-plane-trap <shelf/slot> qos cosq`** CLI command.

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
1	64	64	1040
2	64	64	1040
3	64	64	1040
4	64	64	1040
5	64	64	1040
6	5000	5000	100048
7	64	64	1040
8	64	64	1040
9	104	104	10192
10	104	104	10192
11	64	64	1040
12	64	64	100048
13	64	64	1040
14	504	504	5200
15	64	64	1040
16	64	64	1040
17	256	256	10192
18	256	256	10192
19	64	64	1040
20	64	64	1040
21	752	752	100048
22	504	504	10192
23	504	504	10192
24	1000	1000	50128
25	20000	20000	50128
26	64	64	1040
27	64	64	1040
28	64	64	1040
29	1000	1000	10192
30	256	256	5200
31	64	64	1040
32	64	64	1040
33	20000	20000	20176
34	64	64	1040
35	20000	20000	20176
36	64	64	1040
37	504	504	50128

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
38	104	104	2704
39	256	256	5200
40	104	104	2704
41	10000	10000	400192
42	504	504	10192
43	504	504	10192
44	1000	1000	250016
45	504	504	50128
46	504	504	50128
47	10000	10000	100048
48	504	504	100048

NG1601/GP1611/GP1612: Trap CoSQ Defaults

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
1	468	468	512
2	468	468	512
3	468	468	512
4	468	468	512
5	468	468	512
6	5148	5148	100000
7	468	468	10000
8	468	468	20000
9	936	936	75000
10	936	936	75000
11	468	468	512
12	468	468	512
13	468	468	512
14	468	468	1000
15	468	468	512
16	936	936	100000
17	468	468	5000
18	468	468	5000
19	468	468	512
20	468	468	512
21	468	468	512
22	468	468	512
23	468	468	512
24	936	936	50000
25	468	468	512
26	468	468	512

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
27	468	468	512
28	936	936	10000
29	468	468	512
30	468	468	5000
31	468	468	512
32	468	468	512
33	20124	20124	20000
34	468	468	512
35	20124	20124	20000
36	468	468	512
37	468	468	50000
38	468	468	512
39	468	468	5000
40	468	468	1000
41	10296	10296	400000
42	468	468	10000
43	468	468	512
44	468	468	512
45	468	468	512
46	468	468	512
47	468	468	512
48	468	468	512

E3-2: Trap CoSQ Defaults

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
1	325	325	512
2	325	325	512
3	325	325	512
4	325	325	512
5	325	325	512
6	4875	4875	100000
7	325	325	5000
8	325	325	10000
9	650	650	75000
10	650	650	75000
11	325	325	512
12	325	325	512
13	325	325	512
14	325	325	1000
15	325	325	512

.

CoSQ	Minimum Bandwidth in Kbps	Maximum Bandwidth in Kbps	Queue Depth in bytes
16	975	975	100000
17	325	325	5000
18	325	325	5000
19	325	325	512
20	325	325	512
21	325	325	10000
22	325	325	5000
23	325	325	5000
24	325	325	10000
25	19825	19825	50000
26	325	325	512
27	325	325	512
28	650	650	5000
29	325	325	512
30	325	325	5000
31	325	325	512
32	325	325	512
33	19825	19825	20000
34	325	325	512
35	19825	19825	20000
36	325	325	512
37	325	325	20000
38	325	325	2500
39	325	325	5000
40	325	325	1000
41	325	325	512
42	325	325	512
43	650	650	10000
44	325	325	512
45	325	325	512
46	325	325	512
47	325	325	512
48	325	325	512

Creating a CoPP CoSQ Profile

This topic describes how to create a CoSQ profile to apply to a For-Me CoPP or a Trap CoPP.

AXOS systems support a For-Me set of CoS queues (CoSQs) and a trap set of CoSQs, each with default bandwidth policies. You can configure a CoSQ profile to override the default bandwidth and queue depth for one or more CoSQ entries.

Guidelines

- A For-Me CoPP supports a maximum of 48 CoSQs.
- A Trap CoPP supports a maximum of 48 CoSQs.

  Note: Although 64 CoSQ entries are allowed on the E3-2, the Trap CoPP and ACL cpu-cosq action only support up to 48 CoSQ entries and applying a CoSQ profile on a For-Me CoPP with no ACL has no effect for the E3-2.

- For E9-2 CLX cards, the For-Me CoPP supports cosq-group-scheduling-types SP and WRR only on the CoSQ profile.
- For E3-2 and E9-2 ASM cards, For-Me packets are steered to 1–48 schedulers based on the cpu-cosq value specified in the ACL rule, where each scheduler has 8 queues.
- For a Trap CoPP, only cosq-group-scheduling-type WRR with a fixed weight of 1 is supported on the CoSQ profile; other scheduling types are rejected when attaching the CoSQ profile to the CoPP.
- For any CoSQ entry that is not configured via a CoSQ profile, the value defaults to the system or card default.
- Use the following CLI commands to display default settings for each CoSQ:
  - For-Me CoSQs: **`show control-plane qos cosq`**
  - Trap CoSQs: **`show control-plane-trap <shelf/slot> qos cosq`** (defaults vary by card)

Parameters

You can provision the following parameters for a CoPP CoSQ profile:

Parameter	Description	Valid Options
cosq-profile*	A unique name for the CoSQ profile. Note: Do not use the 'DEFAULT' CoSQ profile; this is intended for Ethernet interfaces.	This is a string of up to 48 characters, including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot).
cosq-group-scheduling-type	Supported traffic class scheduling modes: • **SP**: A hierarchical mechanism that first services the highest queue (up to a max), then the next queue. • **WRR**: Allows all queues to be scheduled dependent on weights up to the max, where the weight is a fair-share percentage over lower weighted and available CPU bandwidth at that time.	SP (default) WRR
cosq-entry	A CoS queue for forwarding traffic. For SP, higher CoS queue numbers have higher priority. For information on reserved queues, see *Configuring a L3 For-Me CoPP* (on page 119) and *Configuring a Trap CoPP* (on page 124). **Note**: On the For-Me CoPP, this value maps to the 'cpu-cosq' action specified in the ACL.	1–48 Note: Although 64 CoS queue entries are allowed on some platforms, only 48 entries are supported in the ACL 'cpu-cosq' action and by the Trap CoPP.
bandwidth maximum	The maximum bandwidth rate in Kbps for the given CoS queue, rounded up to the nearest rate based on the granularity supported by the given AXOS system. The maximum bandwidth must be greater or equal to the minimum bandwidth.	0–10000000 0 (default)
bandwidth minimum	The minimum bandwidth rate in Kbps for the given CoS queue, rounded up to the nearest rate based on the granularity supported by the given AXOS system.	0–10000000 0 (default)
discard-policy	The discard policy for congestion avoidance: **WRED** (Weighted Random Early Detection): Drops lower priority traffic before higher priority traffic if the configured queue depth is exceeded. Starts dropping packets at 75% of the queue depth, and 100% of the packets are dropped. **TAIL-DROP**: Drops traffic when a queue is full. This allows for effective use of the full available queue depth, but may result in abrupt dropping of traffic. Tail-drop treats all traffic equally and does not differentiate between traffic classes.	WRED (default) TAIL-DROP (see Guidelines above)
queue-depth	Maximum queue buffering memory (in bytes) of the CoS queues. Queue buffering memory is a limited resource, shared across all queues in the AXOS system.	0 (default) 64–128000 0 = unlimited
weight	Scheduling weight, applicable only to WRR configurations only.	1–100 1 (default)

Procedure

To provision a CoSQ profile

1. Enter a unique CoSQ policy name.

```
Calix-1(config)# cos cosq-profile <profile name>
```

2. Specify a scheduling policy for servicing the CoSQs.

```
Calix-1(config-cosq-profile-profile name)# cosq-group-scheduling-
type <scheduling-policy>
```

3. Enter a CoSQ.

```
Calix-1(config-cosq-profile-profile name)# cosq-entry <1-64>
```

4. Configure the maximum and minimum bandwidth for the CoSQ entry.

```
Calix-1(config-cosq-entry-number)# bandwidth maximum <0-10000000>
minimum <0-10000000>
```

5. Reference the table above to configure additional CoS queue parameters, as needed.
6. Repeat steps 3–5 to configure additional CoSQs.

Example

```
cos cosq-profile COSQ-CONTROL_PLANE
 cosq-entry 1
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 2
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 3
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 4
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 5
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
```

```
 cosq-entry 6
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 7
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 8
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 9
  bandwidth maximum 1000
  queue-depth    50000
  discard-policy TAIL-DROP
!
 cosq-entry 11
  bandwidth maximum 1000
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 12
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 14
  bandwidth maximum 128
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 18
  bandwidth maximum 5000
  queue-depth    50000
  discard-policy TAIL-DROP
 !
 cosq-entry 27
  bandwidth maximum 10000
  queue-depth    50000
  discard-policy TAIL-DROP
 !
```

```
cosq-entry 29
 bandwidth maximum 256
 queue-depth    50000
 discard-policy TAIL-DROP
!
cosq-entry 30
 bandwidth maximum 1920
 queue-depth    50000
 discard-policy TAIL-DROP
!
cosq-entry 43
 bandwidth maximum 1920
 queue-depth    50000
 discard-policy TAIL-DROP
!
```

Creating a CoPP ACL

This topic describes how to create a CoPP ACL that applies to L3 For-Me traffic only to:

- Deny/permit packet patches.
- Specify CoSQs for permitted traffic.

This type of ACL is bound to a CoSQ profile via a control plane access group.

Guidelines

- Do not reference a CoSQ that is not supported by the given AXOS system.
- For matching packets, the ACL denies or permits.
- For permitted traffic, the ACL specifies a CoSQ.
- The 'cpu-cosq' action in the ACL:
  - Maps to a 'cosq-entry' parameter specified in the CoSQ profile.
  - Identifies the CoSQ that traffic matching a given rule is steered to when the ACL is applied to a control plane access group.
- Multiple flows can be mapped to a queue and will equally share the policy applied to that queue.
- (E3-2/E9-2 ASM only) Once a For-Me CoPP is configured, the actions of its ACL on For-Me traffic takes precedence over all other ACLs.
- Trap traffic (snooped DHCPv4/v6, ARPs, etc.) is not affected by the CoPP ACL.

- If a packet does not match any rule, it will be denied (or dropped). An implicit, non-configured drop rule is used for this, identified by sequence number 65535 when viewing statistics. For example:

```
SEQ       HIT
NUM       ACTIONS   COUNTER
------------------------
65535     d/c/-     95615821
```

- AXOS does not support IPv6 ACLs with prefixes greater than /64 (e.g., /128).

Parameters

You can configure the following parameters for a CoPP ACL:

Parameter	Description	Valid Options
access-list	Specifies the type of ACL.	ipv4 ipv6
name	A unique name for the ACL.	A string up to 48 characters including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot)
description	A description of the access list.	A string of up to 48 characters
rule	Sets a sequence number for the rule, and adds the rule to the ACL. **Note**: ACL rules are evaluated in the order entered into the system.	1–1024
rule <n> description	A description of what this rule is for.	A string of up to 48 characters
action	One or more actions to perform when the traffic flow matches the associated rule. Valid values: • count: Enables counting for packets that hit this rule • cpu-cosq <1–48>: Identifies the CoS queue that permitted traffic is mapped to **Note**: This value maps to the 'cosq-entry' parameter specified in theofile. • deny: Drop matching packets • permit: Pass matching packets Deny and permit are mutually exclusive. For permitted traffic, specify both a permit and cpu-cosq action For information on default CoSQ mappings, see *Configuring a L3 For-Me CoPP* (on page 119) and *Configuring a Trap CoPP* (on page 124).	count cpu-cosq <1–48> deny permit

Parameter	Description	Valid Options
match <keyword>	Per rule number match criteria	
any	Matches all packets.	N/A
destination-ipv4-network *OR* destination-ipv6-network	Matches a destination IP address and prefix. Note: A destination address that is not one of the host's IP addresses is accepted, however the rule does not function.	Syntax: <ip address/prefix> IPv4 prefix: 0–32 IPv6 prefix: 0–128
destination-ipv4-prefix list *OR* destination-ipv6-prefix-list	Matches an *IP prefix list* (on page 274) receiving the packet.	Name of any previously configured IPv4/IPv6 prefix list
destination-port-range	Specifies the destination TCP/UDP port(s) to match as a range or as a single value. Service names and port numbers distinguish different services that run over transport protocols, such as TCP and UDP.	1–65535 Press the tab key twice to display well-known IP protocol transport port enumerations and values.
icmp-type	Specifies the Internet Control Message Protocol (ICMP) type number to match.	0–255 Press the tab key twice to display well-known ICMP type code enumerations and values.
protocol	Specifies the Internet protocol enumeration or number in an IPv4 packet header to match. **Note:** For IPv6, you must include an IPv6 network address. For example, for any IP protocol and any IPv6 address, "protocol ANY destination-ip-network ::/0".	0–255 Press the tab key twice to display well-known IP protocol transport port enumerations and values.
source-ipv4-network *OR* source-ipv6-network	Matches the source IP address and prefix.	Syntax: <ip address/prefix> IPv4 prefix: 0–32 IPv6 prefix: 0–128
source-ipv4-prefix-list *OR* source-ipv6-prefix-list	Matches an *IP prefix list* (on page 274) sending the packet.	Name of any previously configured IPv4/IPv6 prefix list
source-port-range	Specifies the lower/upper boundary of the source TCP/UDP ports to match as a range or as a single value.	1–65535 Press the tab key twice to display well-known IP protocol transport port enumerations and values.
tos	Type of service.	8-bit value expressed in decimal (0–255) or hex (0x00–0xff)
tracking-state	The connection tracking state, either: • ESTABLISHED: connection established • INVALID: invalid state • NEW: new connection • RELATED: connection related to existing connection	ESTABLISHED INVALID NEW RELATED

Procedure

To create a CoPP access list

1. Specify the ACL type and a name.

```
Calix-1 (config)# access-list {ipv4|ipv6} name
```

2. (Optional) Enter a brief description for the ACL.

```
Calix-1 (config-ipv4-name)# description <string>
```

3. Specify a sequence number and optional description for the rule.

```
Calix-1 (config-ipv4-name)# rule 1 description <string>
```

4. Specify match criteria for the rule.

```
Calix-1 (config-ipv4-name)# rule 1 match <match criteria>
```

5. Specify the action to perform.

```
Calix-1 (config-ipv4-name)# rule 1 action {count|cpu-
cosq|deny|permit}
```

Examples

```
!
access-list ipv4 CP_FILTER-IPv4
 description "Control Plane Filter IPv4"
 rule 10 description LIMIT-10M-DST-DHCP
 rule 10 match protocol UDP source-port-range 68 destination-port-
range 67-68
 rule 10 action permit cpu-cosq 9 count
 !
 rule 20 description LIMIT-1M-SRCDST-ICMP
 rule 20 match protocol ICMP
 rule 20 action permit cpu-cosq 11  count
 !
!
 rule 255 description DENY-ALL
 rule 255 match any
 rule 255 action deny count
!
access-list ipv4 COPPv4
 description "Control Plane Filter IPv4"
 rule 10 description LIMIT-10M-DST-DHCP
 rule 10 match protocol UDP source-port-range 68 destination-port-
range 67-68
 rule 10 action permit cpu-cosq 28 count
 rule 20 description LIMIT-1M-SRCDST-ICMP
 rule 20 match protocol ICMP
 rule 20 action permit cpu-cosq 2 count
 rule 30 description LIMIT-1M-DST-TRACEROUTE
 rule 30 match protocol UDP destination-port-range 33434-33523
 rule 30 action permit cpu-cosq 3 count
```

```
 rule 40 description LIMIT-SRC-DIAMETER
 rule 40 match source-ipv4-prefix-list DIAMETER_SOURCE protocol TCP
destination-port-range 3868
 rule 40 action permit cpu-cosq 48 count
 rule 41 match source-ipv4-prefix-list DIAMETER_SOURCE protocol TCP
destination-port-range 9999
 rule 41 action permit cpu-cosq 37 count
 rule 60 description "ALLOW-SRC-SSH"
 rule 60 match source-ipv4-prefix-list PTY_ACCESS_NETWORKS protocol
TCP destination-port-range SSH
 rule 60 action permit cpu-cosq 34 count
 rule 70 description ALLOW-SRC-NETCONF
 rule 70 match source-ipv4-prefix-list NETCONF protocol TCP
destination-port-range 830
 rule 70 action permit cpu-cosq 36 count
 rule 80 description ALLOW-SRC-TACACS
 rule 80 action permit cpu-cosq 32 count
 rule 100 description LIMIT-1M-SRC-NTP
 rule 100 match source-ipv4-prefix-list NTP_SOURCES source-port-
range 123
 rule 100 action permit cpu-cosq 35 count
 rule 130 description LIMIT-1M-SRC-RADIUS
 rule 130 match source-ipv4-prefix-list RADIUS_SERVERS protocol UDP
source-port-range 1646
 rule 130 action permit cpu-cosq 31 count
 rule 131 description LIMIT-1M-SRC-RADIUS
 rule 131 match source-ipv4-prefix-list RADIUS_SERVERS protocol UDP
source-port-range 1813
 rule 131 action permit cpu-cosq 31 count
 rule 140 description "LIMIT-1M-SRC-DOMAIN TCP"
 rule 140 action permit cpu-cosq 7 count
 rule 141 description "LIMIT-1M-SRC-DOMAIN UDP"
 rule 141 action permit cpu-cosq 7 count
 rule 190 description ALLOW-SRC-TELNET
 rule 190 action permit cpu-cosq 33 count
 rule 250 match destination-ipv4-prefix-list LOCAL_INTERFACES
destination-port-range 31107
 rule 250 action deny count
 rule 255 description DENY-ALL
 rule 255 match any
 rule 255 action deny count
!
```

Related topic

- *Creating an IPv4 Prefix List* (on page 274)

Viewing the CoPP Configuration

Note: E3-2 and E9-2 ASM systems do not support counter statistics for CoSQs.

Use the following commands to display CoPP information:

- **show control-plane**
- **show control-plane access-group**
- **show control-plane qos**
- **show control-plane-trap <shelf/slot>**
- **show control-plane-trap <shelf/slot> qos**
- **show control-plane-trap <shelf/slot> cosq-active** (shows only active mappings for trap classifiers based on configured services)
- **show control-plane-trap <shelf/slot> cosq-mapping** (shows all possible mappings for each trap classifier to a CoSQ, if all services were turned up)

For more information, see the *AXOS CLI Reference: Operational Mode*.

Examples

```
Calix-1# show control-plane-trap 1/1 cosq-mapping
cosq-mapping
 cosq 6
  trap-type [ MONITOR ]
 cosq 7
  trap-type [ PROXY_ARP ]
 cosq 8
  trap-type [ PROXY_ICMPV6 ]
 cosq 9
  trap-type [ RELAY_DHCPV6 ]
 cosq 10
  trap-type [ RELAY_DHCPV4 ]
 cosq 14
  trap-type [ ARP ]
 cosq 16
  trap-type [ PPPOE ]
 cosq 17
  trap-type [ IPV4_XCAST ]
 cosq 18
  trap-type [ IPV6_XCAST ]
 cosq 19
  trap-type [ 8021X ]
 cosq 21
  trap-type [ DHCP ]
 cosq 22
  trap-type [ ICMPV4 ]
 cosq 23
```

```
 trap-type [ ICMPV6 MPLS_PING NDP ]
cosq 24
 trap-type [ SOAM ]
cosq 25
 trap-type [ VCA ]
cosq 28
 trap-type [ PROXY_IGMP ]
cosq 29
 trap-type [ IGMP PIM ]
cosq 30
 trap-type [ PROTOTYPE ]
cosq 33
 trap-type [ IPV4_IBMGNT ]
cosq 34
 trap-type [ IPV4-RIF ]
cosq 35
 trap-type [ IPV6_IBMGNT ]
cosq 36
 trap-type [ IPV6_RIF ]
cosq 37
 trap-type [ LLDP ]
cosq 38
 trap-type [ LOAM ]
cosq 39
 trap-type [ LACP SYNCE VRRP ]
cosq 40
 trap-type [ PTP ]
cosq 41
 trap-type [ L2_DISCOVERY ]
cosq 42
 trap-type [ ICL_APS ]
cosq 43
 trap-type [ EAPS ERPS RSTP ]
cosq 44
 trap-type [ ISIS LDP ]
cosq 45
 trap-type [ BGP OSPF RIP ]
cosq 46
 trap-type [ MPLS ]
```

```
Calix-1# show control-plane
control-plane
 qos
  cosq-profile COSQ-CONTROL_PLANE
       S
COSQ   VLAN            SCHEDULING  MINIMUM    MAXIMUM    QUEUE
DISCARD
ENTRY  PCP   EXP  TOS  TYPE        BANDWIDTH  BANDWIDTH  DEPTH
WEIGHT  POLICY
-------------------------------------------------------------------
---------------
1      -     -    -    SP          0          128        1920    0
TAILDROP
2      -     -    -    SP          0          128        1920    0
TAILDROP
3      -     -    -    SP          0          128        1920    0
TAILDROP
4      -     -    -    SP          0          128        1920    0
TAILDROP
5      -     -    -    SP          0          128        1920    0
TAILDROP
6      -     -    -    SP          0          128        1920    0
TAILDROP
7      -     -    -    SP          0          128        1920    0
TAILDROP
8      -     -    -    SP          0          128        1920    0
TAILDROP
9      -     -    -    SP          0          1024       1920    0
TAILDROP
10     -     -    -    SP          0          1024       1920    0
TAILDROP
11     -     -    -    SP          0          1024       1920    0
TAILDROP
12     -     -    -    SP          0          128        1920    0
TAILDROP
13     -     -    -    SP          0          1024       1920    0
TAILDROP
14     -     -    -    SP          0          128        1920    0
TAILDROP
15     -     -    -    SP          500        500        99840   0
TAILDROP
16     -     -    -    SP          500        500        99840   0
TAILDROP
17     -     -    -    SP          500        500        99840   0
TAILDROP
18     -     -    -    SP          0          10048      1920    0
TAILDROP
19     -     -    -    SP          0          10048      1920    0
TAILDROP
20     -     -    -    SP          0          10048      1920    0
TAILDROP
```


.

```
21      -       -       -       SP              500             500             99840   0
TAILDROP
22      -       -       -       SP              500             500             99840   0
TAILDROP
23      -       -       -       SP              500             500             99840   0
TAILDROP
24      -       -       -       SP              500             500             99840   0
TAILDROP
25      -       -       -       SP              2000            20000           199872  0
TAILDROP
26      -       -       -       SP              500             500             99840   0
TAILDROP
27      -       -       -       SP              500             500             99840   0
TAILDROP
28      -       -       -       SP              500             500             99840   0
TAILDROP
29      -       -       -       SP              0               10048           1920    0
TAILDROP
30      -       -       -       SP              500             500             99840   0
TAILDROP
31      -       -       -       SP              0               1024            1920    0
TAILDROP
32      -       -       -       SP              500             500             99840   0
TAILDROP
33      -       -       -       SP              500             500             99840   0
TAILDROP
34      -       -       -       SP              500             500             99840   0
TAILDROP
35      -       -       -       SP              500             500             99840   0
TAILDROP
36      -       -       -       SP              500             500             99840   0
TAILDROP
37      -       -       -       SP              0               5056            1920    0
TAILDROP
38      -       -       -       SP              500             500             99840   0
TAILDROP
39      -       -       -       SP              500             500             99840   0
TAILDROP
40      -       -       -       SP              500             500             99840   0
TAILDROP
41      -       -       -       SP              500             500             99840   0
TAILDROP
42      -       -       -       SP              500             500             99840   0
TAILDROP
43      -       -       -       SP              0               10048           1920    0
TAILDROP
44      -       -       -       SP              500             500             99840   0
TAILDROP
45      -       -       -       SP              500             500             99840   0
TAILDROP
46      -       -       -       SP              500             500             99840   0
TAILDROP
```


.

```
47      -       -       -       SP              500             500             99840   0
TAILDROP
48      -       -       -       SP              500             500             99840   0
TAILDROP

                                                                                QUEUED
QUEUED
                                        OUT     OUT     QUEUED  UC      QUEUED  MC
COSQ    OUT                             DROP    DROP    UC      BYTES   MC
BYTES
ENTRY   PKTS    OUT BYTES       PKTS    BYTES   BYTES   PEAK    BYTES   PEAK
-------------------------------------------------------------------------------
----
1       0       0               0       0       0       0       0       0
2       0       0               0       0       0       0       0       0
3       0       0               0       0       0       0       0       0
4       0       0               0       0       0       0       0       0
5       0       0               0       0       0       0       0       0
6       0       0               0       0       0       0       0       0
7       0       0               0       0       0       0       0       0
8       0       0               0       0       0       0       0       0
9       0       0               0       0       0       0       0       0
10      0       0               0       0       0       0       0       0
11      0       0               0       0       0       0       0       0
12      0       0               0       0       0       0       0       0
13      16      1480            0       0       0       0       0       0
14      0       0               0       0       0       0       0       0
15      0       0               0       0       0       0       0       0
16      0       0               0       0       0       0       0       0
17      0       0               0       0       0       0       0       0
18      0       0               0       0       0       0       0       0
19      0       0               0       0       0       0       0       0
20      0       0               0       0       0       0       0       0
21      0       0               0       0       0       0       0       0
22      0       0               0       0       0       0       0       0
23      0       0               0       0       0       0       0       0
24      0       0               0       0       0       0       0       0
25      0       0               0       0       0       0       0       0
26      0       0               0       0       0       0       0       0
27      0       0               0       0       0       0       0       0
28      0       0               0       0       0       0       0       0
29      0       0               0       0       0       0       0       0
30      622825  45777638        0       0       0       0       0       0
31      0       0               0       0       0       0       0       0
32      0       0               0       0       0       0       0       0
33      0       0               0       0       0       0       0       0
34      0       0               0       0       0       0       0       0
35      0       0               0       0       0       0       0       0
36      0       0               0       0       0       0       0       0
```


.

```
37     0        0          0     0      0       0       0       0
38     0        0          0     0      0       0       0       0
39     0        0          0     0      0       0       0       0
40     0        0          0     0      0       0       0       0
41     0        0          0     0      0       0       0       0
42     1405618  145281675  0     0      0       0       0       0
43     0        0          0     0      0       0       0       0
44     0        0          0     0      0       0       0       0
45     0        0          0     0      0       0       0       0
46     0        0          0     0      0       0       0       0
47     0        0          0     0      0       0       0       0
48     0        0          0     0      0       0       0       0
```

```
 access-group
  statistics
   acl-type IPv4 Ingress Interface
    acl-name CONTROL_PLANE_FILTER-IPv4
SEQ                  HIT
NUM    ACTIONS       COUNTER
------------------------------
10     p/c/cpuQ-28/  0
20     p/c/cpuQ-9/   0
21     p/c/cpuQ-9/   0
29     p/c/cpuQ-11/  0
30     p/c/cpuQ-13/  16
40     p/c/cpuQ-30/  622827
50     p/c/cpuQ-30/  0
100    p/c/cpuQ-18/  0
101    p/c/cpuQ-19/  0
102    p/c/cpuQ-20/  0
130    p/c/cpuQ-31/  0
140    p/c/cpuQ-14/  0
141    p/c/cpuQ-14/  0
150    p/c/cpuQ-42/  1405618
180    d/c/          0
255    d/c/          15199
65535  d/c/          0
```


.

Chapter 7

Configuring Basic System Settings

This section describes how to configure optional basic system settings and consists of the following topics.

Refer to each topic listed above for more information.

Hostname Configuration

This topic describes how to configure the basic parameters for the hostname configuration.

Parameters

You can configure the following hostname parameters for the system:

Parameter	Description	Valid Options
Hostname Configuration		
hostname	A unique name to identify the given AXOS system in the network.	1–63 alphanumeric characters, and special character - (dash). system (default) **Note**: The hostname must include at least one alpha character.
location	System location.	0–64 characters, including letters, numbers, and special characters: ~@#$%^&*()_+`-={}|\:;'?,./ **Note**: The system does not support the following special characters: ! and <>
contact	System contact information.	

Procedure

To configure the hostname configuration

- **Calix-1(config)# hostname <hostname>**
- **Calix-1(config)# location <string>**
- **Calix-1(config)# contact <string>**

DNS Server

This topic describes how to configure DNS server settings.

Parameters

You can configure the following DNS server parameters for the system:

Parameter	Description	Valid Options
DNS Server E3-2 only		
ip name-server {address <DNS name server address>|source-interface <interface>|lb1 <loopback address>}*	Sets the IP address of a Domain Name System (DNS) server. Also allows you to configure the DNS client to use a loopback interface address. A DNS server maps domain names to IP addresses, so that hosts such as the NTP server or upgrade server can be configured via a hostname rather than an IP address. This setting also adds flexibility in the event that IP addresses are changed on servers that the node needs to reach (for example the NTP server). A loopback address is an IP address that is used to test the communication medium on a local network card. Data packets that are sent on a loopback address are re-routed back to the orginating node without any alteration or modification.	IPv4 or IPv6 address IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each IPv6 format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal value source-interface format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each
DNS Server E7-2 only		
ip name-server address <DNS name server address>*	Sets the IP address of a Domain Name System (DNS) server. Also allows you to configure the DNS client to use a loopback interface address. A DNS server maps domain names to IP addresses, so that hosts such as the NTP server or upgrade server can be configured via a hostname rather than an IP address. This setting also adds flexibility in the event that IP addresses are changed on servers that the node needs to reach (for example the NTP server).	IPv4 or IPv6 address IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each IPv6 format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal value

DNS Server E9-2 only		
ip name-server {address <DNS name server address>|vrf <DNS vrf name>|source-interface <interface>loop address <loopback address>}* Note: VRF is supported by E9-2 systems only	Sets the IP address of a Domain Name System (DNS) server. Also allows you to configure the DNS client to use a loopback interface address. A DNS server maps domain names to IP addresses, so that hosts such as the NTP server or upgrade server can be configured via a hostname rather than an IP address. This setting also adds flexibility in the event that IP addresses are changed on servers that the node needs to reach (for example the NTP server). A loopback address is an IP address that is used to test the communication medium on a local network card. Data packets that are sent on a loopback address are re-routed back to the originating node without any alteration or modification.	IPv4 or IPv6 address IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each IPv6 format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal value source-interface format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each DNS VRF name

* User input required

Procedure

To configure DNS server settings (E3-2)

```
Calix-1(config)# ip name-server address <DNS name server address>
Calix-1(config)# ip name-server source-interface <source interface name> lb1
address <loopback address>
```

To configure DNS server settings (E7-2)

```
Calix-1(config)# ip name-server address <DNS name server address>
```

To configure DNS server settings (E9-2 only)

```
Calix-1(config)# ip name-server address <DNS name server address>
Calix-1(config)# ip name-server vrf <vrf name>

Calix-1(config)# ip name-server source-interface system-craft address <DNS
name server address>
```

IP Host

This topic describes how to configure IP host settings.

Parameters

You can configure the following IP host parameters for the system:

Parameter	Description	Valid Options
IP Host		
ip host name*	Name for the IP host, and the IP address to which the name is mapped. Format <string> address <IP address> Associating the name with an IP address, allows the name to become an "alias" for the address.	Name: String of 1–253 letters IPv4 or IPv6 address: IPv4 format - x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each IPv6 format - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal value
IP Host VRF (E9-2 only)		
ip host vrf* name <ip host name> address <ip address>	Name for the IP host in the VRF followed by the name of the ip host and the IP address to which the name is mapped. Associating the name with an IP address, allows the name to become an "alias" for the address.	Name: String of 1–253 letters IPv4 or IPv6 address: IPv4 format - x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each IPv6 format - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal value VRF name

* User input required

Procedure

To configure IP host settings for E3-2 and E7-2 systems

- **`Calix-1(config)# ip host name <ip host name> address <ip address>`**

To configure IP host settings for E9-2 systems

- **`Calix-1(config)# ip host name <ip host name> address <ip address>`**
- **`Calix-1(config)# ip host vrf <vrf name>`**
- **`Calix-1(config)# name <ip host name> address <ip address>`**

Domain Settings

This topic describes how to configure domain settings.

Parameters

You can configure the following domain parameters for the system:

Parameter	Description	Valid Options
Domain Settings		
ip default-domain domain-name <domain name>	Sets a default domain name used to complete unqualified host names.	1–253 alpha numeric characters
ip default-domain [vrf <vrf-name>] domain name <DNS domain name> (E9-2 only)	Sets a default domain name used to complete unqualified host names as well as a default VRF name.	VRF name
ip search-domain domain-name	Configure a maximum of four domain names in a search list used to complete unqualified hostnames. The system uses each domain name until it can resolve a domain qualified host name (or host + domain name) into an IP address.	DNS domain name
ip search-domain vrf <default vrf name> (E9-2 only)	Configure a maximum of four domain names in a search list used to complete unqualified hostnames as well as a default VRF name. The system uses each domain name until it can resolve a domain qualified host name (or host + domain name) into an IP address.	VRF name

Procedure

To configure domain settings for E3-2 and E7-2 systems

- **Calix-1(config)# ip default-domain domain-name <default domain name>**
- **Calix-1(config)# ip search-domain domain-name <DNS domain name>**

To configure domain settings for E9-2 systems

- **Calix-1(config)# ip default-domain domain-name <default domain name>**
- **Calix-1(config)# ip default-domain vrf <vrf name> domain-name <DNS domain name>**
- **Calix-1(config)# ip vrf <vrf name>**
- **Calix-1(config)# ip search-domain domain-name <DNS domain name>**
- **Calix-1(config)# ip search-domain vrf <vrf name>**
- **domain-name <DNS domain name>**

NTP Server

This topic describes how to configure NTP server settings.

Parameters

You can configure the following NTP server parameters for the system:

Parameter	Description	Valid Options
NTP Server		
ntp server	Specifies the NTP server number, and sets the IP address or domain name of the NTP server which the system uses for basic time synchronization. Format: {1|2} {IP address|DNS} You can configure up to two NTP servers. The system supports client/server mode, where a client (the AXOS system) sends an NTP message to one or more servers and processes the replies as received. The server interchanges addresses and ports, overwrites certain fields in the message, recalculates the checksum, and returns the message immediately. Information included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock accordingly.	Server: 1 or 2 IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each 0.0.0.0 = default Domain name: 1–253 alpha numeric characters

Procedure

To configure NTP server settings

- **`Calix-1(config)# ntp server {1|2} <host address>`**

System Time Configuration

This topic describes how to configure system time settings.

Parameters

You can configure the following system time parameters for the system:

Parameter	Description	Valid Options
System Time Configuration		
clock set	Sets the system date and time. Keeping the system time up to date is important for troubleshooting activities, including log analysis. **Note**: This is an Operation mode command.	System date and time in the format: YYYY-MM-DDTHH:MM:SS
timezone	Global time zone (as defined by the IANA timezone database) used by the AXOS system as a reference. See http://www.iana.org/time-zones.	Any available time zone America Los Angeles ‡ **Note**: You can scroll through the timezone list, or type the first few letters (for example 'America' or 'Asia').

Procedure

To configure system time settings

- **`Calix-1# clock set <YYYY-MM-DDTHH:MM:SS>`**
- **`Calix-1(config)# timezone <a timezone location>`**

Reserved VLAN Settings

This topic describes how to configure reserved VLAN settings.

Parameters

You can configure the following reserved VLAN parameters for the system:

Parameter	Description	Valid Options
Reserved VLAN Settings		
reserve-vlan-range {start|end}	A VLAN IDs to start and end the reserve VLAN range. The reserve VLAN settings specify VLANs that cannot be used for subscriber services. By default VLAN IDs 1002-1005 are reserved for AXOS system operation.	1–4094 1002 (default for start VLAN) 1005 (default for end VLAN)

Procedure

To configure basic reserved VLAN settings

- **`Calix-1(config)# reserve-vlan-range end <VlanID> start <VlanID>`**

Chapter 8

Configuring User Authentication and Authorization

This chapter describes user authentication and authorization features for AXOS systems.

About E3-2/E7-2 User Authentication and Authorization

The E3-2/E7-2 supports the following user authentication and authorization features:

- Authentication order
- Local user accounts
- RADIUS
- TACACS+

Authentication Order (E3-2/E7-2)

Authentication is a process of identifying the user and verifying that the user is allowed to login. A user may login into the CLI (via SSH and Telnet) or NETCONF (via SSH).

Three categories of users may login into the management interfaces:

- TACACS+ users
- RADIUS users
- Local users

The E3-2/E7-2 supports the following configurable authentication order:

- **Local only** (default): Authentication using the local databased only.
- **RADIUS if up, else local**: Authentication using RADIUS if up (accessible), or else local database.
- **RADIUS then local**: Authentication using RADIUS server and then the local database if the RADIUS user lookup is unsuccessful.
- **TACACS+ then local**: Authentication using TACACS+ and then the local database if TACACS+ fails.

Note: The supported authentication order assumes the use of one external authentication method—either RADIUS or TACACS+, but not both at the same time.

To configure the authentication order

```
Calix-1(config)# aaa authentication-order <local-only|radius-if-up-else-
local|radius-then-local|tacacs-then-local>
```

Configuring Local User Accounts (E3-2/E7-2)

This section describes how to create and modify user accounts which use local authentication. User accounts provide access to the E3-2/E7-2 and define the specific actions permitted by each user. Each account includes the following criteria:

- Role
- Password
- User name

The E3-2/E7-2 support up to 64 user accounts defined locally (not in a RADIUS or TACACS+ server), including four predefined accounts.

Predefined user accounts

The E3-2/E7-2 provide the following predefined user accounts:

User Name	Password	Role
sysadmin	sysadmin	admin
networkadmin	networkadmin	networkadmin
monitor	monitor	oper
support	support	oper

Note: As a security precaution, Calix recommends changing all default local passwords if your AXOS system has any IP interfaces exposed to the public internet.

Role

A role defines a specific set of tasks or operations that can be performed by a user, and are assigned to user accounts. A user account can have more than one role, and is not valid without an assigned role.

The E3-2/E7-2 provide the following predefined roles:

- **System Administrator (admin)**: Create, read, write, delete and execute permissions.
- **Network Administrator (networkadmin)**: Create, read, write, delete and execute permissions, with the exception of configuring Authentication and Authorization.
- **Operator (oper)**: Read-only permissions

If you do not assign a role when creating a user account, read-only permissions are assigned.

Note: The system does support creating roles.

Password

User passwords are case-sensitive text strings. There are no password length restrictions, however a mix of upper and lower case letters, numbers, and special characters is recommended.

Note: Passwords starting with "1" or "4" are not encrypted, and display as plain text.

User name

In addition to the user names associated with predefined user accounts, you may create unique user names. User names are alpha-numeric strings of 3–16 characters in length, starting with a lower case letter or underscore, followed by lower case letters, numbers, underscore or hyphen. Optionally, the user name can end with a dollar sign.

Creating a User Account

This topic shows you how to create a unique user account for access to the CLI.

Parameters

You can configure the following parameters for a user account:

Parameter	Description
aaa user <username>	User name for the user account. This is a unique string of 3-16 characters. Allowed characters are: [a-z_][a-z0-9_-]*[$]? Valid values: • calixsupport • monitor • networkadmin • support • sysadmin • tac • <any previously created user account, 3-16 chars>
password	Password for the user account. Valid values: • <string of 3-32 characters> **Note 1**: Passwords starting with "1" or "4" are not encrypted, and display as plain text. When a password is not entered, the system auto-generates a default password. **Note 2**: When using the CLI, password strings may also be enclosed in quotes. This is necessary if your password contains the ! character, which is normally used for comments and ignored. For example: • Not good: password 123!!! • Good: password "123!!!"
role	Access level to assign to the system user account. • admin: A role with create, read, write, delete and execute permissions. • calixsupport: A role for Calix TAC called "calixsupport" that has a default password. If this role is deleted and recreated, a new custom password with the standard password rules is required • networkadmin: A role for a network administrator. This role provides the ability to create, read, write, delete and execute permissions, with the exception of configuring Authentication and Authorization. • oper: A role for an operator with read-only permissions.
	E9-2 notes: • The predefined law enforcement agency roles (leaadmin and leauser) are associated with subscriber management functionality. • A TACACS+ RBAC role can also be associated to the locally created user.

Procedure

To create a user account

```
Calix-1(config)# aaa user <Username> password <string> role
{admin|networkadmin|oper}
```

Note: When a system user account is created with this command, the names of roles that are available in the system are not displayed. Issue the command "**show aaa user local-role**" to see the available roles (internally-created and RBAC).

Modifying a User Account

This topic shows you how to modify a unique or predefined system user account.

To edit a system user account

```
Calix-1(config)# aaa user <Username> password <string> role
{admin|networkadmin|oper}
```

To delete a role or system user account

To delete a role, use the following command:

```
Calix-1(config-user-johndoe)# no role
```

To delete an account, use the following command:

```
Calix-1(config)# no aaa user <Username>
```

Configuring TACACS+ (E3-2/E7-2)

This section shows you how to configure a Terminal Access Controller Access-Control System Plus (TACACS+) server for system user login authentication and authorization.

TACACS+ is a client/server protocol that provides secure access to AXOS systems.

The AXOS system as TACACS+ client:

1. Passes user information to TACACS+ servers.
2. Acts upon the response.

The TACACS+ server(s):

1. Receives system user connection requests.
2. Authenticates the system user.
3. Returns all configuration information necessary for the client to deliver service to the system user by granting the appropriate access permissions.

Communications between the client and server are encrypted using a shared secret. The system raises an INFO alarm to alert the operator when a TACACS+ server is unreachable.

High level configuration steps

To use TACACS+ authentication and authorization, do the following:

1. Configure system user accounts and roles in the TACACS+ server(s).
2. Configure the TACACS+ server(s) on the AXOS systems.

Configuring User Accounts on a TACACS+ Server

This topic provides an example for configuring user accounts on a tac_plus server on Linux. You may perform similar steps on a different type of TACACS+ server; refer to the user documentation.

To configure user accounts on a TACACS+ server (tac_plus example)

1. Create a tac_plus.conf file with the following content:

```
key = "testing1234567890"
group = admin {
    service = Login {
       ROLES = admin
       }
}
group = networkadmin {
    service = Login {
       ROLES = networkadmin
       }
}
group = oper {
    service = Login {
       ROLES = oper
       }
}
user = testnetadmin {
    member = Login {
       login = cleartext "hello"
       }
}
user = testoper {
    member = Login {
       login = cleartext "hello"
       }
}
```

2. Create the configuration file start/restart for the tac_plus server using the following command:

```
tac_plus -C tac_plus.conf
```

Configuring a TACACS+ Server on the E3-2/E7-2

This topic describes how to configure a TACACS+ server on the E3-2/E7-2.

Configuration guidelines

- The E3-2/E7-2 supports up to four authentication TACACS servers, each with a unique server IP address, and a shared Secret name and port.
- The system initiates communication with first configured server, and then sends the authentication request to the next configured server if it does not get a response.

Parameters

You can configure the following parameters for a TACACS+ server on the E3-2/E7-2:

Parameter	Description	Valid Options
Server*	IP address or DNS domain name of the TACACS+ server.	IPv4 address 0.0.0.0 (default) Domain name
Port	Port number for the TACACS+ server. This is a TCP or UDP port number.	0-65535 49 (default)
Secret	The "shared secret" for the E3-2/E7-2 and the TACACS+ server. This string must match the string configured in the TACACS+ server.	Text string of 16–63 characters, including spaces
Timeout	Number of seconds to wait for a response from the TACACS+ server before retransmitting or aborting.	1–30 5 (default)

*User input required

Procedure

To configure a TACACS+ server on the AXOS system

```
Calix-1(config)# aaa tacacs server <host address|IPv4 address|domain
name> [port <0-65535>] <secret <string>> [timeout <1-30>]
```

Example:

1. **Calix-1(config)# aaa tacacs server 10.1.1.1**
2. **Calix-1(config-server-10.1.1.1)# port 1900**
3. **Calix-1(config-server-10.1.1.1)# secret testing123456789**
4. **Calix-1(config-server-10.1.1.1)# timeout 2**
5. **Calix-1(config-server-10.1.1.1)# end**

Configuring RADIUS (E3-2/E7-2)

This section shows you how to configure a Remote Authentication Dial-Up Service (RADIUS) server for user login authentication and authorization.

RADIUS is a client/server protocol that provides secure access to E3-2/E7-2 networks.

The E3-2/E7-2 as RADIUS client:

1. Passes user information to RADIUS servers.
2. Acts upon the response.

The RADIUS server(s):

1. Receives user connection requests.
2. Authenticates the user.
3. Returns all configuration information necessary for the client to deliver service to the user by granting the appropriate access permissions.

Communications between the client and server are encrypted using a shared secret.

High level configuration steps

To use RADIUS authentication and authorization, do the following:

1. Configure user accounts and roles in the RADIUS server(s).
2. Configure the RADIUS server(s) on the E3-2/E7-2.

Configuring User Accounts on a RADIUS Server

This topic provides an example for configuring system user accounts on a FreeRADIUS server. You may perform similar steps on a different type of RADIUS server; refer to the user documentation.

Configuration guidelines

- You cannot configure multiple roles for RADIUS users.
- After logging into the AXOS system using a RADIUS user account:
  - You cannot modify the user role in the RADIUS server.
  - You cannot create a local user with the same name configured on the RADIUS server.

Procedure

To configure system user accounts on a RADIUS server (FreeRADIUS example)

1. Create a dictionary file (for example, calix.dictionary) for Vendor Specific Attributes under directory "/etc/raddb/" and include the following:

```
bash-4.2$ cat /etc/raddb/calix.dictionary
VENDOR    Calix    4000
BEGIN-VENDOR    Calix
    ATTRIBUTE    Role 1 string
END-VENDOR     Calix
```

2. Include this dictionary file in the main dictionary (/etc/raddb/dictionary):

```
bash-4.2$ cat /etc/raddb/dictionary
$INCLUDE    /usr/share/freeradius/dictionary
$INCLUDE    /etc/raddb/calix.dictionary
```

3. Configure the RADIUS users in "/etc/raddb/users" file. An example user configuration follows:

```
calix Cleartext-Password := "hello"
Role := "admin",
Reply-Message := "Hello, %{User-Name}"
testuser Cleartext-Password := "hello"
Role := "oper",
Reply-Message := "Hello, %{User-Name}"
```

4. Configure the client IP address (AXOS system IP address) which may use this RADIUS server in the "/etc/raddb/clients.conf" file. An example client configuration follows:

```
client 10.1.28.187 {
secret = testing124
shortname = SBAHardware
}
```

5. To start the RADIUS server on a port other than the default (1812), you may modify the /etc/raddb/radiusd.conf file.

6. Start or restart the RADIUS server (use command "radiusd" if the server is not already running).

Configuring a RADIUS Server on the AXOS System

This topic describes how to configure a RADIUS server on the AXOS system.

Configuration guidelines

- The AXOS system supports up to four authentication RADIUS servers, each with a unique server IP address, and a shared Secret name and port.
- The system initiates communication with first configured server, and then sends the authentication request to the next configured server if it does not get a response.

Parameters

You can configure the following parameters for a RADIUS server on the AXOS system:

Parameter	Description	Valid Options
Retry	The number of times the client can try to access the configured RADIUS server before it resubmits the request to the next configured RADIUS server or aborts. This is a global configuration, applying to all configured servers.	1-10 3 (default)
Server*	IP address or DNS domain name of the RADIUS server. The DNS domain name can contain only upper and lower case characters, numbers, underscore, dash and dot. The # and @ symbols are not supported.	IPv4 address 0.0.0.0 (default) Domain name
Port	Port number for the RADIUS server. This is a TCP or UDP port number.	0-65535 1812 (default)
Secret*	The "shared secret" for the AXOS system and the RADIUS server. This string must match the string configured in the RADIUS server.	Text string of 16–128 characters, including spaces
Timeout	Number of seconds to wait for a response from the RADIUS server before retransmitting or aborting.	1–30 3 (default)

*User input required

Procedure

To configure a RADIUS server on the AXOS system

1. **Calix-1(config)# aaa radius retry <1-10>**
2. **Calix-1(config)# aaa radius server <host address|IPv4 address|domain name> [port <0-65535>] <secret <string>> [timeout <1–30>]**

Example:

1. **Calix-1(config)# aaa radius server 10.1.1.1**
2. **Calix-1(config-server-10.1.1.1)# secret testing123456789**
3. **Calix-1(config-server-10.1.1.1)# port 1900**
4. **Calix-1(config-server-10.1.1.1)# timeout 2**

```
Calix-1(config-server-10.1.1.1)# end
```

Configuring RADIUS Accounting

This topic describes how to configure RADIUS accounting on the AXOS system.

Configuration Guidelines

In order to use RADIUS accounting, RADIUS must first be enabled, the RADIUS accounting servers must be configured to send RADIUS accounting records to all or the first available server, and then you must configure the sending of accounting requests to the RADIUS servers.

The following configuration is required:

- Global accounting enable or disable.
- Radius accounting order ("none", "first-available", all-servers).
- Radius accounting servers configuration (hostname/IP, shared secret, port, timeout and priority)

The following table lists all of the configuration options for RADIUS accounting servers.

Parameter	Valid Options	Description
set radius-accounting-admin-state	<admin-state disable|enable>	Enable AAA Radius Accounting
set radius-accounting-send-to	<send-to none|first-available|all-servers> none (default)	Set radius accounting send-to.
set radius-accounting-server-port	<server (^(.*)$)> <port 0-65535>	Set radius accounting server port.
set radius-accounting-server-priority	<server (^(.*)$)> <priority 1-10>	Set radius accounting server priority.
set radius-accounting-server-timeout	<server (^(.*)$)> <timeout 1-30>	Set radius accounting server timeout.
add radius-accounting-server	<server (^(.*)$)>	Add radius accounting server.
add radius-accounting-server-secret	<server (^(.*)$)> <secret (^(.*)$)>	Add radius accounting secret server.
add radius-accounting-src-if	<iface (^(.*)$)>	Set source-interface for radius accounting requests (global)
del radius-accounting-server <server	<server (^(.*)$)>	Delete a radius accounting server.
del radius-accounting-server-secret	<server (^(.*)$)> <secret (^(.*)$)>	Delete a secret radius accounting server.
del radius-accounting-src-if	<iface (^(.*)$)>	Clear source-interface for radius accounting requests(global)

Parameters

You can configure the following parameters for a RADIUS server on the AXOS system:

Parameter	Description	Valid Options
Server*	IP address or DNS domain name of the RADIUS server. The DNS domain name can contain only upper and lower case characters, numbers, underscore, dash and dot. The # and @ symbols are not supported.	IPv4 address 0.0.0.0 (default) Domain name
Port	Port number for the RADIUS server. This is a TCP or UDP port number.	0-65535 1812 (default)
Timeout	Number of seconds to wait for a response from the RADIUS server before retransmitting or aborting.	1–30 3 (default)
Priority	Radius accounting sever priority.	1-10

*User input required

Procedure

To configure RADIUS Server Accounting on the AXOS system

1. **Calix-1(config)# aaa radius server <host address|IPv4 address|domain name> [port <0-65535>] [timeout <1-30>] [priority <1-10>]**

Example:

1. **Calix-1(config)# aaa radius server 10.1.1.1**
2. **Calix-1(config-server-10.1.1.1)# port 1900**
3. **Calix-1(config-server-10.1.1.1)# timeout 2**
4. **Calix-1(config-server-10.1.1.1)# priority 3**
5. **Calix-1(config-server-10.1.1.1)# end**

About E9-2 User Authentication and Authorization

The E9-2 management interfaces may be accessed locally or remotely.

The E9-2 supports Role Base Access Control (RBAC), where individual users are associated with one or more roles. Each role has a set of permissions that allow or deny access to various configuration data and commands within the system.

The E9-2 supports local or remote authentication/authorization for a user, depending on the configuration.

At a high level, user privileges are established as follows:

1. A user connects to the E9-2 by supplying credentials that are authenticated and authorized. Authorization is a process of identifying if an authenticated user has the privilege to execute a command.
2. As part of the authorization step, the user is provided with one or more roles.
    - Local System Users: The E9-2 uses local system user accounts to provide access to the E9-2 and define the specific actions permitted by each user. The roles associated with the user are locally configured in the E9-2.
    - Remote System Users: The E9-2 supports using Terminal Access Controller Access Control System+ (TACACS+) to authenticate and authorize non-local users who access the system. The authorization process via TACACS+ involves returning the roles and permissions to a user. After a role is created through RBAC or a local system user account, a user must be created through TACACS+ to allow authentication and login.

Note: The E9 SMm uses Remote Authentication Dial-In User Service (RADIUS) protocol for accounting. RADIUS protocol works in a client server model, where the RADIUS client runs on the SMm and contacts an external RADIUS server (following successful IP address allocation) to send accounting records for a subscriber session.

Lawful Intercept

As a legally sanctioned official access to private communications, Lawful Interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations. Users having LI administrative and user roles may be authenticated by a TACACS+ server. The TACACS+ server may also assign LI administrative and user roles to users who are not locally defined in the E9-2 during authentication, but the access permissions for these LI administrative and user roles must be locally defined in the E9-2 and cannot be overridden by the TACACS+ server. For more information, refer to the *AXOS R20.x Access Aggregation and Routing Applications Guide.*

Configuring the Authentication Order (E9-2)

Authentication is a process of identifying the user and verifying that the user is allowed to login. A user may login into the CLI (via SSH and Telnet) or NETCONF (via SSH).

Three categories of users may login into the management interfaces:

- TACACS+ users
- RADIUS users
- Local users

The AXOS system supports the following configurable authentication order:

- **Local only** (default): Authentication using the local databased only.
- **RADIUS if up, else local**: Authentication using RADIUS if up (accessible), or else local database.
- **RADIUS then local**: Authentication using RADIUS server and then the local database if the RADIUS user lookup is unsuccessful.
- **TACACS+ then local**: Authentication using TACACS+ and then the local database if TACACS+ fails.

Note: The supported authentication order assumes the use of one external authentication method—either RADIUS or TACACS+, but not both at the same time.

To configure the authentication order

```
Calix-1(config)# aaa authentication-order <local-only|radius-if-up-
elselocal|radius-then-local|tacacs-then-local>
```

Configuring Local System User Accounts (E9-2)

This section describes how to create and modify system user accounts which use local authentication. System user accounts provide access to the E9-2 and define the specific actions permitted by each user. Each account includes the following criteria:

- Role
- Password
- User name

The E9-2 support up to 64 system user accounts defined locally (not in a TACACS+ server), including five predefined accounts.

Predefined system user accounts

The E9-2 provide the following predefined system user accounts:

User Name	Password	Role
sysadmin	sysadmin	admin
tac	admin	admin
networkadmin	networkadmin	networkadmin
monitor	monitor	oper
support	support	oper
calixsupport*	calixsupport	calixsupport

*This is a special user, meant to be used only by Calix support personnel in order to debug any issues. The user "calixsupport" may be deleted but a new custom password is required if it is subsequently recreated.

Note: As a security precaution, Calix recommends changing all default local passwords if your AXOS system has any IP interfaces exposed to the public internet.

Role

A role defines a specific set of tasks or operations that can be performed by a user, and are assigned to system user accounts. A user account can have more than one role, and is not valid without an assigned role.

The E9-2 provide the following predefined roles that cannot be modified:

- **System Administrator (admin)**: Create, read, write, delete and execute permissions.
- **Security Administrator (secadmin)**: Create, read, write, delete and execute permissions for all management plane AAA aspects
- **Network Administrator (networkadmin)**: Create, read, write, delete and execute permissions, with the exception of configuring Authentication and Authorization.
- **Operator (oper)**: Read-only permissions
- **Calix Support (calixsupport):** This role is associated with the user "calixsupport", which is intended to be used by Calix support personnel only.

The predefined law enforcement agency roles (leaadmin and leauser) are associated with subscriber management functionality.

Password

User passwords are case-sensitive text strings. There are no password length restrictions, however a mix of upper and lower case letters, numbers, and special characters is recommended.

Note: Passwords starting with "1" or "4" are not encrypted, and display as plain text.

System user name

In addition to the user names associated with predefined user accounts, you may create unique user names. User names are alpha-numeric strings of 3–16 characters in length, starting with a lower case letter or underscore, followed by lower case letters, numbers, underscore or hyphen. Optionally, the user name can end with a dollar sign.

Creating a User Account

This topic shows you how to create a unique user account for access to the CLI.

Parameters

You can configure the following parameters for a user account:

Parameter	Description
aaa user <username>	User name for the user account. This is a unique string of 3-16 characters. Allowed characters are: [a-z_][a-z0-9_-]*[$]? Valid values: • calixsupport • monitor • networkadmin • support • sysadmin • tac • <any previously created user account, 3-16 chars>
password	Password for the user account. Valid values: • <string of 3-32 characters> **Note 1**: Passwords starting with "1" or "4" are not encrypted, and display as plain text. When a password is not entered, the system auto-generates a default password. **Note 2**: When using the CLI, password strings may also be enclosed in quotes. This is necessary if your password contains the ! character, which is normally used for comments and ignored. For example: • Not good: password 123!!! • Good: password "123!!!"
role	Access level to assign to the system user account. • admin: A role with create, read, write, delete and execute permissions. • calixsupport: A role for Calix TAC called "calixsupport" that has a default password. If this role is deleted and recreated, a new custom password with the standard password rules is required • networkadmin: A role for a network administrator. This role provides the ability to create, read, write, delete and execute permissions, with the exception of configuring Authentication and Authorization. • oper: A role for an operator with read-only permissions.
	E9-2 notes: • The predefined law enforcement agency roles (leaadmin and leauser) are associated with subscriber management functionality. • A TACACS+ RBAC role can also be associated to the locally created user.

Procedure

To create a user account

```
Calix-1(config)# aaa user <Username> password <string> role
{admin|networkadmin|oper}
```

Note: When a system user account is created with this command, the names of roles that are available in the system are not displayed. Issue the command "**show aaa user local-role**" to see the available roles (internally-created and RBAC).

Modifying a User Account

This topic shows you how to modify a unique or predefined system user account.

To edit a system user account

```
Calix-1(config)# aaa user <Username> password <string> role
{admin|networkadmin|oper}
```

To delete a role or system user account

To delete a role, use the following command:

```
Calix-1(config-user-johndoe)# no role
```

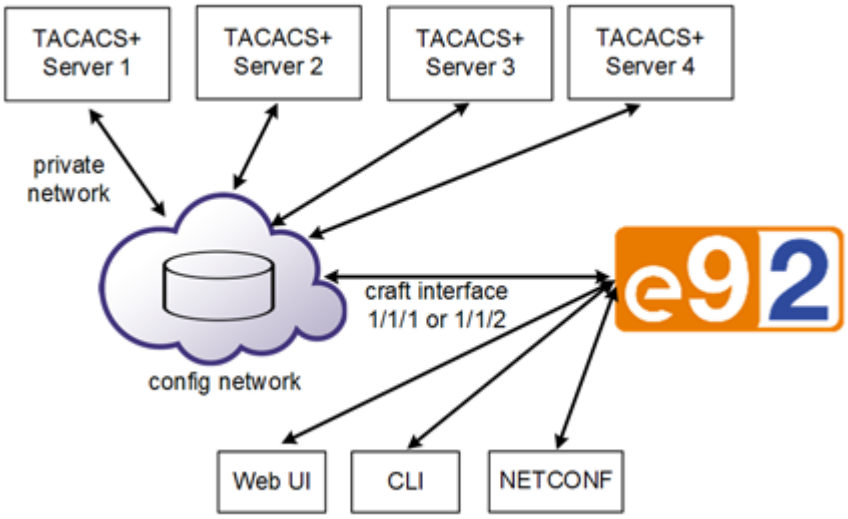
To delete an account, use the following command:

```
Calix-1(config)# no aaa user <Username>
```

Configuring TACACS+ (E9-2)

This section shows you how to configure a Terminal Access Controller Access-Control System Plus (TACACS+) server for system user login authentication and authorization.

TACACS+ is one of the remote Authentication, Authorization and Accounting mechanisms supported by E9-2 to provide non-local authentication and authorization. TACACS+ authenticates and authorizes local and non-local users accessing the system via NETCONF, CLI or Web interfaces. The TACACS+ authorization process involves returning roles and permissions to a user.



In the illustration above, the user connects with the E9-2 via the craft interface. The E9-2 then uses the configured source-interface to connect to TACACS+ servers. The first IP address of that interface will be used as the source IP address for all outbound connections by the application.

The E9-2 as TACACS+ client:

1. Passes user information to TACACS+ servers.
2. Acts upon the response.

The TACACS+ server(s):

1. Receives system user connection requests.
2. Authenticates the system user.
3. Returns all configuration information necessary for the client to deliver service to the system user by granting the appropriate access permissions.

Communications between the client and server are encrypted using a shared secret. The E9-2 raises an INFO alarm to alert the operator when a TACACS+ server is unreachable.

High level configuration steps

To use TACACS+ authentication and authorization, do the following:

1. Configure system roles/groups on the E9-2 and associate rules with it.
2. Configure system user accounts in the TACACS+ server(s). The permissions applicable for a user's role can be overridden by the TACACS+ server via allow-permission and deny-permission statements sent by the server.
3. Configure the TACACS+ server(s) on the E9-2.

Configuring RBAC on the E9-2

Role Based Access Control (RBAC) is a key aspect of network security in a L3 network. The E9-2 supports RBAC, where individual users are associated with one or more roles. Each role has a set of permissions that allow or deny access to various configuration data and commands within the system. A permission defines access rights associated with an operation on a resource in the E9-2 system. Permissions have a name, and description. After a role is created through RBAC, the user must be created through TACACS+ to allow authentication and login.

The E9-2 system contains the following predefined roles which cannot be modified:

- System Administrator (admin): Create, read, write, delete and execute permissions.
- Security Administrator (secadmin): Create, read, write, delete and execute permissions for all device management plane AAA aspects.
- Network Administrator (networkadmin): Create, read, write, delete and execute permissions, with the exception of configuring Authentication and Authorization.
- Operator (oper): Read-only permissions

Note: An RBAC role/group can be associated with a locally-created user.

Configuration guidelines

- A rule-list is collection of a group, rules and cmdrules.
  - A group signifies the role that is assigned to a user at the time of authorization.
  - A rule specifies the configuration tree access (either allow or deny access to a particular config tree). It defines an RPC (Remote Procedure Call), notification and data authorization.
  - A cmdrule defines command authorization, specifying access to a particular command (allow or deny).

- The order of rules and cmdrules are important in rule-list; the E9-2 arranges the cmdrules and rules in ascending order by value. The order in which rules and cmdrules are configured does not matter. When a user issues a command, E9-2 tries to match the user's role with a group configured in the rule-lists. If the role matches with the group, the E9-2 picks the first rule/cmdrule from the group and tries to match. If it matches, the configured action against rule/cmdrule will be executed. If not, the E9-2 moves to next rule/cmdrule. If no match is found, the command will be rejected.
- The E9-2 supports insertion and deletion of cmdrules and rules in rule-list, applied in ascending order. For example, rule 2345 is applied before rule 2500.
- The default values of all the cmdrules and rule is DENY. Hence when the command rule is created, you need to explicitly permit/allow rules that permit specific access.
- The rpc-name, path and notification-name are mutually exclusive parameters. In a rule any one of these parameters can be present.
- If the user needs to open a CLI session for specific access and the cmdrule "cmdRule * access-operations * action permit" is not present, the following rules must be added:
  - command rule startup access-operations * action permit
  - command rule enable access-operations * action permit
- The command in command rule supports regular expression. Command rule "command show_.* action deny access-operations *" indicates all commands after show are denied. For example, "show file" and "show running-config" are denied.
- If a rule-list is modified (a rule or cmdrule is added or deleted), the commands "no rbac apply-aaa" and "rbac apply-aaa" must be issued.
- Rules specific to built in and user defined roles for DENY command rule differ in behavior. A built in command which is denied will throw an error as soon as the Enter/TAB keys are hit but a user defined command will not throw an error until the entire command is completed.

  For example, if permissions are denied for the command "show running-config" or "show cli", an error is displayed immediately after TAB/Enter is issued.
  However, if permissions are denied for the command "show file" or "show subscribers", an error is not displayed until after the entire command is has been typed out.

Parameters

You can configure the following parameters for roles:

Parameter	Description	Valid Options
rule-list	Unique name for the rule-list.	A unique string of 3–16 characters, starting with a lower case letter (a–z) or _ (underscore), followed by lower case letters, numbers, underscore or - (hyphen).
group	Unique name for the group that will be assigned the associated access rights defined by the 'rule' list.	A string of characters

Parameter	Description	Valid Options
rule	Value for the rule. Rules can be configured in any order; the numeric value determines the relative order of the rule in a set of multiple rules. For example, when "rule 20" is configured first followed by "rule 10," the E9-2 inserts 10 first followed by 20 in rule-list.	Numerical value
path	An XPath expression used to represent a special data node instance identifier string. A forward slash (/) refers to all possible data store contents.	A string of characters or a forward slash (/).
rpc-name	The name of RPC operation. An asterisk (*) matches any RPC. Refer to *RPC Names* (on page 198) for a list of RPC operation names.	A string of characters or an asterisk (*).
notification-name	The name of the notification. An asterisk (*) matches any notification.	A string of characters or an asterisk (*).
access-operations	Access operations associated with this rule. Valid values are: • create: Any protocol operation that creates a new data node. • delete: Any protocol operation that removes a data node. • exec: Execution access to the specified protocol operation. • read: Any protocol operation or notification that returns the value of a data node. • update: Any protocol operation that alters an existing data node.> Underscore-separated tokens represent the different access-operations combinations. For example, "read" and "exec" access for a command rule is configured as "read_exec". An asterisk (*) represents all possible values.	exec, update, delete and/or create, or an asterisk (*).
action	The permit or deny action associated with the rule.	permit or deny.
all	Applies the specified action to all command models. This includes config, status, exec, and rpc.	
all-config	Applies the specified action to all the config related models.	
all-exec	Applies the specified action to all the exec related models.	
all-status	Applies the specified action to all the status related models.	
cli-path	This leaf includes xpath generation based on context value.	
context	The CLI or NETCONF interface agent that is requesting access. An asterisk (*) represents all agents.	cli, netconf, or an asterisk (*).
cmdrule	Value for a rule that defines access to a command. You may configure a command rule in any order; the numerical value determines the relative order of command rule in a set of multiple command rules.	Numerical value
command	Underscore-separated values representing the command. (for example, "show running-config" must be configured as "show_running-config"). An asterisk (*) matches any value.	A string of characters or an asterisk (*).

Note: Summary of behavior changes from AXOS R4.1 to R19.x/20.x:

- Rule and cmd rule names are numeric to avoid ordering ambiguity.
- The module name does not have to be specified with the rules. This is defaulted to '*' internally.
- "rbac apply-aaa" has been replaced with a rpc "apply rbac-aaa"
- Top level/root nodes have an alternate way of specification by using the rule types 'all/all-config/all-status/all-exec'. These are internally mapped to the respective single/multiple paths.
- '_' is replaced with space as a delimiter. The command needs to be encapsulated in "".
- A new status command "show rbac-status" is available. It displays the current status of the rule as apply-pending/apply-success/apply-failure along with the last user operation add/modify/delete and the last apply timestamp.
- Rules status is restored after reload. Rules in applied status are reapplied and the pending ones are not. For rules that have pending modifications the pre-modification attributes are applied.
- The context attribute option has been removed from rbac rule configuration.
- Configuring rbac rules using actual cli commands which internally generate xpath.

Procedure

To configure/modify a role

1. Specify a name for the rule list and group or enter the names of a previously configured rule list and group.
2. Create or modify a rule in the rule list. Specify the path, RPC name, or the notification name. These are mutually exclusive parameters and any one of them may be configured in a command rule.
3. Create or modify a cmdrule.
4. Commit the RBAC changes. Example:

```
Calix-1(config)# apply rbac-aaa
```

Note: If the rule-list is being modified (a rule or cmd-rule is added or deleted), the commands "**no rbac apply-aaa**" and "**rbac apply-aaa**" must be issued:

```
Calix-1(config)# no apply rbac-aaa
Calix-1(config)# apply rbac-aaa
```

Example

```
CLX3001(config)#rbac rule-list bnc group bnc

CLX3001(config)#rbac rule-list bnc rule 10010 access-operations read
action permit context * path all
CLX3001(config)#rbac rule-list bnc rule 10020 access-operations *
action permit context * path /config/interface/lag
CLX3001(config)#rbac rule-list bnc rule 10030 access-operations *
action permit context * cli-path "interface full-bridge"

CLX3001(config)#rbac rule-list bnc cmdrule 10012 command startup
access-operations * action permit
CLX3001(config)#rbac rule-list bnc cmdrule 10025 command “redundancy
*” access-operations * action deny

CLX3001# show rbac-status
rbac-status
group bnc
  rule-list bnc
   rule 10010
    status               Apply-Pending
    last-user-operation  Add
    last-apply-timestamp "Rule not yet applied"
    failure-reason       None
   rule 10020
    status               Apply-Pending
    last-user-operation  Add
    last-apply-timestamp "Rule not yet applied"
    failure-reason       None
   rule 10030
    status               Apply-Pending
    last-user-operation  Add
    last-apply-timestamp "Rule not yet applied"
    failure-reason       None
    xpath                /config/interface/full-bridge
   cmdrule 10012
    status               Apply-Pending
    last-user-operation  Add
    last-apply-timestamp "Cmdrule not applied yet"
    failure-reason       None
   cmdrule 10025
    status               Apply-Pending
    last-user-operation  Add
    last-apply-timestamp "Cmdrule not applied yet"
    failure-reason       None
```

```
CLX3001(config)#apply rbac-aaa

CLX3001# show rbac-status
rbac-status
group bnc
  rule-list bnc
   rule 10010
    status               Apply-Success
    last-user-operation  Add
    last-apply-timestamp Thu Oct 4 12:01:55 2018
    failure-reason       None
   rule 10020
    status               Apply-Success
    last-user-operation  Add
    last-apply-timestamp Thu Oct 4 12:01:55 2018
    failure-reason       None
   rule 10030
    status               Apply-Success
    last-user-operation  Add
    last-apply-timestamp Thu Oct 4 12:01:55 2018
    failure-reason       None
    xpath                /config/interface/full-bridge
   cmdrule 10012
    status               Apply-Success
    last-user-operation  Add
    last-apply-timestamp Thu Oct 4 12:01:56 2018
    failure-reason       None
   cmdrule 10025
    status               Apply-Success
    last-user-operation  Add
    last-apply-timestamp Thu Oct 4 12:01:56 2018
    failure-reason       None
```

Configuring a TACACS+ Server on the E9-2

This topic describes how to configure a TACACS+ server on the E9-2.

Configuration guidelines

- The E9-2 supports up to four authentication TACACS servers, each with a unique server IP address, and a shared Secret name and port.
- The system initiates communication with first configured server, and then sends the authentication request to the next configured server if it does not get a response.
- Configure the system craft as the source interface. All TACACS+ communication is out of band. The first IP address of the system craft interface will be used as the source IP address for all outbound connections by the application.
- You must connect with the E9-2 via the craft interface.

Parameters

You can configure the following parameters for a TACACS+ server on the E9-2:

Parameter	Description	Valid Options
server*	IP address or DNS domain name of the TACACS+ server.	IPv4 address 0.0.0.0 (default) Domain name
port	TACACS+ server listening port number. This is a TCP or UDP port number.	0-65535 49 (default)
priority	The order in which server can be tried. 1 is the highest priority and 10 is the least priority.	1-10 9 (default)
secret	The "shared secret" for the E9-2 and the TACACS+ server. This mandatory parameter is used to encrypt/decrypt the messages between the E9-2 and TACACS+ server. This string must match the string configured in the TACACS+ server. **Note**: The secret displays in AES-256-CBC encrypted form in the running/startup configuration. In addition to plain text, you can set secrets using encrypted values to support the copy/paste function.	Text string of 16–63 characters, including spaces. **Note**: The system does not support the following special character: !
timeout	Number of seconds to wait for a response from the TACACS+ server before retransmitting or aborting.	1–30 5 (default)

*User input required

Procedure

To configure a TACACS+ server on the E9-2

1. Configure the system craft as the source interface:

```
Calix-1(config)# aaa tacacs source-interface system-craft
```

2. Configure the IP address or DNS domain name of the TACACS+ server, listening port number, priority, shared secret and timeout period:

```
Calix-1(config)# aaa tacacs server <host address|IPv4 address|domain name>
[port <0-65535>] priority <1-10> <secret <string>> [timeout <1-30>]
```

Example:

1. `Calix-1(config)# aaa tacacs source-interface system-craft`
2. `Calix-1(config)# aaa tacacs server 10.1.1.1 port 1900 secret testing123456789 timeout 2`

Configuring a User Account on a TACACS+ Server

This section provides information that describes how to configure a user account on a tac_plus server on Linux. You may perform similar steps on a different type of TACACS+ server; refer to the user documentation.

Overriding the Role Permission from a TACACS+ Server

Certain permissions may be allowed or revoked from a predefined role for a session or for a user by creating another role with required permissions. An easier method is to override the permissions applicable for a user's role on the TACACS+ server by sending permission statements.

A permission statement contains a keyword that specifies the permission type (either allow-permission or deny-permission) followed by a set of rules separated by parenthesis. These rules are interpreted by the E9-2 system in a sequential way with the first rule taking precedence over the following ones. During user authentication and authorization from TACACS+ server, the E9-2 receives the allow-permission/deny-permission attribute along with roles attribute in the authorization response. The E9-2 will apply the allow/deny permission on top of the role defined permissions.

Syntax for Rules

The allow-permission and deny-permission attributes each use the same syntax. Two types of rules that can be specified and are distinguished by the key word "rule" or "cmd-rule".

- A permission statement contains a keyword that specifies the permission type (either allow-permission or deny-permission) followed by a set of rules separated by parenthesis:
  `<permission-type>="(rule1)(rule2)…"`
- One or more cmd-rules and/or rules can be sent in an allow-permission/deny-permission attribute.
- The cmd-rule/rule parameter is the only mandatory parameter in a rule. In the absence of a cmd-rule/rule, the entire parameter inside () is ignored. All other parameters are optional parameters with default values of '*'.
- There can be only one instance or no instances of allow-permission and deny-permission statements in the authorization response.
- Rules are interpreted by the E9-2 in a sequential way with the first rule taking precedence over the following ones.

  Note: When a command is present in both ALLOW-PERMISSION and DENY-PERMISSION arguments, the order of configuration affects what is finally provided to the user. In the following example, the permission for a configure command would be allowed because the ALLOW-PERMISSION argument is entered first.

```
group = oper {
service = Login
{ ROLES=oper ALLOW-PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)" DENY-
PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)" }
}
user = testoper
{ member = oper login = cleartext "testoper" }
```

Rules with the keyword "rule"

A rule with keyword "rule" is used for specifying a entity in the data model for which access control is required. This rule statement has the following syntax.

```
rule;path|rpc-name|notification-name=<object-path>;acc-
oper=<operation>;module-name=<module>;context=<context>
```

Where:

- "object-path" specifies the path of the configuration entity for which the rule is specified
- "operation" specifies the type of operation and can take values "exec", or "read". Multiple operations can be specified with space as the delimiter. A "*" can be used to denote all operations.
- "module" specifies the module under which the object is defined. A module-name is an optional field and the rule applies to all modules by default (same as *) if it is not specified.
- "context" specifies the way the object is accessed. It can take values "cli" or "netconf". A "*" can be used to denote any access method.

Rules with keyword "cmd-rule"

A rule with keyword "cmd-rule" is used for specifying a command string that must be controlled.

```
cmd-rule;cmd=<command-string>;acc-oper=<operation>;module-
name=<module>;context=<access-method>
```

Where:

- "command-string" specifies the command string that has to be controlled by the rule. The validity of command is not checked. A ".*" can be used anywhere in the command to indicate any character.
- "operation" specifies the type of operation and can take values "exec", or "read". Multiple operations can be specified with space as the delimiter. A "*" can be used to denote all operations
- "module" specifies the particular YANG module under which the object is defined. The default is all modules. A "*" can be used to specify any module. Please refer to *Module Names* (on page 198) for a list of YANG module names.
- "context" specifies the way the object is accessed. It can take values "cli" or "netconf". A "*" can be used to denote any access method

Examples

For example, suppose a user has an admin role which gives them permission to update read, create and delete all of the configuration file. To restrict the access only to /config/interface, configure the TACACS+ server to send the roles, allow-permission and deny-permission in the authorization response as follows:

```
group = admin {
service = Login
{ ROLES=admin ALLOW-PERMISSION="(rule;path=/config/interface;module-
name=exa-base)"  DENY-PERMISSION= "(rule;path=/config;acc-
oper=*;module-name=*)"}
}
```

The following example provides a user access to the CLI command "show subscribers" while denying all other show commands (anything starting with "show "). It allows the user to view and modify configuration that is under the path /config/system/aaa while denying access to all other configuration.

```
group = user1 {
service = Login
{ ROLES=user1 ALLOW-PERMISSION="(cmd-rule;cmd=show subscribers;acc-
oper=read exec)(rule;path=/config/system/aaa)"  DENY-
PERMISSION="(cmd-rule;cmd=show .*;acc-oper=read
exec)(rule;path=/config))"}
}
```

Overriding the RBAC Role with the TACACS+ Configuration on the E9-2

If there is a need to override specific rules or cmdrules created by RBAC, you can allow or deny privileges in TACACS+.

When a rule or command rule is allowed or denied in the TACACS+ server configuration, the rule/cmdrule received from the TACACS+ server is added first and then the system provisions and inserts the rule or cmdrule configured through RBAC.

group = <rbac-created-role> {

service = Login

{ ROLES=oper ALLOW-PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)" DENY-PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)"

}

}

This particular change is added first to the role, and then all the existing rules associated with the given role are added.

Sample User Account on a TACACS+ Server

The following example shows how to create a user account on a tac_plus server on Linux. You may perform similar steps on a different type of TACACS+ server; refer to the user documentation for more information.

1. Create a tac_plus.conf file with the following content:

```
key = "testing1234567890"
group = oper {
service = Login

{ ROLES=oper ALLOW-PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)" DENY-PERMISSION="(cmd-rule;cmd=configure;acc-oper=*)" }
}

user = testoper

{ member = oper login = cleartext "testoper" }
```

2. Create the configuration file start/restart for the tac_plus server using the following command:

```
tac_plus -C tac_plus.conf
```

Authentication Request with User Name

The following are the attribute names and values in the authentication request with a user name:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authentication (1)
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session ID	Constant for a session - selected randomly
Packet length	Total length of the packet body not including header
User length	Length of user name
User	User name
Data	0

Authentication Response Asking for Password

The following are the attribute names and values in the authentication response asking for a password:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authentication (1)
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session ID	Constant for a session - selected randomly
Packet length	Total length of the packet body not including header
Status	Send passed (0x05)
Flags	0x01 (NoEcho)
Server message length	10
Server message	Password:
Data Length	0

Authentication Request with Password

The following are the attribute names and values in the authentication response with a password:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authentication (1)
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session ID	Constant for a session - selected randomly
Packet length	Total length of the packet body not including header
User Length	Length of user name
User	User password
Data	0

Authentication Response

The following table shows attribute names and values in the authentication response:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authentication (1)
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session ID	Constant for a session - selected randomly
Packet length	Total length of the packet body not including header
Status	0x00 (Encrypted payload, Multiple Connections)
Flags	0x00 (Encrypted payload, Multiple Connections)
Server message length	0
Data length	0

Authorization Request

The following are the attribute names and values in the authorization request:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authorization(2)

Attribute Name	Value
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session id	constant for a session - selected randomly
Packet length	Length of packet
Auth method	TACACSPLUS (0x06)
Privilege level	0
Authentication Type	ASCII (1)
Service	Login (1)
User len	Length of username
User	User name
Port len	Port length
Port	client port on which auth is taking place
Remaddr len	Remote address length
Remote address	Remote address
Arg count	Argument count
Arg[0] len	Argument length
Arg[0] value	Argument

Authorization Response

The following are the attribute names and values in the authorization response:

Attribute Name	Value
Major Version	TACACS+
Minor Version	0
Type	Authentication (1)
Sequence number	Monotonically increasing sequence number per session starting at 1
Flags	0x00 (Encrypted payload, Multiple Connections)
Session ID	Constant for a session - selected randomly
Packet length	Total length of the packet body not including header
Auth status	Pass_add (0x01)
Server message length	0
Data length	0
Arg count	3
Arg [0] length	Length of argument
Arg[0] value	Vendor defined attribute – "ROLES" used to assign roles to the user. Example: ROLES=admin
Arg[1] length	Length of argument
Arg[1] value	Vendor defined attribute ALLOW-PERMISSION
Arg[2] length	Length of argument
Arg[2] value	Vendor defined attribute DENY-PERMISSION

Module Names

A module-name indicates the name of the YANG module a rule applies to. A module-name is an optional field and the rule applies to all modules by default (same as *) if it is not specified. The module name is not required if the rule is to be applied on a particular RPC, config or notification across the system.

Possible values are

- exa-base
- bbf-fast
- bng
- tailf-common
- bbf-fast-common
- tailf-aaa
- ietf-netconf-acm
- tailf-webui
- ietf-netconf-monitoring
- tailf-confd-monitoring
- *

RPC Names

The rpc-name indicates the name of the RPC.

Alarm RPCs:

- show-event-definitions-subscope
- show-event-definitions-address
- show-event-instances-subscope
- show-event-instances-filter
- show-event-instances-log
- show-event-instances-address
- show-event-instances-range
- show-event-instances-timerange
- show-event-archive-detail
- show-event-archive-subscope
- show-event-archive-filter
- show-event-archive-log
- show-event-archive-address

- show-event-archive-instance-range
- show-event-archive-timerange
- show-alarm-definitions-subscope
- show-alarm-definitions-address
- show-alarm-instances-active-subscope
- show-alarm-instances-active-address
- show-alarm-instances-active-range
- show-alarm-instances-active-timerange
- show-alarm-instances-history-subscope
- show-alarm-instances-history-filter
- show-alarm-instances-history-log
- show-alarm-instances-history-address
- show-alarm-instances-history-range
- show-alarm-instances-history-timerange
- show-alarm-instances-archive-subscope
- show-alarm-instances-archive-filter
- show-alarm-instances-archive-address
- show-alarm-instances-archive-instance-range
- show-alarm-instances-archive-timerange
- show-alarm-instances-archive-log
- show-alarm-instances-suppressed-subscope
- show-alarm-instances-suppressed-address
- show-alarm-instances-suppressed-range
- show-alarm-instances-suppressed-timerange
- manual-shelve
- manual-un-shelve
- manual-acknowledge
- active-event-log
- active-alarm-log
- archive-event-log
- archive-alarm-log

Configuration-management RPCs:

- copy-running-startup
- copy-startup-running
- copy-configuration
- copy
- accept-running-config
- replay-card-config
- lock-rpc
- lock-rpc
- unlock-rpc
- unlock-rpc

DHCP Server RPCs:

- clear-dhcp-server-statistics
- clear-subscriber-context-id
- clear-subscriber-ip-address
- clear-subscriber-pool
- clear-subscriber-profile

Diagnostic RPCs:

- cancel-diagnostic
- show-diagnostic-test-status

Diameter RPCs:

- show-diameter-profile-detail
- show-diameter-peer-detail
- diameter-restart

Equipment RPCs:

- switchover
- force-switchover
- redundancy-autoswitchover-enable
- redundancy-autoswitchover-disable
- stop-reload
- reload

ERPS RPC:

- erps-clear-counters

Ethernet Interface RPC:

- show-interface-ethernet-performance-monitoring-rmon-session

IETF NETCONF Monitoring RPC:

- get-schema

IETF NETCONF RPCs:

- get-schema
- get-config
- edit-config
- copy-config
- delete-config
- lock
- unlock
- get
- close-session
- kill-session
- commit
- discard-changes
- cancel-commit
- validate

LAG Interface RPCs:

- clear-interface-slot-lag-counters
- clear-interface-slot-lag-performance-monitoring-rmon-session

Logging RPCs:

- generate-techlog
- stop-techlog
- delete-config-file
- delete-core-file
- delete-techlog-file
- stop-transfer
- upload-loghistory-file
- download-config-file
- upload-config-file
- upload-core-file
- upload-syslog-file
- upload-techlog-file
- upload-post-results-file
- upload-diagnostic-results-file
- diff-config-file
- loghistory-file-contents
- config-file-contents
- core-file-contents
- syslog-file-contents
- post-results-file-contents
- diagnostic-results-file-contents
- techlog-recent-file-contents

ONT Upgrade RPCs:

- ont-install
- ont-download
- ont-activate
- ont-commit
- ont-test-download
- ont-test-activate
- ont-test-commit
- ont-cancel
- ont-revert
- config-file-cancel
- config-file-retrieve
- config-file-remove
- config-file-apply
- retry-remote-retrieval

Routing RPCs:

- clear_all_arp_entries
- clear_spec_arp_entry
- clear_arp_on_ethernet
- clear_arp_on_vlan
- clear_arp_on_multibind
- clear_arp_on_lag

Secondary Index RPCs:

- show-event-definitions-subscope
- show-event-definitions-address
- show-event-instances-subscope
- show-event-instances-filter
- show-event-instances-log
- show-event-instances-address
- show-event-instances-range
- show-event-instances-timerange
- show-event-archive-detail
- show-event-archive-subscope
- show-event-archive-filter

- show-event-archive-log
- show-event-archive-address
- show-event-archive-instance-range
- show-event-archive-timerange
- show-alarm-definitions-subscope
- show-alarm-definitions-address
- show-alarm-instances-active-subscope
- show-alarm-instances-active-range
- show-alarm-instances-active-timerange
- show-alarm-instances-history-subscope
- show-alarm-instances-history-filter
- show-alarm-instances-history-log
- show-alarm-instances-history-range
- show-alarm-instances-history-timerange
- show-alarm-instances-archive-subscope
- show-alarm-instances-archive-filter
- show-alarm-instances-archive-instance-range
- show-alarm-instances-archive-timerange
- show-alarm-instances-archive-log
- show-alarm-instances-suppressed-subscope
- show-alarm-instances-suppressed-range
- show-alarm-instances-suppressed-timerange
- manual-shelve
- manual-un-shelve

Timing RPCs:

- switch_network_clock_manual
- switch_network_clock_force
- clear_network_clock_override
- network_clock_ssm_force_ql_set
- network_clock_ssm_force_ql_clear
- network_clock_synce_primary_force_ql_set
- network_clock_synce_primary_force_ql_clear
- network_clock_synce_secondary_force_ql_set
- network_clock_synce_secondary_force_ql_clear

Upgrade RPCs:

- cancel
- download
- activate
- deactivate
- switch
- package-info

User Agents RPCs:

- generate-ssl-certificate
- clear_snmp_statistics

Viewing Information About the TACACS+ Server (E9-2)

Issue the CLI command **show aaa tacacs** on the E9-2 to display status and statistics for configured TACACS+ server.

For example:

```
Calix-1# show aaa tacacs
aaa tacacs
server 10.243.250.183
authentication-requests-tx 12
authentication-responses-rx 12
authentication-error 4
authorization-requests-tx 4
authorization-responses-rx 4
authorization-error 0
accounting-requests-tx 0
accounting-responses-rx 0
accounting-error 0
status secret-invalid
```

Field	Description
server <IP address>	IP address of the TACACS+ server
authentication-requests-tx	Authentication request sent to TACACS+ server
authentication-responses-rx	Authentication response received from the TACACS+ server
authentication-error	Error or invalid message received from the server for authentication request.
authorization-requests-tx	Authorization request sent to TACACS+ server.
authorization-responses-rx	Authorization response received from the TACACS+ server.
accounting-requests-tx	Accounting request sent to TACACS+ server.
accounting-responses-rx	Accounting response received from the TACACS+ server.
accounting-error	Error or invalid message received from the server for accounting request. status [unknown, up, down]: Status of the TACACS+ server.
status	Status of the TACACS+ server (unknown, up, down)

.

Chapter 9

Configuring the System for Remote Management

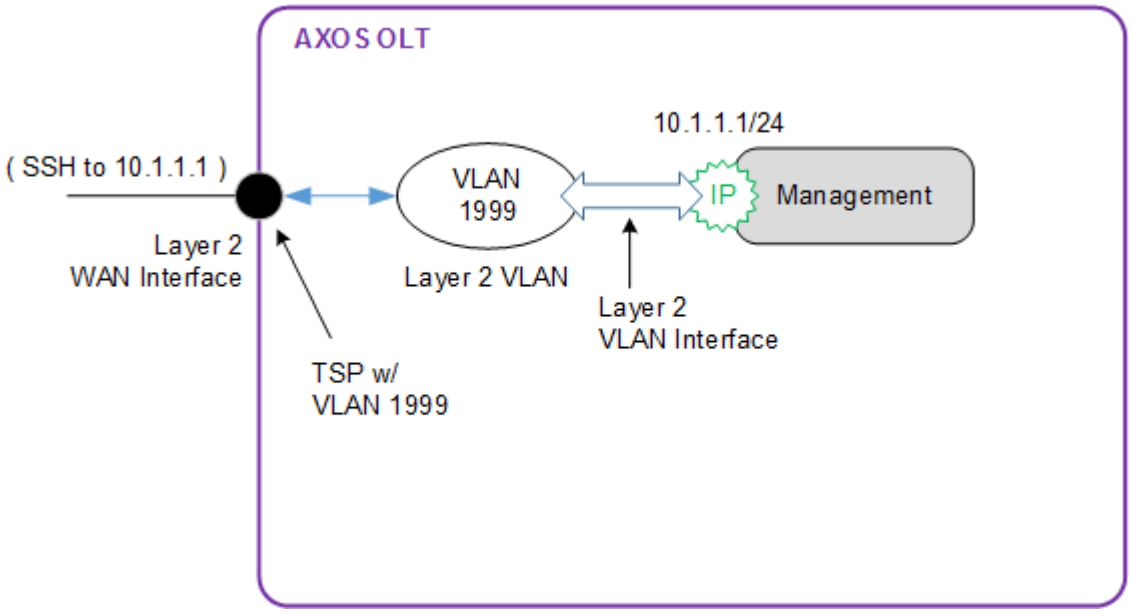
This chapter describes how to configure the AXOS system to support remote management, via an existing uplink interface or via a permanent out-of-band connection.

Configuring Layer 2 In-Band Management

This topic describes how to configure Layer 2 in-band management.

Layer 2 in-band management provides IP-based management control over a Layer 2 infrastructure; the supporting AXOS system configuration is comprised of the following elements:

- Layer 2 VLAN for management
- VLAN interface (for the above VLAN) with the following:
  - IP interface using static or DHCP addressing
  - (optional) access-list
  - (optional) cosq-profile
- Layer 2 uplink with TSP that includes the management VLAN



Configuration guidelines

- Some AXOS systems are pre-configured to support Layer 2 in-band management (as shown below); for such systems, the default configuration may be modified or replaced with another configuration to support your deployment.
  - Default management VLAN (999)
  - Default VLAN interface (999) with an IP interface ready for assignment (via DHCP)
  - Layer 2 single-port uplink (1/1/x1) with the default SYSTEM_TSP containing the default management VLAN (999)
- The PCP value for in-band management traffic is automatically set to 3.
- With static IP addressing, if the host (establishing management sessions) is on a different subnet, configuring a default route is required. For example:

```
Calix-1(config)# ip route 0.0.0.0/0 next-hop 10.1.1.254
```

Related topics

- *Creating and Modifying Transport Service Profiles* (on page 292)

Configuration process (new configuration)

This configuration consists of the following steps:

1. (If applicable) Delete the following default in-band management elements:
   - VLAN 999
   - VLAN interface 999
2. Create a new Layer 2 management VLAN.
3. Create a new TSP that contains the new management VLAN, and apply it to your Layer 2 uplink.
4. (Optional) Configure an access list to apply to the interface.

   Note: The access list may be created with or without cpu-cosq actions (to rate limit specific traffic to the CPU). If created with cpu-cosq actions, a supporting cosq-profile must also be created.
5. Create a new VLAN interface for the new management VLAN.
6. Configure an IP address on the interface.
7. (Optional) Add an access list to the interface.
8. (Optional) Add a cosq profile to the interface.
9. (If using static addressing) Configure a default route.

Example 1

```
!!Delete VLAN 999 and its associated VLAN interface
no interface vlan 999
no vlan 999
top

!!Create a new Layer 2 management VLAN
vlan 1999
top

!!Create/modify your TSP to add the new VLAN
transport-service-profile TSP_L2-Triple-UL
vlan-list 1999
top

!!Create a new VLAN interface for the above VLAN
interface vlan 1999
ip address 10.1.1.1/24
no shutdown
top

!!Configure a default route
ip route 0.0.0.0/0 next-hop 10.1.1.254
top
```

Example 2 (E7-2, with access list, without cosq-profile)

```
!!steps 1-3 not shown

ip prefix-list SSH_pre1
 seq 1 192.168.37.0/24
 seq 2 192.168.38.0/24
!

ip prefix-list SSH_pre2
 seq 1 10.245.51.0/24
!

access-list ipv4 acl_ipv4_mgmt1
 rule 10 description ICMP
 rule 10 match protocol ICMP
 rule 10 action permit count
 rule 20 description "Trace Route"
 rule 20 match protocol UDP destination-port-range 33434-33523
 rule 20 action permit count
 rule 30 description SSH
 rule 30 match source-ipv4-prefix-list SSH_pre1 protocol TCP
destination-port-range 22
 rule 30 action permit count
```

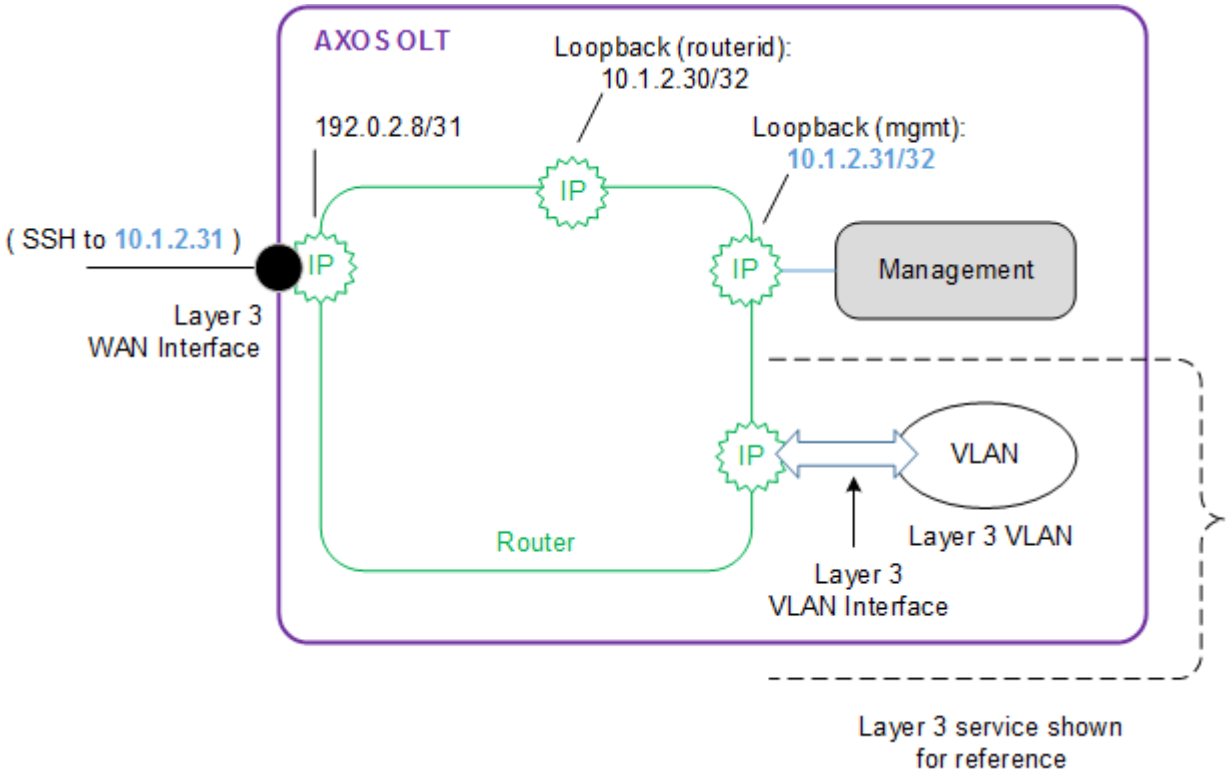
```
 rule 40 description SSH2
 rule 40 match source-ipv4-prefix-list SSH_pre2 protocol TCP
destination-port-range 22
 rule 40 action permit count
 rule 50 description RADIUS
 rule 50 match protocol UDP source-port-range 1812-1813
 rule 50 action permit count
 rule 60 description NETCONF
 rule 60 match protocol TCP destination-port-range 830
 rule 60 action permit count
 rule 70 description IPFIX
 rule 70 match protocol TCP tracking-state [ ESTABLISHED NEW ]
source-port-range 4729
 rule 70 action permit count
 rule 80 description "SSH from 10.245.28.0"
 rule 80 match source-ipv4-network 10.245.28.0/24 protocol TCP
destination-port-range 22
 rule 80 action deny
 rule 90 description NTP
 rule 90 match protocol UDP destination-port-range 123
 rule 90 action permit count
 rule 100 description DNS
 rule 100 match protocol UDP source-port-range 53
 rule 100 action permit count
 rule 110 match protocol TCP destination-port-range 22
 rule 110 action permit count
 rule 250 description "All other traffic"
 rule 250 match any
 rule 250 action deny count
!

interface vlan 1999
 access-group ipv4-acl acl_ipv4_mgmt1
 ip address 10.245.51.139/24
 no shutdown
!
```

Example 3 (E7-2, with access list and cosq-profile)

```
!!steps 1-3 not shown

cos cosq-profile cpu_acl_1
 cosq-entry 1
  bandwidth maximum 100
 !
 cosq-entry 2
  bandwidth maximum 10000

access-list ipv4 acl_ipv4_cpu_cos
 rule 10 description ICMP
 rule 10 match protocol ICMP
 rule 10 action cpu-cosq 1
 rule 20 description "Trace Route"
 rule 20 match protocol UDP destination-port-range 33434-33523
 rule 20 action permit cpu-cosq 1 count
 rule 30 description SSH
 rule 30 match source-ipv4-prefix-list SSH_pre1 protocol TCP
tracking-state [ ESTABLISHED ] destination-port-range 22
 rule 30 action cpu-cosq 2
 rule 250 description "All other traffic"
 rule 250 match any
 rule 250 action deny count
!

interface vlan 1999
 access-group ipv4-acl acl_ipv4_cpu_cos
 cosq     cpu_acl_1
 ip dhcp server disable
 ip address 10.245.51.118/24
 no shutdown
!
```

Configuring Layer 3 In-Band Management

Layer 3 in-band management provides IP-based management control over a routed WAN Ethernet interface, where no VLANs are associated with the interface. This section describes how to configure Layer 3 in-band management.



Configuration guidelines

- Layer 3 in-band management consists of the following elements:
  - Layer 3 (routed) uplink
  - Loopback interface dedicated for management

Configuration process

This configuration consists of the following steps:

Note: This process assumes that a Layer 3 uplink for your deployment has been configured.

1. Create a loopback interface for management.
2. Configure management traffic (for example, SSH) to use the loopback interface as the source address for packets.
3. Ensure that the path to the loopback interface is known by all routers between your PC and the system (via dynamic protocols or static routes).
4. Ensure that the MTU setting of the Layer 3 uplink WAN interface(s) and all other router Ethernet interfaces are consistent and set to a minimum of 2000 bytes (default value for the system).

Example

```
Calix-1(config)# interface loopback mgmt
Calix-1(config-loopback-mgmt)# ip address 10.1.2.31/32
Calix-1(config-loopback-mgmt)# no shutdown
Calix-1(config-loopback-mgmt)# exit
Calix-1(config)# ssh interface mgmt
```

Configuring Out-of-Band Management (E7-2)

Note: This section only applies to the E7-2.

You may configure the MGT-3 interface (RJ-45 jack on the E7-2 rear panel) to provide a permanent out-of-band management connection.

Configuration guidelines

- If both the front and rear Ethernet management ports are both enabled, their IP addresses must belong to different subnets. Also, the craft management ports cannot use IP addresses from the same subnet where DHCP Snooping is enabled.
- The OOB next hop address is added with a conventional static route (since there is no configurable gateway field for craft ports). For example:

```
ip route 0.0.0.0/0 next-hop 11.209.252.1
```

Procedure

1. (Optional) Configure an access list to apply to the interface.

   Note: The access list may be created with or without cpu-cosq actions (to rate limit specific traffic to the CPU). If created with cpu-cosq actions, a supporting cosq-profile must also be created.

2. Configure an IP address on the interface.
3. (Optional) Add an access list to the interface.
4. (Optional) Add a cosq profile to the interface.
5. Configure other features as desired, such as the built-in DHCP server (disabled by default).
6. Enable the interface.

Example 1

```
interface craft 2
ip address 10.20.30.1/24
no shutdown
top
```

Example 2 (with access list, without cosq-profile)

```
ip prefix-list SSH_pre1
 seq 1 192.168.37.0/24
 seq 2 192.168.38.0/24
!

ip prefix-list SSH_pre2
 seq 1 10.245.51.0/24
!
```

```
access-list ipv4 acl_ipv4_mgmt1
 rule 10 description ICMP
 rule 10 match protocol ICMP
 rule 10 action permit count
 rule 20 description "Trace Route"
 rule 20 match protocol UDP destination-port-range 33434-33523
 rule 20 action permit count
 rule 30 description SSH
 rule 30 match source-ipv4-prefix-list SSH_pre1 protocol TCP
destination-port-range 22
 rule 30 action permit count
 rule 40 description SSH2
 rule 40 match source-ipv4-prefix-list SSH_pre2 protocol TCP
destination-port-range 22
 rule 40 action permit count
 rule 50 description RADIUS
 rule 50 match protocol UDP source-port-range 1812-1813
 rule 50 action permit count
 rule 60 description NETCONF
 rule 60 match protocol TCP destination-port-range 830
 rule 60 action permit count
 rule 70 description IPFIX
 rule 70 match protocol TCP tracking-state [ ESTABLISHED NEW ]
source-port-range 4729
 rule 70 action permit count
 rule 80 description "SSH from 10.245.28.0"
 rule 80 match source-ipv4-network 10.245.28.0/24 protocol TCP
destination-port-range 22
 rule 80 action deny
 rule 90 description NTP
 rule 90 match protocol UDP destination-port-range 123
 rule 90 action permit count
 rule 100 description DNS
 rule 100 match protocol UDP source-port-range 53
 rule 100 action permit count
 rule 110 match protocol TCP destination-port-range 22
 rule 110 action permit count
 rule 250 description "All other traffic"
 rule 250 match any
 rule 250 action deny count
!

interface craft 2
 access-group acl_ipv4_mgmt1
 ip dhcp server disable
 ip address 10.245.51.118/24
 no shutdown
!
```

Example 3 (with access list and cosq-profile)

```
cos cosq-profile cpu_acl_1
 cosq-entry 1
  bandwidth maximum 100
 !
 cosq-entry 2
  bandwidth maximum 10000

access-list ipv4 acl_ipv4_cpu_cos
 rule 10 description ICMP
 rule 10 match protocol ICMP
 rule 10 action cpu-cosq 1
 rule 20 description "Trace Route"
 rule 20 match protocol UDP destination-port-range 33434-33523
 rule 20 action permit cpu-cosq 1 count
 rule 30 description SSH
 rule 30 match source-ipv4-prefix-list SSH_pre1 protocol TCP
tracking-state [ ESTABLISHED ] destination-port-range 22
 rule 30 action cpu-cosq 2
 rule 250 description "All other traffic"
 rule 250 match any
 rule 250 action deny count
!

interface craft 2
 access-group ipv4-acl acl_ipv4_cpu_cos
 cosq     cpu_acl_1
 ip dhcp server disable
 ip address 10.245.51.118/24
 no shutdown
!
```

Parameters

You can configure the following parameter values for the "craft 2" interface:

Note: The following table covers both front and rear craft ports.

Parameter	Description
interface craft {1|2}	Specifies the craft interface index. Valid values: • craft 1 (MGT-1) • craft 2 (MGT-3, E7-2 rear panel)
access-group ipv4-acl	(E7-2 only) Valid values: • <valid IPv4 access list>

Parameter	Description
cosq	(E7-2 only) Valid values: • <cosq profile >
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. Valid values: • dhcp • <IP address>/<mask> Craft 1 default = 192.168.1.1; craft 2 default = 192.168.1.2. If you change the factory default address, the current value becomes the default.
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable (default for craft 1) • disable (default for craft 2) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)
ipv6 address	Valid values: • <IPv6 address>
ipv6 redirects	Valid values: • true (default) • false
ipv6 unreachables	Valid values: • true (default) • false
shutdown	Administrative state of the craft management port. Valid values: • no shutdown (default for craft 1) • shutdown (default for craft 2)

Configuring Out-of-Band System Management (E9-2)

The E9-2 requires the following interfaces for out-of-band (OOB) system management:

- A logical system-craft interface, with a single system IP address for remote connectivity. The system-craft interface's IP address requires a mask.
- A physical rear-craft port on each of the aggregation cards to route packets from the logical system-craft interface, and provide fixed OOB connections for use in a troubleshooting, and so forth. The IP addresses for these interfaces must be in the same subnet.

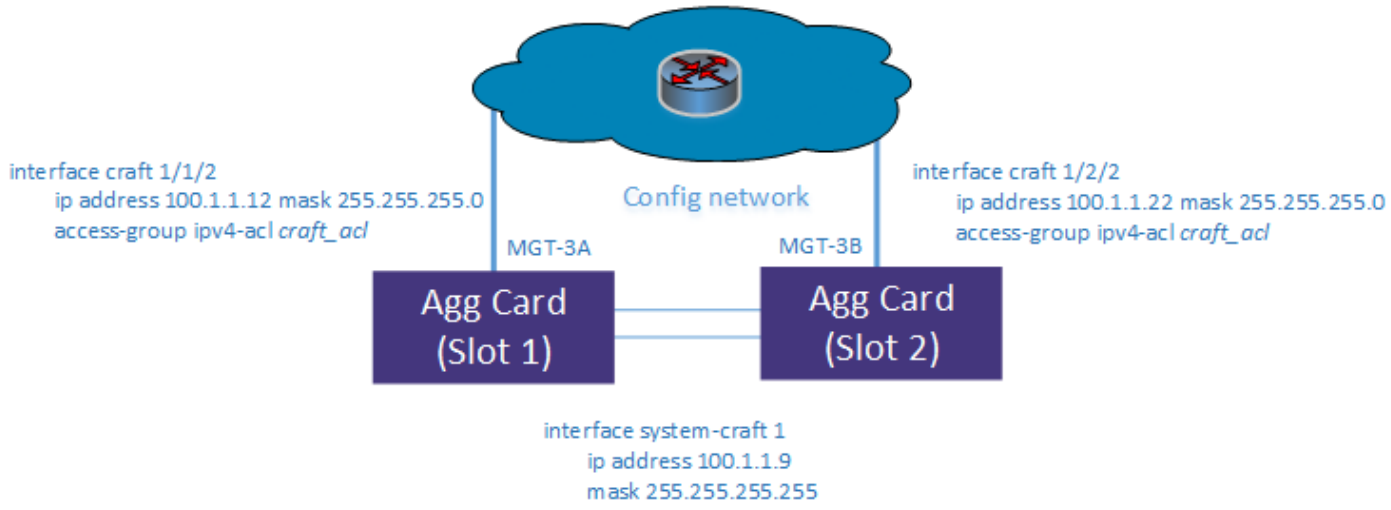
You can apply an optional access control list (ACL) to the rear craft interfaces, restricting access to a specific set hosts or networks.

When connected to the E9-2 system through the system-craft interface, all configuration takes place on the active aggregation card and is replicated on the standby aggregation card. In the case of a system failover, the system-craft interface follows the switchover to the new active aggregation card.

Configuring OOB system management consists of the following basic steps:

1. (Optional) Creating a VRF for management
2. (Optional) *Creating an ACL for OOB Management* (on page 225)
3. *Configuring the system-craft interface* (on page 223).
4. *Configuring the rear craft interfaces* (on page 228).
5. Verifying OOB management configurations.

Example:



Note: After configuring OOB system management, Calix recommends shutting down the front craft ports on the aggregation cards.

Configuring the System-Craft Interface

This topic describes how to configure the logical system-craft interface for remote OOB craft connectivity.

Configuration guidelines

- The system-craft subnet mask must be in the same subnet as the rear craft interfaces (1/X/2); Calix recommends using subnet mask 225.225.255.255 (/32 in cidr notation) for the system-craft interface.
- Only one default route is allowed on E9-2 system. When Border Gateway Protocol (BGP) is enabled, a default route is given to the E9 from the routers. Calix recommends that you configure static routes for the management network to avoid overwriting the default route learned via BGP.
- After configuring OOB management (including rear craft interfaces), all CLI configuration may be done from the system-craft.
- The OOB next hop address is added with a conventional static route (since there is no configurable gateway field for craft ports). See *Configuring Static Routes* (on page 236) for more information.

Procedure

To configure the system-craft interface

1. Connect to a local management port on the active aggregation card, and log into the CLI.
2. Specify craft interface index 1.

```
calix-1(config)# interface system-craft 1
```

3. (Recommended) Verify that the DHCP server is disabled.

```
calix-1(config-system-craft-1)# ip dhcp server disable
```

4. Configure an IP address and mask for the interface.

```
calix-1(config-system-craft-1)# ip vrf forwarding <management VRF
name> !!optional, recommended step
calix-1(config-system-craft-1)# ip address <x.x.x.x>/<mask in cidr
notation>
```

Example

```
!
interface system-craft 1
ip dhcp server disable
ip address 10.1.1.9/32
no shutdown
!
```

Parameters

You can configure the following parameter values for the "system-craft 1" interface:

Parameter	Description
interface system-craft <index>	System Logical Craft Port
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. (default 0.0.0.0/0) Valid values: • dhcp • <IP address>/<mask>
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable • disable (default) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)
ip vrf forwarding ip vrf forwarding ipv6 address	Associates a VRF with the interface Valid options: • <VRF name> • ipv6-address: The list of configured IPv6 addresses on the interface
ipv6	Craft interface IPv6 address and vrf configuration Valid values: • address: The list of configured IPv6 addresses on the interface • redirects: Enable or disable the processing of ICMPv6 redirects Valid values: • true (default) • false • unreachables: Enable or disable the transmission of ICMPv6 unreachables Valid values: • true(default) • false
shutdown	Administrative state of the craft management port. Valid values: • no shutdown • shutdown

Creating an ACL for OOB Management

This topic describes how to create an ACL to filter packets on the rear craft interfaces, restricting access to the management interfaces from a specific host or network.

Configuration guidelines

- IPv6 and IPv4 ACLs are supported.
- Apply the same or meaningful ACL to both rear craft interfaces.
- The ACL on the uplink is used to block unwanted ingress traffic.
- For valid match rules, see below; match rules not listed in the table are not supported.
- For matching packets, the ACL can count, deny, or permit.
- If a packet does not match any rule, it will be denied (or dropped). An implicit, non-configured drop rule is used for this and takes effect when applied to the craft interface. The drop rule is identified by sequence number 65535 when viewing statistics. Removing the ACL from the interface removes the drop rule.
- When applied to the rear craft interface, the ACL does not support specifying a CoS queue.

Parameters

You can configure *only* the following parameters and valid options when creating an IPv4 ACL for OOB management:

Note: Parameters and values not listed in the table are not supported, and may raise an error message when the ACL is applied to the rear craft interface.

Parameter	Description	Valid Options
access-list	Specifies the type of ACL.	ipv4
name	A unique name for the ACL.	A string up to 48 characters including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot)
description	A description of the access list.	A string of up to 48 characters
rule	Sets a sequence number for the rule, and adds the rule to the ACL. Note: ACL rules are evaluated in the order entered into the system.	1–128
description	A description for the specified rule number.	A string of up to 255 characters

Parameter	Description	Valid Options
action	Action to perform when the traffic flow matches the associated rule. Valid values: • count: Count packets (optional action, valid alone or with deny or permit) • deny: Drop matching packets • permit: Pass matching packets	count deny permit
match <keyword>	Per rule number match criteria	
any	Matches all packets.	N/A
destination-ipv4-network	Matches a destination IPv4 address and prefix. IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each	Syntax: <ip address/prefix> IPv4 prefix: 0–32
destination-ipv4-prefix-list	Matches an IPv4 prefix list receiving the packet.	Name of any previously configured IPv4 prefix list
destination-port-range	Specifies the destination TCP/UDP port(s) to match as a range or as a single value. Service names and port numbers distinguish different services that run over transport protocols, such as TCP and UDP. Refer to the IANA transport protocol port number registry for more information (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1).	1–65535 Press the tab key twice to display well-known IP protocol transport port enumerations and values.
protocol	Specifies the Internet protocol enumeration or number in an IPv4 packet header to match.	ANY ICMP (1) TCP (6) UDP (17)
source-ipv4-network	Matches the source IPv4 address and prefix. IPv4 format: x.x.x.x, where x is a decimal integer, ranging from 0 to 255 each	Syntax: <ip address/prefix> IPv4 prefix: 0–32
source-ipv4-prefix-list	Matches an IPv4 prefix list sending the packet.	Name of any previously configured IPv4 prefix list
source-port-range	Specifies the lower/upper boundary of the source TCP/UDP ports to match as a range or as a single value. Refer to the IANA transport protocol port number registry for more information (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1).	1–65535 Press the tab key twice to display well-known IP protocol transport port enumerations and values.

* User input required.

Procedure

To create an IPv4 access list

1. Specify ACL type 'IPv4' and a name.
   ```
   Calix-1 (config)# access-list ipv4 name
   ```
2. (Optional) Enter a brief description for the ACL.
   ```
   Calix-1 (config-ipv4-name)# description <string>
   ```
3. Specify a sequence number and optional description for the rule.
   ```
   Calix-1 (config-ipv4-name)# rule 1 description <string>
   ```
4. Specify match criteria for the rule.
   ```
   Calix-1 (config-ipv4-name)# rule 1 match <matching criteria>
   ```
5. Specify the action to perform.
   ```
   Calix-1 (config-ipv4-name)# rule 1 action {count|deny|permit}
   ```

Example

```
!
access-list ipv4 OOB_INGRESS
description "Management Plane - OOB - Craft - Ingress ACL"
rule 10 description ALLOW_ICMP
rule 10 match protocol ICMP
rule 10 action permit count
!
rule 20 description SSH
rule 20 match protocol UDP destination-port-range 22
rule 20 action permit count
!
!
!
rule 250 description DENY-ALL
rule 250 match any
rule 250 action deny count
!
```

Related topic

- Configuring IPv4 Prefix Lists

Configuring the Rear Craft Interfaces

This topic describes how to configure the two (2) rear-craft interfaces (one on each aggregation card) for OOB system management. The rear-craft interfaces forward packets from the logical system-craft interface, and provide fixed OOB connections for use in a troubleshooting, and so forth.

Configuration guidelines

- From the CLI, the rear-craft ports are identified by a "2" in the format shelf/slot/port, and assigned as follows:
  - Aggregation card in slot 1 (bottom): rear craft 1/1/**2** (labeled MGT-3A)
  - Aggregation card in slot 2 (top): rear craft 1/2/**2** (labeled MGT-3B)

  Note: The rear craft ports on access shelves are not used.
- The rear-craft 1/x/2 IP addresses must be in the same subnet.
- Calix recommends using static routes for the management network to avoid overwriting default routes learned via BGP.
- For additional security and routing separation, Calix recommends using a VRF for management.
- Calix recommends that both rear-craft interfaces connect to the same management switch.

Procedure

To configure a rear-craft interface

1. Specify a craft interface port (either 1/1/2 or 1/2/2;shown as 1/x/2, below).

   ```
   Calix-1(config)# interface craft 1/x/2
   ```

2. Verify that the DHCP server is disabled.

   ```
   calix-1(config-craft-1/x/2)# ip dhcp server disable
   ```

3. Configure an IP address and mask for the interface.

   ```
   Calix-1(config-craft-1/x/2)# ip vrf forwarding <management VRF name>
   !!optional, recommended step
   Calix-1(config-craft-1/x/2)# ip address <x.x.x.x>/<mask in cidr
   notation>
   ```

4. (Optional) Apply the previously configured ACL to the interface.

   ```
   Calix-1(config-craft-1/x/2)# access-group ipv4-acl <name>
   ```

   Note: The ACL is validated when applied to the interface.

Example

This example shows an ACL configuration and how the ACL is applied to craft interfaces.

Access List configuration

```
access-list ipv4 CRAFT_INTERFACE_CONTROL
 description "Control Plane Filter IPv4"
 rule 30 description "SSH to AXOS"
 rule 30 match source-ipv4-prefix-list SSH_CONFIG_SERVERS_OOB_IPV4
protocol TCP destination-port-range 22
 rule 30 action permit count
 rule 40 description Netconf
 rule 40 match source-ipv4-prefix-list
NETCONF_CONFIG_SERVERS_OOB_IPV4 protocol TCP destination-port-range
830
 rule 40 action permit count
 rule 50 description TACACS
 rule 50 match source-ipv4-prefix-list TACACS_SERVERS protocol TCP
source-port-range 49
 rule 50 action permit count
 rule 60 description SYSLOG
 rule 60 match source-ipv4-prefix-list SYSLOG_SERVERS protocol TCP
source-port-range 5343-5344
 rule 60 action permit count
 rule 70 description IPFIX
 rule 70 match source-ipv4-prefix-list IPFIX_SERVERS protocol TCP
source-port-range 4739
 rule 70 action permit count
 rule 80 description SFTP
 rule 80 match source-ipv4-prefix-list SFTP_SERVERS protocol TCP
destination-port-range 22
 rule 80 action permit count
 rule 90 description NTP
 rule 90 match source-ipv4-prefix-list NTP_SOURCES_MGMT protocol UDP
destination-port-range 123
 rule 90 action permit count
 rule 128 description "All other traffic"
 rule 128 match any
 rule 128 action deny count
!
```

ACL applied to craft interfaces

Note that the ACL is applied to the actual craft interfaces, not the system craft interface.

```
ip vrf MGMT_VRF
!

interface system-craft 1
 ip dhcp server disable
 ip vrf forwarding MGMT_VRF
  ip address 10.201.33.131/32
 !
 no shutdown
!

interface craft 1/1/2
 access-group ipv4-acl CRAFT_INTERFACE_CONTROL
 ip dhcp server disable
 ip vrf forwarding MGMT_VRF
  ip address 10.201.33.137/22
 !
 no shutdown
!

interface craft 1/2/2
 access-group ipv4-acl CRAFT_INTERFACE_CONTROL
 ip dhcp server disable
 ip vrf forwarding MGMT_VRF
  ip address 10.201.33.138/22
 !
 no shutdown
!
```

Parameters

You can configure the following parameter values for the rear "craft 1/x/2" interface of the E9-2 aggregation shelf:

Note: The following table covers both front and rear craft ports.

Parameter	Description
interface craft <shelf>/<slot>/<port>	Specifies the craft interface index. For example, 1/1/1. Valid values: • 1/x/1: located on the faceplate, labeled MGT-1 • 1/x/2: located on the shelf rear, labeled MGT-3A or MGT-3B An aggregation shelf supports one 'system-craft 1' port, which is logical port that rides over a pair of back craft ports (to route packets from the logical interfaced). Each access line card supports a 'craft 1' port located on the rear of the shelf, labeled MGT-3A or MGT-3B.
access-group	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates an access list with the interface Valid options: • ipv4-acl: Apply an Ipv4 Access Control List • ipv6-acl: Apply an Ipv6 Access Control List
cosq	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates a cosq profile with the interface Valid options: • <profile name>
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. Valid values: • dhcp • <IP address>/<mask> • (1/x/1 default = 0.0.0.0/0)
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable • disable • (craft 1/x/1 default = enable) • (all other craft ports default = disable) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)

Parameter	Description
ip gateway	(Only present for E9-2 access shelves craft x/y/1; not aggregation shelves.) Default gateway IP address. Valid values: • <IP address> (default = 0.0.0.0) • <fully qualified domain name, 1–253 alpha numeric characters>
ip vrf forwarding ip vrf forwarding ipv6 address	Associates a VRF with the interface Valid options: • <VRF name> • ipv6-address: The list of configured IPv6 addresses on the interface
ipv6	Craft interface IPv6 address and vrf configuration Valid values: • address: The list of configured IPv6 addresses on the interface • redirects: Enable or disable the processing of ICMPv6 redirects Valid values: • true (default) • false • unreachables: Enable or disable the transmission of ICMPv6 unreachables Valid values: • true(default) • false
mtu	Interface maximum transmission unit Valid value: • 1500-9600
shutdown	Administrative state of the craft management port. Valid values: • no shutdown • shutdown • (craft 1/x/1 default = no shutdown) • (all other craft ports default = shutdown)

Management Plane Protection

This topic describes how to add a COSQ profile to the craft rear interface. This feature allows you to meter specific ingress flows on the OOB management interface; all traffic is destined for the craft IP address.

Note: This feature provides meter support only. It is not supported for front craft or system-craft interfaces. Scheduling/shaping is not supported.

Configuration guideline

If the ACL defines a match action for permitted without referencing a CoSQ profile, then matching packets won't be metered.

Procedure

1. Configure an access list to apply to the craft rear interface (see *Creating an ACL for OOB Management* (on page 225) for details).

   Note: A supporting CoSQ profile must also be created.

2. Configure an IP address on the interface.
3. Add an access list to the interface.
4. Add a CoSQ profile to the interface.
5. Configure other features as desired, such as the built-in DHCP server (disabled by default).
6. Enable the interface.

Example

```
cos cosq-profile cpu_acl_1
 cosq-entry 1
  bandwidth maximum 100
 !
 cosq-entry 2
  bandwidth maximum 10000

access-list ipv4 acl_ipv4_cpu_cos
 rule 10 description ICMP
 rule 10 match protocol ICMP
 rule 10 action cpu-cosq 1
 rule 20 description "Trace Route"
 rule 20 match protocol UDP destination-port-range 33434-33523
 rule 20 action permit cpu-cosq 1 count
 rule 30 description SSH
```

```
 rule 30 match source-ipv4-prefix-list SSH_pre1 protocol TCP
tracking-state [ ESTABLISHED ] destination-port-range 22
 rule 30 action cpu-cosq 2
 rule 250 description "All other traffic"
 rule 250 match any
 rule 250 action deny count
!


interface craft 2
 access-group ipv4-acl acl_ipv4_cpu_cos
 cosq     cpu_acl_1
 ip dhcp server disable
 ip address 10.245.51.118/24
 no shutdown
!
```

Parameters

You can configure the following parameter values for the "craft 2" interface:

Note: The following table covers both front and rear craft ports.

Parameter	Description
interface craft {1|2}	Specifies the craft interface index. Valid values: • craft 1 (MGT-1) • craft 2 (MGT-3, E7-2 rear panel)
access-group	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates an access list with the interface Valid options: • ipv4-acl: Apply an Ipv4 Access Control List • ipv6-acl: Apply an Ipv6 Access Control List
cosq	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates a cosq profile with the interface Valid options: • <profile name>
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. Valid values: • dhcp • <IP address>/<mask> Craft 1 default = 192.168.1.1; craft 2 default = 192.168.1.2. If you change the factory default address, the current value becomes the default.

Parameter	Description
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable (default for craft 1) • disable (default for craft 2) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)
ipv6 address	Valid values: • <IPv6 address>
ipv6 redirects	Valid values: • true (default) • false
ipv6 unreachables	Valid values: • true (default) • false
shutdown	Administrative state of the craft management port. Valid values: • no shutdown (default for craft 1) • shutdown (default for craft 2)

Configuring Static Routes

This topic describes how to configure static routes on the E9-2. The E9-2 supports 4,000 IPv4 routes in its routing table, with no limit per protocol (for example, static vs BGP).

The E9-2 system supports only one default route. When Border Gateway Protocol (BGP) is enabled, a default route is given to the E9-2 system from the router(s). Because all IP interfaces (internal and external) on the system are in the same routing table, including all management interfaces, Calix recommends that you configure static routes for management traffic to prevent the E9-2 from sending it out the uplink.

Parameters

You can configure the following parameters and valid options when configuring a static route:

Parameter	Description
ip route	An IPv4 network-prefix in CIDR format. For the default route, host bits and mask set to zero. Example (default route): 0.0.0.0/0 Example (static route): 192.0.2.0/24
next-hop	The next-hop IP address (for example, the next router interface in the path to the destination network or host address). This address must be reachable from an interface in the routing instance. Set the next hop to NULL0 to configure blackhole route. Valid values: • <IPv4 address> • <IPv6 address> • NULL0
distance	(Optional) Administrative distance value, used in route selection. Routes with smaller distance value are given preference. Valid values: • 1-255 (default = 1)
interface	(Optional) Static route for a specific interface: Valid values: • craft <...> • ethernet <...> • lag <...> • loopback <...> • multibind <...> • vlan <...>
tag	(Optional) Value of route tag attribute.

Procedure

To configure a static route

- To add a static route:

```
Calix-1(config)# ip route <IPv4 static route> next-hop <IPv4
address> [distance <administrative distance>] [tag <route tag>]
```

- To remove a static route:

```
Calix-1(config)# no ip route <IPv4 static route> next-hop <IPv4
address>
```

- To view the static routes configured:

```
Calix-1# show ip route static
```

- To view the routes currently in the E9-2 forwarding information base (the forwarding table):

```
Calix-1# show ip route fib
```

Example

```
ip route 10.243.0.0/16 next-hop 10.243.24.1
ip route 172.20.0.0/16 next-hop 10.243.24.1
ip route 192.168.102.0/24 next-hop 10.243.24.1
ip route 192.168.100.0/24 next-hop 10.243.24.1
ip route 172.23.0.0/16 next-hop 10.243.24.1
ip route 10.0.3.0/24 next-hop 10.243.24.1
ip route 10.0.1.0/24 next-hop 10.243.24.1
```

Chapter 10

Saving the Configuration

After your initial turn-up configuration has been completed, you may wish to save your configuration. You may save the configuration (running) to the startup configuration and/or to a configuration file.

For additional information on saving and retrieving configurations, see *Managing AXOS Configuration Files* (on page 345).

Procedures

To save the running configuration as the startup configuration

```
Calix-1# copy running-config startup-config
```

To save the running configuration to a file

```
Calix-1# copy config from running-config to <file.xml>
```

Chapter 11

Using Auto-Provisioning

Note: To confirm the level of support for auto-provisioning, call-home (to SMx or DPx), and ZTP for your AXOS system, see the latest Product Planning Guide for your AXOS system.

For supported AXOS systems, this chapter describes how to use the auto-provisioning feature, as well as the options for connecting to an instance of SMx hosted in Calix Cloud.

Auto-Provisioning Overview

Auto-prov overview

Some AXOS systems support auto-provisioning, where the factory-default system is pre-configured with an active uplink port and in-band management. Upon power-on and boot-up, the system sends DHCP requests from the active uplink port, and is ready to act upon the information received from a DHCP server.

For example:

- Via options, a DHCP server may provided the IP address of a TFTP server and configuration file name; in this case, the AXOS system contacts the TFTP server, downloads the configuration file, and applies it. If the configuration file contains call-home information for SMx, the AXOS system calls home to SMx for further configuration.
- Via options, a DHCP server may provide the IP address of a DPx controller; in this case, the AXOS system calls home to DPx for further configuration. For more information, see the *DPx Operations Guide*.

Note: Auto-provisioning only works for SFP+ and XFP ports.

Auto-prov with call home to SMx

Note: Do not use both the CLI and Calix SMx to provision services on an AXOS system, as changes made via the CLI are not synced to SMx.

This chapter focuses on this application and the following options to connect an AXOS system to an instance of SMx hosted in Calix Cloud:

- Manually add an AXOS system to SMx using a static IP address
- Manually trigger call home to SMx from an AXOS system
- Connect to SMx via auto-provisioning and call home
    - Calix's call home feature provides a mechanism to navigate through a NAT/Carrier-grade NAT (CGN) to limit the need for VPNs. The call home feature allows the AXOS node to establish a TCP connection to the SMx server. The SMx server uses this connection to manage the AXOS node via NETCONF. The AXOS node monitors the connection and automatically re-establishes it when lost due to network issues. Because the AXOS node establishes and maintains the connection from the private network side, no VPN is needed. Note that use of a private IP address requires a corporate router to provide NAT functionality so you can route to the internet.
    - The full Calix solution incorporates auto-provisioning, allowing the AXOS system to acquire an IP address from a DHCP server and download a configuration file from a TFTP server, giving it all the information needed to initiate a TCP connection to the SMx server.

For more details, see the following sections of this chapter.

Auto-prov with call home to DPx

For detailed information on this application, see the *DPx Operations Guide*.

Notes on ZTP with the E7-2/E3-2 and NAP DPx

ZTP boot using untagged traffic (and a management VLAN other than 999) is supported. Upon boot, the E7-2/E3-2 initially looks for LLDP frames with Management TLV to determine uplink type and VLAN, using the following workflow:

- If LLDP is received, and the Mgmt VLAN TLV is present, the specified VLAN is created and used (added to TSP); if the Mgmt VLAN TLV is not present, the E7-2/E3-2 will perform ZTP on VLAN 999.
- If LLDP is not received, ZTP enters fallback mode, switching back and forth between untagged ZTP and tagged ZTP on VLAN 999 (for 60 seconds each) until a DHCP offer is received.

Manually Adding an AXOS System to SMx via a Static IP Address

You may manually add an AXOS system to Calix SMx using a static IP address for the node.

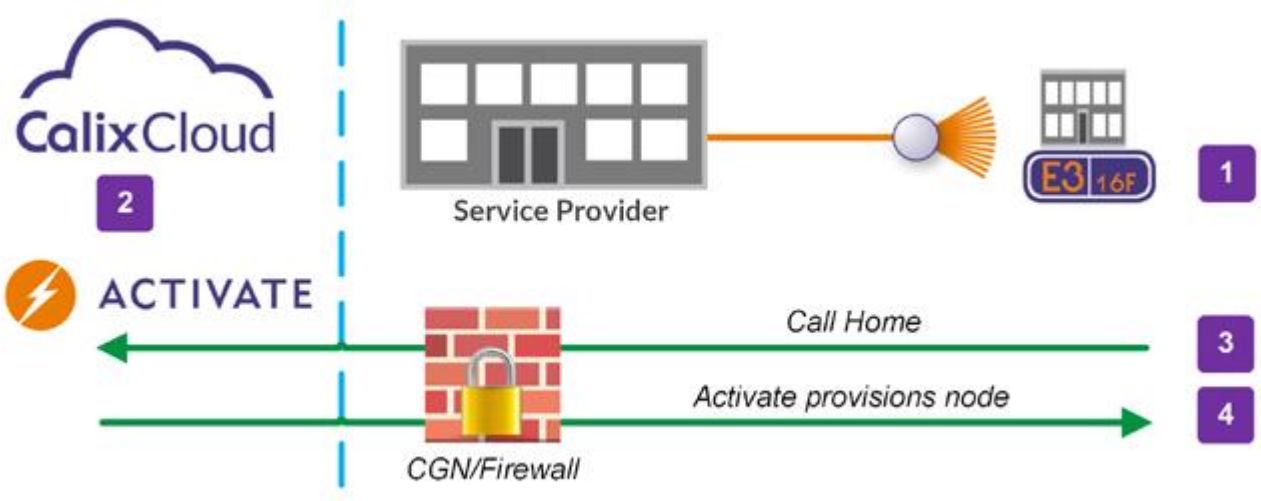
1. Statically provision either a private or public IP address for the AXOS system.

   Note: If a private IP address is statically provisioned on the AXOS system, you need to contact Calix TAC so they can establish VPN connectivity to the node. Use of a private IP/VPN is only used for lab demonstration purposes and is not valid for wide scale deployments.

2. Add the AXOS system to SMx using the static IP address.
3. SMx connects to the AXOS system.
4. If supported, SMx configures the AXOS system (refer to SMx user documentation).

Triggering a Call Home Connection to SMx from an AXOS System

The AXOS system supports the ability to be configured to "call home" (initiate a connection to SMx). The following diagram shows a broad overview of this process.



1. Statically assign either a private or public IP address to the AXOS system.
2. Include commands in the AXOS system configuration so it initiates a Call Home connection to SMx.
3. If supported, Calix SMx provisions the AXOS system.

To connect to SMx via Call Home

1. Update your AXOS system configuration with the following call home commands:
   - The following are the minimum parameters needed to configure call home on an AXOS system:
     Calix-1(config)# **`call-home netconf-client`** <*NETCONF-client-name*> **`ssh endpoints endpoint`** <*endpoint name*> **`address`** <*endpoint IP address*>
   - For resiliency you may provision multiple end points.
   - By default, the AXOS system will use port number 7777 after resolving DNS. Calix strongly recommends that you do not change this port number and that you notify Calix TAC if you do so.

- If required by your network, you may also configure the following "reconnect-strategy"commands. The reconnection strategy defines how a NETCONF server reconnects to a NETCONF client, after losing connectivity to it, even if due to a reboot. By default, the AXOS system tries to connect 3 times with the first endpoint listed and then moves on to the next endpoint. If it cannot connect to the last listed endpoint, it will return to the first listed endpoint and try to connect to it, attempting connections with the endpoint list in a round robin format. If there is only one endpoint listed, the AXOS system will try to connect continuously. The AXOS system will wait one second between every connection attempt.

Note: Calix strongly recommends using the default settings for the "reconnect-strategy"commands.

Calix-1(config)# **call-home netconf-client** <*name*> **reconnect-strategy max-attempts** <*number*>

Calix-1(config)# **call-home netconf-client** <*name*> **reconnect-strategy start-with** <*first-listed*|*last-connected*>

2. Using the call home configuration data, the AXOS system initiates a call home process with SMx:

a. The AXOS system opens a TCP connection to SMx.

- The TCP connection traverses the service provider firewall(s), the public intranet (unless there is a E-LINE service between the two) and the Calix firewall.
- IP address:
  - IPv6: The AXOS system supports provisioning an IPv6 mgmt address via SLAAC. This means that there must be a router in the network that can respond to AXOS system Router Solicitations with Router Advertisements (RA). The RA must have O bit set (Other config exists in DHCP server). The AXOS system can retrieve a list of config servers from the DHCPv6 server. It will prepend this list to the factory default list.
  - IPv4: If the AXOS system is using an IPv4 mgmt address, the AXOS system cycles through DHCPv4 discover, request and offer sequence. The offer included the list of configuration servers the the AXOS system should use to retrieve its bootstrap configuration.
- The TCP connection includes an IDevID cert that was generated on the AXOS system using an a issuing certificate with a private key. This cert includes mention of Calix and the AXOS system's serial number.

b. SMx accepts the TCP connection.

c. The AXOS system sends SMx its identity information over the TCP connection.

d. SMx reads the identity information from the AXOS system.

e. SMx closes the TCP connection.

f. SMx identifies a PMA instance for this AXOS system or creates one if needed.

g. SMx establishes a NETCONF session with the AXOS system with the default username and password (sysadmin/sysadmin) via a newly created SSH connection. The AXOS system will check every 5 seconds to see if the SSH connection is still up.

h. SMx retrieves the serial number from the AXOS system via the newly created NETCONF session.

i. SMx provisions the AXOS system.

3. The AXOS system is now configured and is operational.

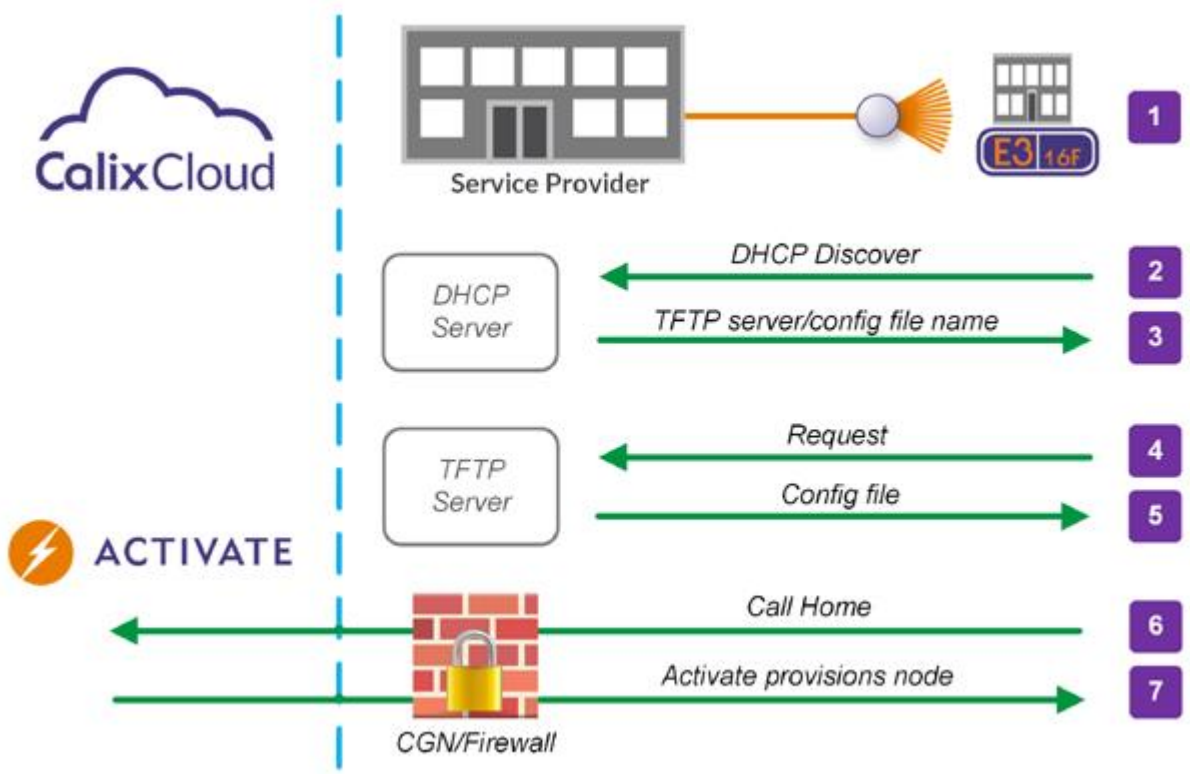
Connecting to Calix SMx via Auto-Provisioning and Call Home

The AXOS system supports the ability to automatically request a call home connection to SMx via auto-provisioning. This turn up method allows a technician to go onsite, power up the AXOS system and simply plug in the uplink. The AXOS system will call home, connect to SMx, upgrade, and provision itself for service. CO Personnel only need to associate a subscriber to the existing service and edit the name/region of the AXOS system.

When call home and auto-prov are used to turn up an AXOS system, the node uses information from a DHCP server to automatically download a configuration file from a TFTP server when it initially boots up or it is reloaded with the factory default configuration. This config file includes information that allows the AXOS system to "call home" (initiate a connection to SMx).

Note: This turn up method assumes that you are using the default management VLAN (999) to connect to the AXOS system.

The following diagram shows a broad overview of this process.



The basic auto-provisioning process is as follows:

1. Connect the AXOS system to the network via the INNI interface that is enabled by default and power up the AXOS system.
2. When the AXOS system boots up it uses this interface to automatically request an IP address for the internal IP host interface via DHCP on the management VLAN (999).
3. The DHCP server refers the AXOS system to the TFTP server and a config file name.
4. The AXOS system contacts the TFTP server.
5. The AXOS system downloads the config file from the TFTP server.
6. The config file instructs the AXOS system to open a TCP connection to SMx, using the IP address of an SMx/other NETCONF server in this file.

   Note: To provision services, use Compass SMx or the CLI but not a combination of both to avoid provisioning conflicts, profile sync issues, and other issues.

7. Calix SMx provisions the AXOS system.

Detailed Steps to Connect to SMx via Auto-Provisioning/Call Home

This topic provides detailed instructions that show how to use auto-prov to configure the AXOS system to automatically "call home (initiate a connection to SMx). This turn up method requires both a TFTP server and a DHCP server be available via VLAN 999, the default management VLAN. This may require you to provision a path for this VLAN on any network nodes (for example, E7s) that are between the DHCP server and AXOS system.

Note: You must modify dhcpd.conf file on the DHCP server to include the parameters needed to identify the AXOS system config.xml file, the AXOS system and TFTP server. Make sure to restart the DHCP service after implementing the changes, or the new configuration will not take effect. If the dhcpd.conf file has no config file information or if the TFTP server cannot be reached, the AXOS system releases the IP address obtained via DHCP and cycles through the complete DHCP handshake on a regular ~60 second interval. This allows a service provider to either begin to configure the AXOS system manually (entering a single configuration command disables auto provisioning) or determine what is wrong with the dhcpd.conf file.

To connect to SMx via Call Home and Auto-Provisioning

1. Using an AXOS system in a lab, create an config file that includes the call home configuration. This configuration for the AXOS system may be a global configuration or site-specific configuration.

   a. Include the following "**call-home netconf-client**" CLI commands in this config file to specify the call home feature parameters:

      - The following are the minimum parameters needed to configure call home on an AXOS system:
        Calix-1(config)# **call-home netconf-client** <*NETCONF-client-name*> **ssh endpoints endpoint** <*endpoint name*> **address** <*endpoint IP address*>
      - By default, the AXOS system will connect to the SMx server on port number 7777 after resolving DNS. Calix strongly recommends that you do not change this port number and that you notify Calix TAC if you do so.
      - For resiliency you may provision multiple end points.

   - If required by your network, you may also configure the following "reconnect-strategy"commands. The reconnection strategy defines how a NETCONF server reconnects to a NETCONF client, after losing connectivity to it, even if due to a reboot. By default, the AXOS system tries to connect 3 times with the first endpoint listed and then moves on to the next endpoint. If it cannot connect to the last listed endpoint, it will return to the first listed endpoint and try to connect to it, attempting connections with the endpoint list in a round robin format. If there are is only one endpoint listed, the AXOS system will try to connect continuously. The AXOS system will wait one second between every connection attempt.

   Note: Calix strongly recommends using the default settings for the "reconnect-strategy"commands.

   Calix-1(config)# **call-home netconf-client** <*name*> **reconnect-strategy max-attempts** <*number*>

   Calix-1(config)# **call-home netconf-client** <*name*> **reconnect-strategy start-with** <*first-listed*|*last-connected*>

2. On the lab AXOS system, save the running configuration to the start-up configuration file by issuing the CLI command "**copy running-config startup-config**" from Operational mode.

3. Save the configuration file to your PC by issuing the CLI command "**copy config from running-config to <config location>**" from Operational mode.

4. Upload the XML configuration file from your PC to a TFTP server.

   Note: Calix recommends that you put the file in the ROOT directory so it can be found easily. For example:
   upload file config from-file startup-config.xml to-URI ftp://calixftp@172.23.34.xxx:21/tftpboot/startup-config.xml password ***

5. Modify the dhcpd.conf on the DHCP server to include the parameters needed to download the configuration file and an DHCP address assignment that is within the appropriate subnet declaration of the dhcpd.conf file.
6. Install an AXOS system, connect the INNI uplink and power up the node. Refer to the installation guide for detailed instructions.
7. Confirm successful completion of the auto-provisioning process by viewing the LED activity on the AXOS system. After the configuration file has been successfully downloaded from the TFTP server, it is automatically applied to the running configuration.
8. As the AXOS system interacts with the DHCP server:
   a. A DHCP request is sent from the AXOS system when it boots up via VLAN 999.
   b. The DHCP server responds to this request with the following
      - an IP address for the AXOS system's management interface
      - a designated TFTP server (via Option 66)
      - a configuration file name
   c. The AXOS system receives the DHCP response and configures its IP address
9. The AXOS system interacts with the TFTP server:
   a. The AXOS system uses the TFTP information from the DHCP response to download a config file from the TFTP server.
   b. The downloaded config file contains the AXOS system call-home configuration data.
10. Using the call home configuration data, the AXOS system initiates a call home process with SMx:
    a. The AXOS system opens a TCP connection to the SMx server.
       - The TCP connection traverses the service provider firewall(s), the public intranet (unless there is a E-LINE service between the two) and the Calix firewall.
       - IP address:
         - IPv6: The AXOS system supports provisioning an IPv6 mgmt address via SLAAC. This means that there must be a router in the network that can respond to AXOS system Router Solicitations with Router Advertisements (RA). The RA must have O bit set (Other config exists in DHCP server). The AXOS system can retrieve a list of config servers from the DHCPv6 server. It will prepend this list to the factory default list.
         - IPv4: If the AXOS system is using an IPv4 mgmt address, the AXOS system cycles through DHCPv4 discover, request and offer sequence. The offer included the list of configuration servers the the AXOS system should use to retrieve its bootstrap configuration
       - The TCP connection includes an IDevID cert that was generated on the AXOS system using an a issuing certificate with a private key. This cert includes mention of Calix and the AXOS system's serial number.

b. SMx accepts the TCP connection.

c. The AXOS system sends SMx its identity information over the TCP connection. This connection is a TLS "pipe" or tunnel.

d. SMx reads the identity information from the AXOS system.

e. SMx identifies a PMA instance for this AXOS system or creates one if needed.

f. SMx establishes a NETCONF session with the AXOS system with the username and password (by default this is sysadmin/sysadmin) via a newly created SSH connection within the TLS "pipe". The AXOS system will check every 5 seconds to see if the SSH connection is still up.

g. SMx retrieves the serial number from the AXOS system via the newly created NETCONF session.

h. SMx provisions the AXOS system.

11. The AXOS system is now configured and is operational.

Configuring a DHCP Server for Auto-Provisioning

To configure a DHCP server to support auto-provisioning, you must modify the dhcpd.conf file to identify the following:

- The AXOS system config.xml file
- Options to identify the host (for example: Client ID [Option 61] or MAC address)
- Option to be sent to the host: TFTP server ID (sname, Option 66 or siaddr)

Note: This topic assumes that you have a DHCP server up and running in your network. Make sure to restart the DHCP service after implementing the changes, or the new configuration cannot take effect.

AXOS system configuration file identification

The dhcpd.conf must be modified to send the file name of the AXOS system config file. Add the file name of the AXOS system config file for each AXOS system via the following keyword:

```
filename "node_name.xml";
```

For example:

```
filename "node2.xml";
```

AXOS system identification

The DHCP server must identify the AXOS system via one of the following methods to send appropriate file name in the DHCP response.

Note: Calix recommends that you use the serial number to identify a new AXOS system, as printed on the system label and shipping box.

Client ID

This is an ID unique to any AXOS system device. It is the serial number encoded as option 61 in the server bound DHCP messages.

Servers can match on this with the keyword "dhcp-client-identifier." Due to differences in server architecture, MS Servers and Linux Servers interpret this string differently. For MS Servers a requirement to precede each digit in the serial number by the number 3 is required. For Linux Servers the entire serial number must be preceded by "\000".

The following server configuration examples use the serial number of 031307000512.

For MS Servers:

```
                    host Petalumahost {
                                option dhcp-client-identifier
"303331333037303030353132";
                                filename "node1.xml"
                     }
```

For Linux Servers:

```
                    host Petalumahost {
                                option dhcp-client-identifier
"\000031307000512";
                                filename "node1.xml"
                     }
```

Identify the AXOS system serial number for the AXOS system by issuing the following command:

```
node# show inventory baseboard serial-number
```

MAC address

All DHCP packets carry their sender's MAC address. An example of the server configuration using the MAC address is shown below.

```
                    host ncd1 {
                                      hardware ethernet
00:c0:c3:49:2b:57;
                                      filename "node1.xml"
                     }
```

Identify the MAC address for the AXOS system by issuing the following CLI command:

```
node2# show interface ip-host 1
interface ip-host 1
status
name "ip-host 1"
admin-state enable
oper-state up
mac-addr 00:02:5D:BA:54:16 <----------------
net-config-type static
ip-address 10.201.29.36
ip-mask 255.255.252.0
ip-gateway 10.201.28.1
vlan "185:6 "
config-download enable
ip-host-cntrs
rx-pkts 114193
rx-octets 7920722
tx-pkts 22052
```

tx-octets 2583870

TFTP server identification

TFTP server identification must be provided via the sname, Option-66, or the siaddr command in the DHCP configuration syntax.

- **sname**: Server host name, null terminated string. Example: server-name "192.168.1.5";
- **option 66**: Used to identify a primary TFTP server when the "sname" field in the DHCP header has been used for other DHCP options. Option 66 has a minimum length of 1 and allows you to assign TFTP server IP addresses to the message header for packet routing.Example: option tftp-server-name "192.168.1.5";
- **siaddr**: IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server. Example: next-server "192.168.1.5";

The following rules apply when identifying the TFTP server:

- The system checks for the server name from either the sname field in the DHCP header or Option 66 (sname takes precedence over Option 66).
- If the server name is not available, the system checks for the IP address of the next server in the DHCP header siaddr field.

dhcpd.conf file example

The following example shows a modified dhcpd.conf file on a server, with the added text in bold and explanations in the right column.

subnet 10.15.0.0 netmask 255.255.255.0 {	
vendor-option-space CALIX-ONT-SERVER;	
option CALIX-ONT-SERVER.cms-address 10.15.0.50;	
option CALIX-ONT-SERVER.validateMIC off;	
#option CALIX-ONT-SERVER.second-tftp-address 10.15.0.13;	
max-lease-time 172800;	
default-lease-time 172800;	
server-name 10.15.0.50;	*IP address of the TFTP server the XML config file will be downloaded from.*
host Node2 {	*This line simply opens a new class – the Node2 portion is irrelevant*
option dhcp-client-identifier "\000031307000512";	*This line identifies the serial number of the system.*
fixed-address 10.15.0.98;	*Fixed DHCP address assigned to the device*
filename "Node2.xml";	*Name of the XML config file that Node2 will download*
}	*Close the class*
range 10.15.0.100 10.15.0.250;	
option subnet-mask 255.255.255.0;	*Default subnet mask to be used by DHCP clients*
option routers 10.15.0.50;	
option domain-name "dvtlnx06-local";	
#next-server 10.15.0.13;	
log-facility local7; **}**	

Provisioning Call Home Commands

This section provides details about the commands used to configure the call home feature an AXOS system. Once the AXOS system has successfully called home, it will confirm every 5 seconds that the SSH connection is active.

call-home netconf-client

List of NETCONF clients the NETCONF server is to initiate call-home connections to.

This topic is organized as follows:

- Syntax
  - Starting point
  - Possible completions
- Parameters

Syntax

Starting point:

```
call-home netconf-client <name>
```

Possible completions:

```
connection-type periodic reconnect-timeout <unsignedshort>
reconnect-strategy max-attempt <unsignedByte> start-with {first-listed|last-connected}
ssh endpoints endpoint <value> address <value> port <value>
```

Parameters

The parameters for the "call-home netconf-client" command are described below.

Parameter	Description
call-home netconf-client <name>	An arbitrary name for the remote NETCONF client. List of NETCONF clients the NETCONF server is to initiate call-home connections to.
connection-type periodic reconnect-timeout	For the periodic connection-type, indicates the reconnect-timeout value in seconds. With the periodic connection-type, the NETCONF server periodically connects to the NETCONF client, so that the NETCONF client may deliver messages pending for the NETCONF server. The NETCONF client is expected to close the connection when it is ready to release it, thus starting the NETCONF server's timer until next connection. The reconnect-timeout is the maximum amount of unconnected time the NETCONF server will wait before establishing a connection to the NETCONF client. The NETCONF server may initiate a connection before this time if desired (e.g., to deliver a notification). Valid values: • 1-65535 (default = 60) **(recommended = 1)** **Note:** Calix recommends setting this value to 1 since the default value (60) may be longer than expected by most users, resulting in a poor user experience.

Parameter	Description
reconnect-strategy max-attempts	Part of the reconnection strategy, which guides how a NETCONF server reconnects to an NETCONF client after losing a connection to it, even if due to a reboot. The NETCONF server starts with the specified endpoint and tries to connect to it max-attempts times before trying the next endpoint in the list (round robin). The max-attempts value specifies the number times the NETCONF server tries to connect to a specific endpoint before moving on to the next endpoint in the list (round robin). Valid values: • 1-255 (default = 3)
reconnect-strategy start-with	Part of the reconnection strategy, specifies which of the NETCONF client's endpoints the NETCONF server should start with when trying to connect to the NETCONF client. Valid values: • first-listed(default): The reconnection strategy guides how a NETCONF server reconnects to an NETCONF client, after losing a connection to it, even if due to a reboot. The NETCONF server starts with the specified endpoint and tries to connect to it max-attempts times before trying the next endpoint in the list (round robin). • last-connected: Indicates that reconnections should start with the endpoint last connected to. If no previous connection has ever been established, then the first endpoint configured is used. NETCONF servers SHOULD be able to remember the last endpoint connected to across reboots. Specifies the number times the NETCONF server tries to connect to a specific endpoint before moving on to the next endpoint in the list (round robin).
ssh endpoints endpoint	Specifies the SSH-specific call-home transport configuration. User-ordered list of endpoints for this NETCONF client. Valid values: • <string - arbitrary name for the endpoint>
ssh endpoints endpoint <endpoint> address	For a given endpoint, IP address or hostname. If a hostname is configured and the DNS resolution results in more than one IP address, the NETCONF server will process the IP addresses as if they had been explicitly configured in place of the hostname. Valid values: • <IP address> • <hostname: string, 1-253 chars>
ssh endpoints endpoint <endpoint> port	For a given endpoint (with IP address or hostname), optional IP port value. The NETCONF server will use the IANA-assigned well-known port if no value is specified. Valid values: • 0 - 65535 (default = 7777)

call-home source-interface

call-home source interface

Syntax

```
call-home source-interface <interface name>
```

Parameters

The parameters for the "call-home source-interface" command are described below.

Parameter	Description
call-home source-interface <name>	An interface to act as source interface Valid value: • system craft(E9 only)

netconf interface

Restricts communications of the NETCONF application to the specified interface.

Note: Before configuring the NETCONF source-interface to use a loopback interface, you must configure a loopback interface with an IP address which is reachable from the intended NETCONF server.

Syntax

E9-2

```
netconf interface {loopback interface name|system-craft}
```

E3-2/E7-2

```
netconf interface <loopback interface name>
```

Parameters

The parameters for the "netconf interface" command are described below.

Parameter	Description
interface	Name of an interface. Valid values: • A previously configured loopback interface name, for example LB1 • system-craft (default) • IP address of WAN interface • Note: Different applications may reference the same loopback interface. When the source-interface is specified, the first IP address is used as the source IP address for all outbound connections by NETCONF. When the source-interface is not specified (default), NETCONF attempts to connect using any available interface with a route to the destination.

Example

```
Calix-1(config)# netconf interface LB1
```

netconf session-timeout

Sets the time in minutes for logging out all current NETCONF sessions after inactivity.

Note: The AXOS system system supports up to 32 simultaneous NETCONF sessions.

Syntax

```
netconf session-timeout <0-255>
```

Parameters

The parameters for the "netconf session-timeout" command are described below.

Parameter	Description
session-timeout	Time in minutes for logging out all current NETCONF sessions after inactivity. Valid values: • 0–255; (default =0, never time out)

Chapter 12

Performing System Tasks (E9-2)

This chapter covers the following topics:

- Configuring the forward-table mode
- Switching active and standby controllers
- Performing an ICL LAG switchover
- Configuring line card reload sequencing
- Reloading system cards
- Backing up the system configuration
- Shutting down an inter-chassis link

Configuring the Forward-Table Mode

The forward-table mode sets the max number of supported L2 MACs, IP hosts, and IP routes for the system.

CLI commands

```
!!CLI config mode
system-limits forward-table {mode-1|mode-2}
```

Guidelines

- Ensure that the desired mode for your deployment has been selected:
  - Mode 1 (default) is optimized for Layer 2 services, supporting 40K MACs, 40K IPv4 hosts, and 64K IPv4 routes
  - Mode 2 is optimized for Layer 3 services, supporting 8K MACs, 72K IPv4 hosts, and 64K IPv4 routes
- After changing modes [for example, changing from mode 1 (default) to mode 2], you must reload the system.

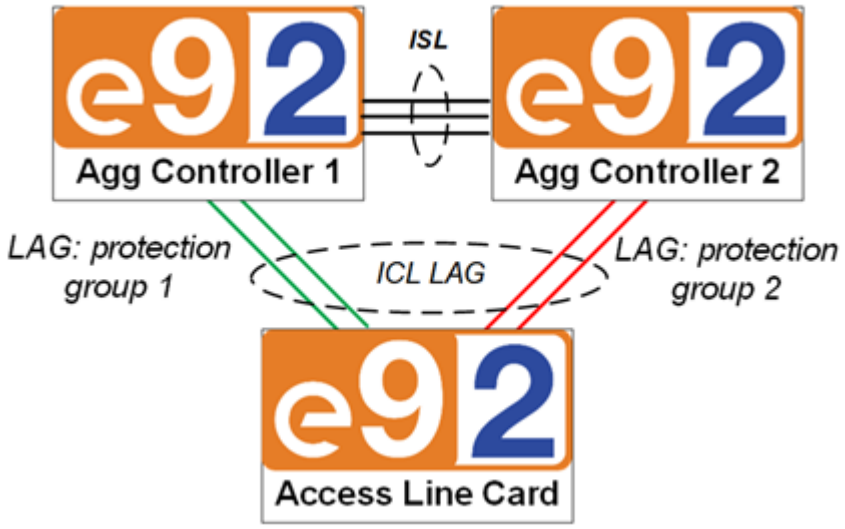
Performing an ICL LAG Switchover

This topic describes how to configure the ICL LAG switchover, which allows you to manually determine which ICL protection group to keep active between an access line card and an active aggregation card.

The E9-2 uses Inter-Chassis Links (ICL) between the aggregation cards and the access line cards that operate in an Active/Standby LAG arrangement. Two links are members of the LAG from the Active aggregation card and two links are members from the Standby aggregation card. Four member-links are combined to form a single LAG to each line card. The aggregate capacity of the ICL to each line card is 200GE as only one Aggregation card is in the Active state at any given time.

Note: See the *Calix E9-2 Installation Guide* for information on interconnecting the E9-2 shelves. Refer to *E9-2 Inter Chassis Links- Active/Standby LAG* (on page 34) for more information about the ICLs.

All ICLs on any access line card are in one ICL LAG interface. The ICL LAG interface consists of four 100 gig ports, with two ports homing in on one card running active and the other two ports as standby. The port pairs are configured in discrete protection groups, 1 and 2. This affinity allows for the protection path to switch as a group in response to degradations/failures in member ports in one of the protection groups. The standby ICL LAG links carry no bearer traffic in normal operation (only OAM-CFM/CCM).



The E9-2 supports an ICL LAG switchover feature which allows you to manually determine which ICL protection group to keep active between an access line card and an active aggregation card. This ICL LAG switchover feature is independent of the ability to switch active and standby controllers. The control plane on both cards is active/standby but the dataplane is all active. The ICL is part of the dataplane, allowing it to home in independently on either card, regardless of the active/standby state of the control plane. An access line card can communicate with the active aggregation card via the connection towards the standby aggregation cards card. In this instance, from the line card's perspective the ICL LAG is active towards the standby aggregation card.

Considerations

- A manual switch is best effort. If you try to switch to a protection group to a worse path, the manual switch will not occur
- A forced switch will take effect even if the switch would be to a path that is degraded. Note that the force is not allowed if the switch will cause the card to which the ICL link is connected to become isolated.
- If a force is in effect on an ICL link and the protection group to which the link is forced goes completely down, the force will be autonomously removed by the E9-2 system so that the access line card associated with the ICL link will not become isolated from the E9-2 system's aggregation cards.
- The command **perform icl-aps interface lag <lag-interface name> clear** is used to remove a force condition.
- A manual switch will not override a force if a force is in place for a given ICL link.
- The manual switch all interfaces is best effort in a link by link iteration across all ICL links. This command allows you to switch all ICL links in an E9-2 system via a single command.
- The command **perform icl-aps interface all manual-switch protection-group** is best effort in a link by link iteration across all ICL links. This command allows you to switch all ICL links in an E9-2 system via a single command.
- The command **show interface summary icl** displays the current ICL status and additional status details concerning each ICL link.

To perform an ICL LAG switchover

The following commands allow you to manually or forcefully determine which ICL protection link should be active.

- Manually switch all ICL links in an E9-2 system, specifying if you wish ICL protection group 1 or 2 to become active:

  `Calix-1# perform icl-aps interface all manual-switch protection-group <1|2>`

- Manually switch ICL links on a specific LAG interface, specifying if you wish ICL protection group 1 or 2 to become active:

  `Calix-1# perform icl-aps interface lag <lag-name> manual-switch protection-group <1|2>`

- Forcefully switch ICL links on a specific LAG interface, specifying if you wish ICL protection group 1 or 2 to become active:

  `Calix-1# perform icl-aps interface lag <lag-name> forced-switch protection-group <1|2>`

To clear a forced ICL LAG switchover

The following command removes a forced switch condition on a specified LAG interface:

`Calix-1# perform icl-aps interface lag <lag-interface name> clear`

To view an ICL LAG switchover status

- To view which protection groups are active, issue the following command:

  `Calix-1# show interface lag <lag-interface name> members`

- To view current status details for each ICL link, issue the following command:

  `Calix-1#show interface summary icl`

- To check if a force is in place, issue the following command:

  `Calix-1# show interface lag <lag-interface name> status`

Example

1. Issue the command **show interface lag la25 members** to confirm that protection group 2 is active (interfaces from slot 2 are active).

```
Calix-1# show interface lag la25 members
members
group la25
                                                  LACP        RX          TX
SHELF  SLOT  PORT  INTERFACE  OPER STATE  STATUS       UTILIZATION  UTILIZATION
-------------------------------------------------------------------------------
1      1     c1    1/1/c1     up/standby  static-icl   0            0
1      1     c2    1/1/c2     up/standby  static-icl   0            0
1      2     c1    1/2/c1     up/active   static-icl   0            0
1      2     c2    1/2/c2     up/active   static-icl   0            0
```

2. Forcefully switch protection group 1, making the interfaces from slot 1 become active.

```
Calix-1# perform icl-aps interface lag la25 forced-switch protection-group 1
```

3. Verify your configuration:

   - Confirm that protection group 1 is now active:

```
Calix-1# show interface lag la25 members
members
group la25
                                                    LACP          RX            TX
SHELF  SLOT  PORT  INTERFACE  OPER STATE  STATUS       UTILIZATION  UTILIZATION
-------------------------------------------------------------------------------
1      1     c1    1/1/c1     up/active   static-icl   0            0
1      1     c2    1/1/c2     up/active   static-icl   0            0
1      2     c1    1/2/c1     up/standby  static-icl   0            0
1      2     c2    1/2/c2     up/standby  static-icl   0            0
```

   - Confirm that the force is in place:

```
Calix-1# show interface lag la25
status
status
 group                    la25
 if-index                 25
 admin-state              enable
 oper-state               up
 topology-protocol        none
 fwd-state                forwarding
 hardware-type            LAGGroup
 description              ICL-2/1
 mtu                      9390
 service-role             icl
 hash-method              src-dst-mac
 active-protection-group  1(f)
```

   - View current status details for the ICL link:

```
Calix-1# show interface summary icl
                                                    TO        ACTIVE
          ADMIN   OPER                    OPER      SHELF     PROTECTION
NAME      STATE   STATE   FWD STATE       SPEED     SLOT      GROUP
-------------------------------------------------------------------------
2/1/la1   enable  up      forwarding      200Gbs    1/1,1/2   1
2/2/la1   enable  up      forwarding      200Gbs    1/1,1/2   1
la25      enable  up      forwarding      200Gbs    2/1       1
la26      enable  up      forwarding      200Gbs    2/2       1(f)
la27      enable  down    blocking        0Bps      3/1       none
la28      enable  down    blocking        0Bps      3/2       none
la29      enable  down    blocking        0Bps      4/1       none
la30      enable  down    blocking        0Bps      4/2       none
la31      enable  down    blocking        0Bps      5/1       none
la32      enable  down    blocking        0Bps      5/2       none
```

Configuring Line Card Reload Sequencing

The command **card reset-mode** configures the order in which access line cards are reloaded. By default, all line cards are reloaded/upgraded in shelf/slot numeric order.

Configuration guidelines

- This command applies to access line cards only. The controller card reset sequence is internally managed.
- This command setting may not apply to all live or full upgrades.

Parameters

You can configure the following parameters for the **card reset-mode** command:

Parameter	Description
all	All line cards are reloaded/upgraded at the same time (no protection)
sequenced	All line cards are reloaded/upgraded in shelf/slot numeric order (default) For example, the access line card 2/1 is reloaded first. After card 2/1 has completely reloaded, access line card 2/2 is reloaded. After card 2/2 hs completely reloaded, access line card 3/2 is reloaded, etc.
odd-even	Odd line cards are reloaded/upgraded first
even-odd	Even line cards are reloaded/upgraded first

To configure line card reload sequencing

```
Calix-1(config)# card reset-mode [all | sequenced | odd-even | even-odd]
```

Reloading System Cards

This topic describes the **reload** commands supported by the E9-2 system.

Note: There is a five second delay before invoking the entered reload command.

- The reload command reloads the active aggregation card:

  ```
  Calix-1# reload
  ```

- The **reload** <*shelf/slot*> command reloads the specified card. For example:

  ```
  Calix-1# reload 2/1
  ```

- The **reload all** command reloads all cards (aggregation and access) simultaneously:

  ```
  Calix-1# reload all
  ```

- The **reload all sequenced** command reloads all cards in the following orchestrated sequence:
  - The standby aggregation card (for example, 1/2) reloads.
  - The active and standby aggregation cards switchover. For example, aggregation card 1/2 becomes the active aggregation card and card 1/1 becomes the standby aggregation card.
  - Line cards are reloaded based on the setting of the **card reset-mode** command. By default, all line cards are reloaded/upgraded in shelf/slot numeric order (sequenced mode). Refer to *Configuring Line Card Reload Sequencing* (on page 267) for information about how to configure this command.
  - The standby aggregation card (for example, 1/1) reloads.

  ```
  Calix-1# reload all sequenced
  ```

- The **reload line-card** command reloads all access line cards based on the setting of the **card reset-mode** command.

  ```
  Calix-1# reload line-cards
  ```

Example

```
Calix-1# reload all
Proceed with reload? [Y/N] Y
```

Shutting Down an Inter-Chassis Link (ICL)

The E9-2 uses ICLs between the aggregation cards and access line cards which operate in an Active/Standby LAG arrangement. Two links are members of the LAG from the Active aggregation card and two links are members from the Standby aggregation card. Four member-links are combined to form a single LAG to each line card.

An ICL that has member ports may not be shut down (including the LAG child Ethernet ports). This restriction is designed to prevent an operator from inadvertently disconnecting all subscribers on a line card. You must either pull the cable or remove the ICL member port from the bundle before shutting down an ICL.

Configuring the ICLs for 5 or 9-Shelf Nodes

There are two primary configurations for E9-2 nodes:

- A 5-shelf node with one aggregation shelf and up to four access shelves with 200 Gbps inter-connect links (ICLs).
- A 9-shelf node with one aggregation shelf and up to eight access shelves with 100 Gbps ICLs.

You can easily configure the ICLs for one of these modes by using the "icl remap" command.

Configure the 5-shelf/200G ICL mode (default):

1. Run the remap command to put the system in 5-shelf mode
   ```
   CLX3001# perform icl remap card-ports-in-lag 2
   ```
2. Save the config
3. Reload the node

Configure the 9-shelf/100G ICL mode:

1. Run the remap command to put the system in 9-shelf mode
   ```
   CLX3001# perform icl remap card-ports-in-lag 1
   ```
2. Save the config
3. Reload the node

System restore process in the 9-shelf/100G ICL mode

For the system restore process in the 9-shelf/100G ICL mode, use a known good config file (in the 9-shelf mode) as the startup config instead of deleting the startup config. Otherwise, the system will come up in the 5-shelf mode and in a mismatched state (to recover from this issue, see the box below).

Issue: Deleting the startup config file during a restore procedure
Description: If the startup config file is deleted as part of a system restore procedure, upon resetting the system, it will come up in the 5-shelf mode and in a mismatched state. **Corrective actions:** 1. Run the remap command to put the system in 9-shelf mode. `CLX3001# perform icl remap card-ports-in-lag 1` 2. Save the configuration. 3. Reload the node. **Preventive actions:** Back up a known good config file (in the 9-shelf mode) to use during future system restore procedures, and use this file as the startup config instead of deleting the startup config.

Chapter 13

Configuring Profiles and Objects

This section describes the profiles and objects that may be referenced during the turn-up of an AXOS system (for example, during the uplink configuration).

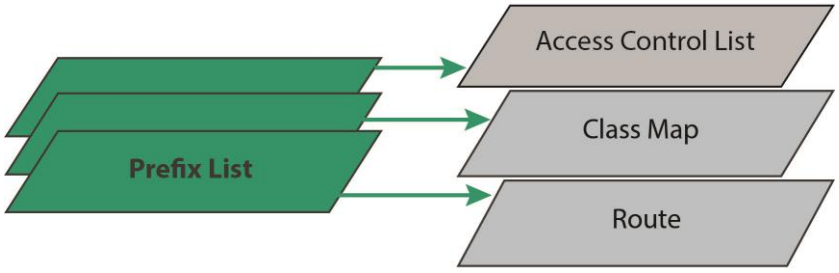
Creating an IPv4 Prefix List

This topic describes how to create an IPv4 Prefix list, and is organized as follows:

- Overview | Configuration guidelines | Procedures | Parameters

Overview

A prefix list defines one or more IPv4 addresses and subnets to match against. Prefix lists help to control network traffic based on subnet addressing, and reduce the need for duplicate configuration entries. You apply an IP prefix list as match criteria for an IP access control list (ACL), IP class map profile, or for routing.



IP Prefix lists are referenced in access lists and class-maps for service delivery and for routing.

When configuring uplinks, IP prefix lists are used to add the static management interfaces to the routing table. They are referenced in the WAN access lists.

IPv4 prefix lists are also used for BGP redistribution and policy maps.

An IP address is represented as x.x.x.x/n, where *n* is the IP prefix. The prefix identifies the number of bits (left to right) used to identify a network. For example, 192.28.101.26/18 means that the first 18 bits are used for the network and the remaining 14 bits are used to identify the host.

Configuration guidelines

- To filter by an exact prefix length, use format x.x.x.x/n
- (Routing only) To filter within a range use:
  - Greater than or equal to (ge): Minimum prefix length (the "from" portion of the range)
  - Lesser than or equal to (le): Maximum prefix length (the "to" portion of the range)
  - ge and le together: Exact match on the prefix length and subnet mask
- The prefix length cannot be less than the ge value and the ge value cannot be less than the le value. For example, 192.10.0.0/16 ge 8 is not valid because 8 is less than the number of bits needed to identify the network.
- For an IP class map policy or access list using an IP prefix list as a match criteria, ge and le are not supported.
- The host portion of the network address must use zeros so as not to overlap the prefix. For example, for IPv4, 200.20.0.0/16 is correct and 200.20.20.0/16 is not correct.
- You can use a prefix list to help define:
  - An allow list, explicitly allowing IP addresses and subnets
  - A block list, explicitly denying IP addresses and subnets

Note: The IP prefix is matched via the class map, which specifies all allowed traffic for an allow list or block list.

Procedures

Creating an IPv4 Prefix List (via SMx)

1. From the navigation bar, select **Profiles**.
2. From the Service navigation menu, select **IPv4 Prefix Profile**.
3. Click **Create**.
4. Enter a name for the prefix list.
5. Click on the plus (+) sign, and then enter a sequence number to apply a unique number to the entry.
6. Reference the parameters below to provision any required additional parameters.
7. Click the **Submit** button.

Creating an IPv4 Prefix List (via CLI)

For a prefix list to associate with an IP class map or ACL:

Specify a name, sequence number, and IP prefix for the list.

```
Calix-1(config)# ip prefix-list <name> seq <1-4294967295> <ip
address/length>
```

For a prefix list to associate with a route:

Specify a name, sequence number, IP prefix and optional ge and/or le operator for the list.

```
Calix-1(config)# ip prefix-list <name> seq <1-4294967295> <ip
address/length> [ge <0-32>][le <0-32>]
```

Parameters

You can configure the following parameters when creating an IP prefix list:

Parameter	Description
ip prefix-list <prefix list name>	Creates a new IPv4 prefix list or modifies an existing prefix list to match IP packets or routes against. Issue the no form of the command to delete a prefix list. Valid values: • A string of up to 48 characters, including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot)
ip prefix-list seq <sequence number>	Specifies the number to order entries in the prefix list. The lower sequence number will be applied first, and if there is a match the higher sequence number will not be tried. **For routing**: Applies a unique order number to the entry, where the software to interprets the lowest sequence number first. **For class maps and ACLs**: Applies a unique number to the entry, similar to an index. To modify a prefix list, re-enter the sequence number Valid values: • 0–4294967295
<prefix>/<prefix-length>	IP prefix in 0.0.0.0/length format (IP address/bit mask), for example 192.0.2.0/24. You can configure a prefix list to include a single or multiple IP prefixes. **Note:** The host portion of the network address must use zeros so as not to overlap the prefix. For example, for IPv4, 200.20.0.0/16 is correct and 200.20.20.0/16 is not correct. Valid values: • <x.x.x.x>/<0-32>
ge	**For routing**: Applies a greater than or equal to value to the range. The prefix length cannot be less than the ge value **Note:** This parameter does not affect a prefix list applied to a class map or ACL. Valid values: • 0–32 (default = 0)
le	**For routing**: Applies a lesser than or equal to value to the range. **Note:** This parameter does not affect a prefix list applied to a class map or ACL. Valid values: • 0–32 (default = 0) For example, ip prefix-list DHCPpool 5 11.0.0.0/24 ge 24 le 24

IPv4 Prefix List Examples

In the following example, the first 8 bits of the prefix 10.0.0.0 are used for the network and the remaining 24 are used to identify the host. The subnet mask must be greater than or equal to 21, and less than or equal to 29.

```
Calix-1(config)# ip prefix-list LIST 5 10.0.0.0/8 ge 21 le 29
```

The following sample IP prefix lists will be shown applied to ACLS in the example section of the following topic, Creating a WAN Access Control List:

- This IP prefix list is named "VOL-DHCPv4-POOL". The sequence number is "1" (you can have multiple sequence numbers in a prefix list). It says to match all prefixes in the 10.66.250.64/26 address space and the subnet mask must be exactly 26.

  ```
  Calix-1(config)# ip prefix-list VOL-DHCPv4-POOL 1 10.66.250.64/26 ge
  26 le 26
  ```

- This IP prefix list is named "LOCAL_INTERFACES" because it refers to the two routed interfaces on the VLAN uplinks and the multibind gateway interface. The sequence number of this IP prefix list is "5" and it says to match all prefixes in the 10.66.250.9/32 address space:

  ```
  Calix-1(config)# ip prefix-list LOCAL_INTERFACES 5 10.66.250.9/32
  ```

- This IP prefix list is named "LOCAL_INTERFACES" and the sequence number is "10". It says to match all prefixes in the 10.66.250.11/32 address space:

  ```
  Calix-1(config)# ip prefix-list LOCAL_INTERFACES 10 10.66.250.11/32
  ```

- This IP prefix list is named "LOCAL_INTERFACES" and the sequence number is "15". It says to match all prefixes in the 10.66.250.65/32 address space:

  ```
  Calix-1(config)# ip prefix-list LOCAL_INTERFACES 15 10.66.250.65/32
  ```

Additional examples:

IP Prefix List	Means
ip prefix-list test 5 0.0.0.0/0	Match the network 0.0.0.0 with a prefix length of zero (default route)
ip prefix-list test 6 192.0.0.0/8	Match all prefixes in the 192.x.x.x/8 address space
ip prefix-list XYZ_SERVERS 20 192.148.0.0/16	Match all prefixes in the 192.148.x.x/16 address space
ip prefix-list test 7 0.0.0.0/0 le 32	Match any address or subnet
ip prefix-list test 8 0.0.0.0/0 ge 30 le 30	Matches any prefix with a subnet mask of exactly 30 bits
ip prefix-list test 9 192.120.0.0/16 ge 16	Match any prefix starting with 192.120.0.0/16 to 192.120.x.x/32
ip prefix-list DHCPpool 15 192.0.0.0/8 ge 8 le 16	Matches all prefixes in the 192.x.x.x/8 address space that have a subnet mask between 8 and 16 bits (192.0.0.0/8 to 192.x.0.0/16)
ip prefix-list DHCPpool 5 11.0.0.0/24 ge 24 le 24	Matches all prefixes in the 11.0.0.0/24 address space and the subnet mask must be 24
ip prefix-list DHCPpool 1 10.66.250.64/26 ge 26 le 26	Matches all prefixes in the 10.66.250.64/26 address space and the subnet mask must be exactly 26
ip prefix-list test 10.0.0.0/16 le 30	Matches all prefixes in the 10.0.0.0/16 with a subnet mask less or equal to 30.
ip prefix-list test 192.168.0.0/24 ge 26 le 30	Matches all prefixes in the 192.168.0.0/24 with a subnet mask between 26 and 30 bits.

```
ip prefix-list CMS_SERVERS 5 140.108.21.0/24
ip prefix-list DEFAULT-ONLY 10 0.0.0.0/0
ip prefix-list DIAMETER_SOURCE 3 10.66.70.251/32
ip prefix-list DIAMETER_SOURCE 5 70.1.1.1/32
ip prefix-list LOCAL_INTERFACES 5 72.1.1.1/32
ip prefix-list LOCAL_INTERFACES 7 70.1.1.1/32
ip prefix-list LOCAL_INTERFACES 9 13.1.1.0/24
ip prefix-list LOCAL_INTERFACES 10 130.81.1.115/32
ip prefix-list LOCAL_INTERFACES 20 11.0.0.1/32
ip prefix-list LOCAL_INTERFACES 25 11.0.1.1/32
ip prefix-list LOCAL_INTERFACES 30 11.0.2.1/32
ip prefix-list LOCAL_INTERFACES 35 11.1.0.1/32
ip prefix-list LOCAL_INTERFACES 40 11.2.0.1/32
ip prefix-list LOCAL_INTERFACES 45 11.4.0.1/32
ip prefix-list NETCONF 5 172.30.127.0/24
ip prefix-list NSP_SERVERS 5 138.83.161.0/24
ip prefix-list NTP_SOURCES 5 130.81.248.130/32
ip prefix-list PTY_ACCESS_NETWORKS 5 172.29.255.0/24
ip prefix-list RADIUS_SERVERS 3 70.1.1.1/32
ip prefix-list RADIUS_SERVERS 5 10.66.70.251/32
```

```
ip prefix-list RADIUS_SERVERS 10 70.1.1.1/32
ip prefix-list SLIP2-SERVERS 5 206.46.232.195/32
ip prefix-list VOL-DHCPv4-POOL 1 11.0.0.0/24 ge 24 le 24
ip prefix-list VOL-DHCPv4-POOL 10 11.0.1.0/24 ge 24 le 24
ip prefix-list VOL-DHCPv4-POOL 15 11.0.2.0/24 ge 24 le 24
ip prefix-list VOL-DHCPv4-POOL 20 11.1.0.0/24 ge 24 le 24
ip prefix-list VOL-DHCPv4-POOL 25 11.2.0.0/24 ge 24 le 24
ip prefix-list VOL-DHCPv4-POOL 30 11.4.0.0/24 ge 24 le 24
ip prefix-list SMTP-ALLOW 5 68.142.203.0/24
ip prefix-list WG_ALLOW LIST_IP 5 52.1.132.62/32
ip prefix-list WG_ALLOW LIST_TCP 5 63.140.32.0/19
```

Creating a COSQ Profile

This topic describes how to create a COSQ profile to apply to an Ethernet or PON interface.

Note: To create a CoSQ profile to apply to a CoPP, see 'Creating a CoPP CoSQ Profile' in the *AXOS Turn-Up and Transport Guide*.

Guidelines

- An Ethernet interface can support a maximum of 8 CoS (8-SP or 8-WRR)
- A PON interface can support a maximum of 6 CoS (3-SP or 3-WRR)

  Note: On a PON interface you can configure CoSQ entries 3–8 with min/max bandwidth, however the queue-depth and weight parameters are ignored.

- Use the default CoSQ profile (identified as 'DEFAULT') is intended for Ethernet interfaces. This profile consists of the default parameters listed in the following table with cosq-entries 1–8 and cannot be changed.

Parameters

Parameter	Description
cos cosq-profile <Profile name>	A unique name for the CoSQ profile. Valid Values: • A string of up to 48 characters, including letters, numbers, and special characters:_ (underscore), - (hyphen), . (dot) • (E9-2 only) default CoSQ profile name is DEFAULT.
cosq-group-scheduling-type	Specifies the scheduling policy. Valid values: • SP (default): All CoS queues operate in strict priority order. With strict priority queuing, all traffic (in the queues) with the highest priority is delivered to the network first, then the lower priority queue traffic is delivered. For example, a frame with priority 5 transmits from the queue before a frame with priority 0. • WRR: All CoS queues operate in Weighted Round Robin order. *An equal weight value is assigned to each CoS queue*, similar to simple Round Robin (RR) scheduling. The scheduler alternates between each queue and transmits the same number of frames from each queue. • 1SP-7WRR: The highest priority queue operates in strict priority order. The remaining queues operate in Weighted Round Robin order. With SP-WRR queuing, traffic on the SP queues receive higher priority, and the bandwidth cannot be limited. Therefore traffic in the SP queue receives the highest priority and minimum bandwidth cannot be guaranteed for the WRR queues. • 2SP-6WRR: The two highest priority queues operate in strict priority order. The remaining queues operate in Weighted Round Robin order. With SP-WRR queuing, traffic on the SP queues receive higher priority, and the bandwidth cannot be limited. Therefore traffic in the two SP queues receive the highest priority and minimum bandwidth cannot be guaranteed for the WRR queues. • 3SP-3WRR:Three traffic classes in SP and three traffic classes in WRR mode. • 8-SP: All 8 Traffic class in Strict Priority (SP) mode • 8-WRR: All 8 traffic classes in Strict Priority (SP) mode.

Parameter	Description
cosq-entry	A CoS queue for forwarding traffic. Refer to AXOS Turn-up and Transport Guide for CoSQ ID to CoS type mapping, as well as default protocol to CoSQ ID mapping. For SP, higher CoS queue numbers have higher priority. Valid values: • 1–64
bandwidth minimum bandwidth maximum	Specifies the minimum and maximum bandwidth rate for the given CoS queue. The maximum bandwidth must be greater or equal to the minimum bandwidth. Valid values: • 0–100000000 (kbps in 64K increments) 0=default (unlimited)
discard-policy	Specifies the discard policy for congestion avoidance. Valid values: • WRED (default): Weighted random early detection per queue. Drops lower priority traffic before higher priority traffic if the configured queue depth is exceeded. • TAIL-DROP: Drops frames when a queue is full. This allows for effective use of the full available queue depth, but may result in abrupt dropping of traffic. Tail-drop treats all traffic equally and does not differentiate between traffic classes. Select WRED for metered queues to ensure that the maximum queue depth is enforced. Metered queues are shared across multiple services and experience more congestion than shaped queues which are dedicated to a single service.
queue-depth	Specifies the maximum queue buffering memory (in bytes) of the CoS queues. Valid values: • 0–100000000; 0=default (unlimited)
weight	Specifies the scheduling weight, applicable only to WRR configurations only. Valid values: • 1–100; default=1

•

Creating a DSCP Map (E9-2 CLX)

AXOS protocols send messages at a specified DSCP and VLAN PCP value. This topic describes how to create a custom DSCP map to define DSCP to PCP mappings at the WAN LAG uplink for control plane traffic generated by the E9-2 CLX. You apply a DSCP map to the CoPP.

If you do not create and apply a DSCP map, the values shown in the table below are used by default.

Protocol	DSCP Per-Hop Behavior (PHB)	Binary Value	DSCP Value	802.1p PCP (S-Tag)
BNG				
Diameter (PCRF)	BE-CS0	000 000	0	N/A[1]
DHCPv4:				
• Discover	CS6	110 000	48	7
• Offer	BE-CS0	000 000	0	0
• Request	CS6	110 000	48	7
• Ack	BE-CS0	000 000	0	0
DHCPv6:				
• Solicit	BE-CS0	000 000	0	7
• Advertise	BE-CS0	000 000	0	0
• Request	BE-CS0	000 000	0	7
• Reply	BE-CS0	000 000	0	0
ICMP (WAN):				
• Ping request	BE-CS0	000 000	0	0
• Ping response	BE-CS0	000 000	0	0
• Traceroute request	BE-CS0	000 000	0	0
Lawful Intercept:				
• LI packets to LI decoder	BE-CS0	000 000	0	0
• Mirrored packets	CS5	101 000	40	0
RADIUS (subscriber accounting)	BE-CS0	000 000	0	N/A[1]

Protocol	DSCP Per-Hop Behavior (PHB)	Binary Value	DSCP Value	802.1p PCP (S-Tag)
WAN				
BFD	BE-CS0	000 000	0	7
eBGP	CS6	110 000	48	0
iBGP	CS6	110 000	48	0
IGMPv2	CS3	011 000	24	0
ISIS	N/A	N/A	N/A	0
OSFP	CS6	110 000	48	0
PIM-SM	CS6	110 000	48	0
RIP	BE-CS0	000 000	0	0
TACACS Device Authentication	BE-CS0	000 000	0	N/A[2]
Other				
IPC (between aggregation and access cards)	AF12 (ipcfwd) BE-CS0 (ICMP)	001 100 000 000	12 0	N/A
IPFIX	BE-CS0	000 000	0	N/A[3]
Name resolution queries	BE-CS0	000 000	0	0
NTP	EF	101 110	46	N/A[2]
SSH, SFTP, SCP (inband WAN and craft interface)	BE-CS0	000 000	0	TBD
Syslog	BE-CS0	000 000	0	N/A[2]

[1] Packets captured at the remote side.

[2] Outgoing via the craft interface.

[3] Checked via system-craft interface.

.

Guidelines

- A DSCP map configured on a CoPP only applies to egress traffic, not ingress traffic that hits CoPP CoSQs.
- When a DSCP map is configured on the 'For-Me' CoPP and the global host application QoS admin state is:
  - DISABLED, packets egressing the CPU will be mapped to a PCP value based on a packet's DSCP value.
  - ENABLED, any protocol mapped (DSCP to PCP) via the host application QoS functionality will override the DHCP map.
- You cannot set DSCP values independently per protocol; if multiple protocols set the same DHCP PHB value, they receive the same PCP value, with the following exceptions:
  - Diameter (PCRF)
  - ICMP (WAN) ping requests
  - RADIUS (subscriber accounting)
- You can create a DSCP to PCP mapping to change the PCP value for any given DSCP PHB.
- You can apply the default DSCP map named "UNI" to the CoPP, if desired; when applied, the following DSCP to PCP mapping is used:

```
Profile Name: UNI
DSCP        PCP
----------------
AF11(10)    1
AF12(12)    1
AF13(14)    1
AF21(18)    2
AF22(20)    2
AF23(22)    2
AF31(26)    3
AF32(28)    3
AF33(30)    3
AF41(34)    4
AF42(36)    4
AF43(38)    4
BE/CS0(0)   0
CS1(8)      1
CS2(16)     2
CS3(24)     3
CS4(32)     4
```

```
CS5(40)     5
CS6(48)     5
CS7(56)     5
EF(46)      5
VA(44)      5
Default : 0 (p-bit for DSCP values not in map)
```

Procedure

To create a DSCP Map Profile via the SMx

1. From the menu bar, click **Profiles**.
2. In the Quick Links menu, click **Common** > **DSCP Map**.
3. In the Global DSCP Map Profile panel, click **Create**.
4. In the Create DSCP Map Profile panel, reference the table below and do the following:
   a. Click in the Name box and enter a name for the profile.
   b. Click the down arrow to select a DSCP value.
   c. Click the down arrow to select a PCP value.
   d. Click **Submit** to save your profile.

Creating a DSCP map profile via the CLI

1. From configuration mode, create a unique name for the DSCP map profile.

   ```
   dscp-map <name>
   ```

2. Specify a PHB or DSCP value followed by a PCP value. For all possible values, see parameter descriptions.

   ```
   dscp <PHB or DSCP value> <PCP value>]
   ```

Parameters

You can configure the following parameters to create a DSCP map profile:

CLI Parameter	SMx Parameter	Description
dscp-map <map name>	Name	A unique name for the DSCP map. Valid values: • A unique name for the DSCP map, consisting of a string of up to 48 characters, including letters, numbers, and special characters:]_ (underscore), - (hyphen), . (dot) • UNI (default), which provides the following values: **Profile Name: UNI** **DSCP PCP** **----------** **AF11(10) 1** **AF12(12) 1** **AF13(14) 1** **AF21(18) 2** **AF22(20) 2** **AF23(22) 2** **AF31(26) 3** **AF32(28) 3** **AF33(30) 3** **AF41(34) 4** **AF42(36) 4** **AF43(38) 4** **BE/CS0(0) 0** **CS1(8) 1** **CS2(16) 2** **CS3(24) 3** **CS4(32) 4** **CS5(40) 5** **CS6(48) 5** **CS7(56) 5** **EF(46) 5** **VA(44) 5** **Default : 0 (p-bit for DSCP values not in map)**

CLI Parameter	SMx Parameter	Description
dscp <PHB>	DSCP	Specifies a DSCP per-hop behavior (PHB) or Differentiated Services Code Point (DSCP) value. DSCP PHB or hex value (0x00-0x3F) or decimal value (0-63). Valid values: • AF11: Assured Forwarding Class 1 - Low Drop(10) • AF12:Assured Forwarding Class 1 - Medium Drop(12) • AF13:Assured Forwarding Class 1 - High Drop(14) • AF21: Assured Forwarding Class 2 - Low Drop(18) • AF22:Assured Forwarding Class 2 - Medium Drop(20) • AF23:Assured Forwarding Class 2 - High Drop(22) • AF31:Assured Forwarding Class 3 - Low Drop(26) • AF32: Assured Forwarding Class 3 - Medium Drop(28) • AF33: Assured Forwarding Class 3 - High Drop(30) • AF41: Assured Forwarding Class 4 - Low Drop(34) • AF42: Assured Forwarding Class 4 - Medium Drop(36) • AF43: Assured Forwarding Class 4 - High Drop(38) • BE-CS0: Best Effort • CS1: Class Sector 1(8) • CS2: Class Sector 2(16) • CS3: Class Sector 3(24) • CS4: Class Sector 4(32) • CS5: Class Sector 5(40) • CS6: Class Sector 6(48) • CS7: Class Sector 7(56) • EF: Expedited Forwarding(46) • VA: Voice Admit(44)
<pcp>	PCP	0-7

Creating IP Access Control Lists

This topic describes how to create IPv4 or IPv6 access control lists (ACLs) to accomplish packet filtering, and is organized as follows:

- Configuration guidelines | Procedures | Parameters

Configuration guidelines

- Relationship to other profiles and objects:
  - **ACL** > interface for in-band or out-of-band management (IPv4 access group)
  - **ACL** > control plane (IPv4 or IPv6 access group)
  - **ACL** > VLAN interface (IPv4 or IPv6 access group) > Layer 3 VLAN
  - **ACL** > WAN Ethernet interface (IPv4 or IPv6 access group)
  - **ACL** > ONT Ethernet interface (service VLAN IPv4 or IPv6 access group)
- ACLs are currently supported for ingress traffic (by default, no keyword required)
- ACLs are currently supported for Layer 3 IPv4 and IPv6 applications, and must be specified for one or the other
- AXOS does not support IPv6 ACLs with prefixes greater than /64 (e.g., /128).
- For match rules, see below
- For matching packets, ACLs can count, deny, or permit packets. For use with the control plane object only, ACLs can specific a CPU QoS queue.
- If a packet does not match any rule, it will be denied (or dropped). An implicit, non-configured drop rule is used for this, identified by sequence number 65535 when viewing statistics. For example:

```
SEQ      HIT
NUM      ACTIONS  COUNTER
-------------------------
65535    d/c/-    95615821
```

- ACLs take precedence over packets trapped to the CPU. For example, if an ACL does not permit DHCP packets, DHCP packets will be dropped by the ACL instead of being trapped to the CPU.
- ACLs may be applied to:
  - In-band or out-of-band management interface
  - The control plane
  - Layer 3 VLANs (via VLAN interface)
  - WAN Ethernet interfaces
  - ONT Ethernet interfaces

Note: On ONTs, there is no command to see packet counts.

Procedure

To create an IP access list (via CLI)

1. In the CLI configuration mode, enter the starting point command "access-list ipv4" and enter a unique name for the access control list.

```
access-list ipv4 <name>
```

2. Reference the table below to configure other parameters as required.

Example

```
access-list ipv4 ACL_L3HSI
rule 5 match destination-ipv4-network 224.0.0.0/4
rule 5 action deny
rule 5 description "DENY MULTICAST"
rule 10 match protocol 1
rule 10 action permit
rule 10 description "PERMIT ICMP"
rule 15 match destination-ipv4-network 172.16.1.0/24
rule 15 action permit
rule 15 description "PERMIT ATL TELEMETRY"
rule 20 match destination-port-range 25
rule 20 action permit
rule 20 description "RESIDENTIAL FILTER PERMIT SMTP"
top
```

Parameters

You can configure the following parameters to create an ipv4 access control list.

Parameter	Description
access-list ipv4 <name>	A unique name for the IPv4 access list. Valid value: • A string of up to 48 characters, including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot)
description	Description for the access list. Valid value: • A string up to 48 characters.
rule <n>	Sets a sequence number for the rule, and adds the rule to the ACL. **Note**: ACL rules are evaluated in the order entered into the system. Valid values: • 1–1024

Parameter	Description
rule <n> action	Action to be performed when the traffic flow matches the associated rule. Valid values: • count: Enables counting for packets that hit this rule • cpu-cosq <1–48>: Specifies the CoS queue identifier that permitted traffic is mapped to **Note**: This value maps to the 'cosq-entry' parameter specified in the CoSQ profile. For permitted traffic, specify both a permit and cpu-cosq action. • deny: Drop matching packets • permit: Pass matching packets
rule <n> description	Description for the specified ACL rule. Valid value: • A string up to 48 characters.
rule <n> match	Per rule number match criteria. Press the tab key twice to display well-known enumerations and values, if applicable. Valid values: • any: Match all traffic. • destination-ipv4-network: Matches a destination IP address and prefix. Syntax: <ip address/prefix>. Valid values for IPv4 prefix: 0–32. **Note**: A destination address that is not one of the host's IP addresses is accepted, however the rule does not function. • destination-ipv4-prefix-list: Matches an IPv4 prefix-list receiving the packet. Valid value: Name of any previously configured IPv4 prefix list. • destination-port-range: Specifies the destination TCP/UDP port(s) to match as a range or as a single value. If specified, upper port must be greater than or equal to lower port. Well-known enumeration or value. • *dscp: Differentiated Services Code Point. Valid values: DSCP PHB or hex value (0x00-0x3F) or decimal value (0-63). • *icmp-type: Specifies the Internet Control Message Protocol (ICMP) type number to match. Well-known enumeration or value. • *protocol: Specifies the Internet protocol enumeration or number in an IPv4 packet header to match. Valid values: 0–255. • source-ipv4-network: Matches the source IP address and prefix. Syntax: <ip address/prefix>. Valid values for IPv4 prefix: 0–32. • source-ipv4-prefix-list: Matches an IPv4 prefix-list sending the packet. Valid value: Name of any previously configured IPv4 prefix list. • source-port-range: Specifies the lower/upper boundary of the source TCP/UDP ports to match as a range or as a single value. Well-known enumeration or value. • *tos: IPv4 Type Of Service. Valid values: 8-bit value expressed in decimal (0–255) or hex (0x00–0xff). • tracking-state: Connection tracking state. Valid values: ESTABLISHED, INVALID, NEW, RELATED. ***Note:** Not applicable to the E7-2 for applying an access list to management interfaces.

You can configure the following parameters to create an ipv6 access control list.

Parameter	Description
access-list ipv6 <name>	A unique name for the IPv6 access list. Valid values: • A name for the ACL, consisting of a string of up to 48 characters, including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot)
description	Description for the access list. Valid value: • A string up to 48 characters.
rule <n>	Sets a sequence number for the rule, and adds the rule to the ACL. **Note**: ACL rules are evaluated in the order entered into the system. Valid values: • 1–1024
rule <n> action	Action to be performed when the traffic flow matches the associated rule. Valid values: • count: Enables counting for packets that hit this rule • cpu-cosq <1–48>: Specifies the CoS queue identifier that permitted traffic is mapped to **Note**: This value maps to the 'cosq-entry' parameter specified in the CoSQ profile. For permitted traffic, specify both a permit and cpu-cosq action. • deny: Drop matching packets • permit: Pass matching packets
rule <n> description	Description for the specified ACL rule. Valid value: • A string up to 48 characters.
rule <n> match	Per rule number match criteria. Press the tab key twice to display well-known enumerations and values, when applicable. Valid values: • any: Match all traffic. • destination-ipv6-network: Matches a destination IP address and prefix. Syntax: <ip address/prefix>. Valid values for IPv6 prefix: 0–64. • destination-ipv6-prefix-list: Matches an IPv6 prefix-list receiving the packet. Valid value: Name of any previously configured IPv6 prefix list. • destination-port-range: Specifies the destination TCP/UDP port(s) to match as a range or as a single value. If specified, upper port must be greater than or equal to lower port. Well-known enumeration or value. • dscp: Differentiated Services Code Point. Valid values: DSCP PHB or hex value (0x00-0x3F) or decimal value (0-63). • icmp-type: Specifies the Internet Control Message Protocol (ICMP) type number to match. Well-known enumeration or value. • next-header: IPv6 Next Header number. Well-known enumeration or value. • source-ipv6-network: Matches the source IP address and prefix. Syntax: <ip address/prefix>. Valid values for IPv6 prefix: 0–64. • source-ipv6-prefix-list: Matches an IPv6 prefix-list sending the packet. Valid value: Name of any previously configured IPv6 prefix list. • source-port-range: Specifies the lower/upper boundary of the source TCP/UDP ports to match as a range or as a single value. Well-known enumeration or value. • tracking-state: Connection tracking state. Valid values: ESTABLISHED, INVALID, NEW, RELATED. • traffic-class: IPv6 Traffic Class. Valid values: 8-bit value expressed in decimal (0–255) or hex (0x00–0xff).

Creating and Modifying Transport Service Profiles (TSPs)

This topic describes how to create and modify transport service profiles (TSPs), and is organized as follows:

- Overview | Configuration guidelines | Procedures | Parameters

Overview

Transport service profiles (TSPs) facilitate the transport of tagged traffic without any manipulation. A TSP contains a list of VLAN IDs, and is applied to an interface to instantiate each VLAN on the interface. TSPs are applied to INNI Ethernet or LAG interfaces, which may in turn be used as interfaces in a transport ring.

Configuration guidelines

- You may create one or more new TSPs (with descriptive profile names) as well as use the system default "SYSTEM_TSP."

  Note: Some AXOS systems are pre-configured with SYSTEM_TSP containing the default management VLAN (999) and applied to a Layer 2 single-port uplink (e.g., 1/1/x1). If VLAN 999 is not required in the SYSTEM_TSP, it may be removed; if the SYSTEM_TSP is not required on 1/1/x1, it may be removed from that interface.

- For a TSP associated with a non-ring interface (simplex or LAG), add all the VLANs either serving or passing through the node, including the management VLAN (if required).
- For a TSP associated with transport ring interfaces on a given node:
  - For transit nodes: Add all the VLANs either serving or passing through the node.
  - For the primary node: Add all the VLANs passing through the node.

  Note: (E7-2 rings only) If a VLAN is only "passing through" a node, it does not have to be created on the node; it only has to be defined in the TSP used by the node. Only VLANs serving a given node must be created on the node.

- You can apply only one TSP per interface; however, you can modify an existing TSP to add or remove additional VLANs as needed.
- SMx vs. AXOS CLI usage
  - Creating, applying, and editing TSPs may be done via CLI or SMx.
  - Creating and applying TSPs is usually done via CLI during the configuration of uplink/transport interfaces.
  - Editing TSPs is usually done via SMx after new service VLANs are created in SMx.

Procedure

To create a Transport Service Profile (TSP) [via CLI]

1. Enter a name for the TSP.

```
Calix-1(config)# transport-service-profile <name>
```

2. (Optional) Enter a description for the TSP.

```
Calix-1(config-transport-service-profile-<name>)# description
<string>
```

3. Specify a VLAN ID or range of VLAN IDs to add to the TSP.

```
Calix-1(config-transport-service-profile-<name>)# vlan-list <VLAN
ID>
```

Example

The following example creates a TSP named 'uplink_TSP' and adds VLAN IDs 45, 88, 150, and 100–120 to the TSP

```
transport-service-profile uplink_TSP
vlan-list 45,88,150
vlan-list 100-120
```

To modify a Transport Service Profile (TSP) [via CLI]

1. Enter the name of the TSP to modify.

```
Calix-1(config)# transport-service-profile <name>
```

2. If required, specify a VLAN ID or range of VLAN IDs to add to the TSP.

```
Calix-1(config-transport-service-profile-<name>)# vlan-list <VlanID>
```

3. If required, specify a VLAN ID or range of VLAN IDs to remove from the TSP.

```
Calix-1(config-transport-service-profile-<name>)# no vlan-list <VLAN
ID>
```

Example

The following example adds new VLAN IDs 90 and 121–135 to the TSP and removes VLAN ID 150

```
transport-service-profile uplink_TSP
vlan-list 90
vlan-list 121-135
no vlan-list 150
```

Parameters

You can configure the parameters below to create a transport service profile:

Parameter	Description
transport-service-profile <profile name>	A unique name for the transport service profile. Valid values: • A string of up to 48 characters, including letters, numbers, and special characters: _ (underscore), - (hyphen), . (dot) • SYSTEM_TSP
description	Description for the TSP. Valid values: • A string of up to 48 character
vlan-list	A list of VLAN IDs separated by a comma, or a range of VLANs separated by a hyphen (for example, 100–105) to add to the TSP. Valid values: • a–b, c, d where each letter represents a VLAN ID (1–4094)

Creating an ENNI PCP Map

This topic describes how to create an ENNI PCP Map profile, and is organized as follows:

- Overview | Procedures | Parameters

Overview

An ENNI PCP Map profile allows P-bits to be modified on an uplink interface.

Procedures

To create a PCP Map Profile (via SMx)

1. From the menu bar, click **Profiles**.
2. In the Quick Links menu, click **Common > ENNI PCP Map**.
3. In the Global ENNI PCP Map Profile panel, click **Create**.
4. In the Create ENNI PCP Map Profile panel, do the following:
   a. Reference the table below to provision the parameters.
   b. Set a value for the **Set PCP To** field for each Ingress PCP (Primary Control Point) as needed.
   c. Click Submit to save your profile.

To create a PCP Map Profile (via CLI)

1. In the CLI configuration mode, enter the starting point command "pcp-map" and enter a unique name for the profile.

```
pcp-map <name>
```

2. Reference the table below to configure other parameters as required.

Example

```
pcp-map pcpmap1
pcp 0 set-pcp 1
pcp 1 set-pcp 1
pcp 6 set-pcp 5
pcp 7 set-pcp 5
!
```

Parameters

You can configure the parameters below to create a PCP map:

CLI Parameter	SMx Parameter	Description
pcp-map <name>	Name	Enter a name for this profile. Valid values: • a string of up to 48 characters, including letters, numbers, and special characters:_ (underscore), - (hyphen), . (dot)
pcp <pcp value> set-pcp <pcp value>		(CLI only) Select an incoming PCP value to map. Valid values: • 0-7
pcp <pcp value> **set-pcp <pcp value>**	Set PCP To	Select a PCP value to set the incoming PCP vlaue to. Valid values: • (SMx only) No change • 0-7

Configuring Ethernet Interface Parameters

This topic describes how to configure an Ethernet interface, and is organized as follows:

- Procedures | Parameters

Procedures

To configure an Ethernet interface (via CLI)

1. Navigate to an Ethernet interface.
2. Enter parameter values as required.

Example

```
configure
interface ethernet 1/1/x1
...
no shutdown
```

Parameters

You can configure the following parameters for an Ethernet interface:

Ethernet interface parameters > top level

Parameter	Description
Starting point	
interface ethernet <interface name>	An Ethernet interface of an AXOS system. Valid values: • <shelf>/<slot>/<port type><port number> Where <port type> is c, q, x, or g, where • c is for CDFP 400GE (4x100GE) ports • q is for QSPF 100GE/40GE ports • x is for 10GE port • g is for 1GE ports For example (via CLI): • interface ethernet 1/1/x1
Key parameters	
switchport	(Only available if no role is selected) Configures the switchport mode on the interface. Valid values: • ENABLED (default): switched (Layer 2) interface • DISABLED: routed (Layer 3) interface

Parameter	Description
role	(Only available if switchport = enabled) Configures the service role for the interface. Choose a supported role for your system hardware and use case, such as inni, lag, or uni. Valid values: • none (default) • bonded-group: Part of the ethernet bonded group • enni: External network to network interface • fullbridge: Subtended member of full bridge • icl: Inter-chassis link • inni: Internal network to network interface • lag: Part of a link aggregation group • mirror: Mirror network to network interface • nid: Subtended member of network interface device • rg: Subtended member of residential gateway • uni: User network interface **Note:** Some roles are not applicable or not supported.
All parameters	
access-group ipv4-acl	(Only available if switchport = disabled) Applies an IPv4 access control list (ACL) to the Ethernet interface. Valid values: • Name of previously defined IPv4 access-list
access-group ipv6-acl	(Only available if switchport = disabled) Applies an IPv6 access control list (ACL) to the Ethernet interface. Valid values: • Name of previously defined IPv6 access-list
alarm-suppression	Enables or disables suppression of all alarms associated with the interface. Valid values: • enabled • disabled (default)
arp	Interface arp configuration. Valid values: • arp-accept <disable (default)|enable> • arp-announce {any|prefer primary|source-ip-in-target-subnet} • arp-filter <disable (default)|enable> • arp-ignore {any|do-not-reply|source-ip-in-target-ip-subnet|target-ip-on-received-interface|target-ip-scope-not-local} • arp-notify <disable (default)|enable> • drop-gratuitous-arp <disable (default)|enable> • proxy-arp <<disable (default)|enable> • proxy-arp-pvlan <disable (default)|enable>
cosq	Applies a Class of Service queue (CoSQ) profile to the interface. Valid values: • Name of previously defined cosq profile
description	Applies a description to the interface. Valid values: • description in string format

Parameter	Description
dot1x state	802.1X configuration. Valid values: • enabled • disabled (default)
dot1x username	802.1X configuration. Valid values: • user name in string format
dot1x supplicant state	802.1X configuration. Valid values: • enabled • disabled (default)
dot1x supplicant username	802.1X configuration. Valid values: • user name in string format
dot 1x supplicant password	The password string for authentication. It is stored with a cipher string. Valid values: • password in string format
dscp-map	Binds a DSCP to PCP map profile to this interface. Valid values: • Name of a previously configured DSCP to PCP map profile.
dtag-vlan	Specifies a pre-configured S-VLAN and C-VLAN to create a double-tagged service on the Ethernet port. Format: dtag <s-vlan> <c-vlan>
dtag-vlan <s-vlan> <c-vlan> meg	Name of a Maintenance Entity Group (MEG), consisting of a text string, to add a MEG configuration to the specified double-tagged service. For an explanation of possible completions for the MEG configuration, see the meg command.
duplex	Configures the duplex mode for the interface. valid values: • auto (default): Duplex mode is negotiated with the link partner through auto-negotiation. • half: Either transmits or receives packets at a given time. Uses Carrier Sense Multiple Access (CSMA) to detect collisions and recover. • full: Transmits and receives packets at the same time.
dwdm-channel	Tunable DWDM module channel setting. Represents a channel number in ITU-T G694.1 frequency grid of fixed channel spacing at 50GHz or 100GHz. The most common 50-GHz grid is from 1 (190.100 THz) to 72.5 (197.250 THz). Valid options: • 1 - 72.5 (supported entry by the AXOS CLI) • 13.5 - 61 (supported by Calix DWDM SFP+ optics)
egress shaper maxburst	Egress shaper burst BW Valid values: • <0-4 MBytes> (default = 0)
egress shaper maximum	Egress shaper maximum BW (in 64K increments) Valid values: • <0-10000000> (default = 0)

Parameter	Description
erps-ring	ERPS ring associations and primary/secondary lag group role assignment Valid options: • domain-id • role (default = none)
ethertype	Configures the Ethertype for the interface. Sets the Ethertype to match; the Ethertype indicates the protocol transported in the Ethernet frame. Valid values: • 0x8100 (default) - IEEE 802.1Q-tagged (default setting) • 0x88a8 - IEEE 802.1AD S-Tag • 0x88ab - ETHERNET Powerlink (EPL) real-time protocol • 0x9100 - Q-in-Q (double tagged)
fec	Desired state of attribute. Valid values: • DISABLED (default) • ENABLED
flow-control	Configures the flow control setting for the interface. This setting applies back pressure to a transmitter that is outrunning the receiver's capacity to process incoming data. Valid values: • none (default): Does not send pause packets and does not honor the partner link's pause packets. • auto: Pause attribute is negotiated with the partner link. • rx-tx: Sends pause packets and honors the partner link's pause packets. • rx-pause: Honors the partner link's pause packets and stops transmitting, when asked. • tx-pause: Sends pause packets to the partner link, when needed. A pause packet notifies the partner link to temporarily suspend sending of packets when traffic congestion occurs to help avoid dropping of packets. Flow control must be enabled on both the ingress and egress interfaces.
g8032-ring	(Only available if role = inni) G.8032 ring associations and ethernet port ring rpl-mode assignment. Valid values: • rpl-mode • ccm-protection rpl-mode: G.8032 ring instance ethernet port RPL mode Valid options: • inter-connect: G.8032 ring instance port role sub-ring inter-connect • neighbor: G.8032 ring instance port role neighbor • none(default): G.8032 ring instance port role none • owner: G.8032 ring instance port role owner ccm-protection: Type of MEG to use for ring protection Valid options: • auto (default) • mep • name • identifier

Parameter	Description
ip	(Only available if switchport = disabled) Configures IPv4 parameters on this interface. Valid values: • address • rip • vrf • neighbor
ip-unicast-rpf	Configures parameters for unicast Reverse path forwarding (RPF) on an Ethernet interface. Valid values: • loose: Configures loose mode uRPF on the interface. Loose mode checks each incoming interface against the routing table, and the packet is dropped only if the source address is not reachable via any interface. • strict: Configures strict mode uRPF on the interface. Strict mode checks each incoming packet against the routing table and if the incoming interface is not the best reverse path, the packet is discarded.
ipv6	(Only available if switchport = disabled) Configures IPv6 parameters on this interface. Valid values: • address • neighbor
isis	(Only available if switchport = disabled) IS-IS interface configuration. Opens up a new level of provisioning.
l2transport	L2 Transport Information Valid values: • bridge-domain: Bridge-domain information for L2Transport • point-to-point: P2P information for L2Transport • rewrite-ingres: Explicit tag rewrite option for ingress • rewrite-ingres dot1q: value to be written • rewrite-ingres tag: TAG information for rewriting
lacp-port-priority	(Only available if role = lag) Ethernet port LACP port priority. Valid values: • 0-65535 (default = 32768)
lacp-port-timeout	Ethernet port LACP port timeout. Valid values: • long • short (default)
lldp admin-state	Sets the Link Layer Discovery Protocol (LLDP) agent on an Ethernet interface. Administrative state of the LLDP agent. Valid values: • disabled: Disable LLDP agent • enabled: Enable LLDP agent for receive and transmit operations

Parameter	Description
lldp destination-agent	Select the LLDP destination agent type to send and receive LLDP PDUs on. Valid values: • nearest-bridge(deafult): Propagation is constrained to a single physical link; stopped by all types of bridge. • nearest-non-tpmr-bridge: Propagation is constrained by all bridges other than Two-port MAC Relays (TPMRs); intended for use with provider bridged networks. • nearest-customer-bridge: Propagation is constrained by customer bridges; this provides the same coverage as a customer-customer MAC connection.
lldp notifications	Generates neighbor notification events. Valid values: • enabled (default) • disabled
lldp profile	Name of a previously configured LLDP profile for the LLDP agent to use. A LLDP profile defines which optional TLVs to transmit and/or suppress by the LLDP agent. When the LLDP agent is enabled, the agent sends a set of mandatory default TLVs, unless overridden by an LLDP profile. The set of default TLVs is determined by the service role of the port when the agent is active.
mep	Adds a MEP reference to the transport service. Enter the following parameters in sequence: • MEG name: Previously configured MEG name. • MEP ID: Previously configured identifier for the MEP within the MEG. • MEP ID Valid values: • 1-8191
mpls	MPLS configuration. Valid values: • discovery-hello: Configure mpls ldp interface discovery-hello timers • discovery-hello hold-time: Set mpls discovery-hello holdtime • keep-alive: Configure mpls ldp interface keepalive timers • keep-alive hold-time: Set mpls keepalive holdtime • state: Enable/Disable mpls ldp on interface vlan Valid values for state • enable • disable (default) Valid values for discovery-hello hold-time: • 30-65535. (default = 45) Valid values for keep-alive hold-time: • 30-65535. (default = 40)
mpls-exp-map	MPLS EXP to traffic class map applied to tunnel-switch labels on LAG/interface
mtu	Configures the MTU for the interface. The MTU value for the interface. Valid values: • 1500–9600 (default = 2000)
native-vlan	Sets the native VLAN to receive/transmit untagged frames on. Valid values: • 1–4094

Parameter	Description
protection group	Ethernet port ICL LAG protection group. ICL LAG protection group • 1: ICL protection group 1 • 2: ICL protection group 2 • auto: ICL protection group auto assignment • none: ICL protection none
rmon-session	Creates a Remote Monitoring (RMON) session for monitoring traffic that flows through Ethernet interfaces (configured for any service role). Calix recommends configuring up to two RMON sessions per Ethernet interface. Opens up a new level of provisioning.
role	(See description in "Key parameters," above.)
rstp cost	Configures the RSTP path cost, which is the cost of transmitting a frame onto a network through the interface. It is assigned according to the speed of the bridge. The slower the media, the higher the cost. Valid values: • 1–200000000; (default = 4)
rstp domain	Runs RSTP on the interface in the specified RSTP domain.
rstp priority	Configures the interface priority to determine which interface should be disabled when more than one forms a loop. Interfaces with a higher priority numeric value are disabled first. Valid values: • 0–240 in multiples of 16; (default = 128).
rstp topology	Specifies the MAC for RSTP BPDUs. Valid values: • 1d-addr (default) results in the AXOS system transmitting BPDUs with a DA of 01:80:C2:00:00:00. Use this selection when the node is connected to an 802.1d compliant switch with redundant link. • 1ad-addr results in the AXOS system transmitting BPDUs with a DA of 01:80:C2:00:00:08. Use this selection when the node is connected to an 802.1ad compliant switch with redundant link.
sampling-point	IPFIX sampling-point reference.
slot-lag	(Only for E9 access card q1 to q4 ports) Ethernet port slot LAG membership. Valid values: • la1
shutdown	Configures the administrative state for the interface. Valid values: • no shutdown (default) • shutdown

Parameter	Description
speed	Configures the data rate of the interface. Data rate of port (bits/s). Valid values: • 1Gbs • 2.5Gbs • 10Gbs • 10Mbs • 12.5Gbs • 40Gbs • 100Gbs • 100Mbs • auto (default) • module-rate auto (default): • If the link supports auto-negotiation, the link partners auto-negotiate the speed while advertising the duplex and flow control parameters specified. • If the link does NOT support auto-negotiation, the setting is for the fastest rate that the module can support. module-rate: • This setting is for SFP+ ports. The bit rate of the installed module is forced as the port speed. No auto-negotiation takes place with this setting. Fixed speed settings force the speed to the specified value.
storm-control broadcast	Sets broadcast storm control by providing the ability to rate limit ingress broadcast, multicast and unknown unicast traffic on Ethernet interfaces in packets per second. Sets a rate limit for ingress broadcast packets. Valid values: • 1–1000000
storm-control multicast	Sets a rate limit for ingress multicast packets. Valid values: • 1–1000000
storm-control unknown-multicast	Sets a rate limit for ingress unknown-multicast packets. Valid values: • 1–1000000
switchport	(See description in "Key parameters," above.)
system-lag	(Only available if role = lag) Assign the Ethernet interface to a LAG interface. Valid values: • Previously configured LAG interface
transport-service <vlan id>	(Only available if role = inni) Configures the following transport service features on the interface: • cvlan-list <range or list of vlans> • igmp mode {router|host} • mep <meg name MEP ID, 1-8191> • mip <meg name MIP ID, 1-8191> • sampling-point <previously configured sampling point name>

Parameter	Description
transport-service-profile	(Only available if role = inni) Specifies a previously configured transport service profile. Valid values: • Previously configured TSP
vlan	(Only available if role = uni or enni) VLAN for UNI or ENNI service provisioning on the port. Opens a new level of provisioning. Valid values: • VLAN ID of previously defined service VLAN, in the range of 1-4094 Example (via CLI): • interface ethernet 1/1/x1 role uni vlan 500
vlan-l2transport	VLAN information for L2Transport. Valid values: • bridge-domain: Bridge-domain instances for VLAN L2Transport • point-to-point: P2P instances for VLAN L2Transport • point-o-point mtu: Maximum transmission unit (payload) for this point-to-point instance, MTU range [64-9192] (default = 1500) • priority-map: Priority-map-profile for VLAN L2Transport • rewrite-ingress • rewrite-ingress tag: TAG information for rewriting • rewrite-ingress translate: Translate the ingress tag • rewrite-ingress dot1q: Value to be written
vlan-l3transport	VLAN information for L3 Transport.

Ethernet interface parameters > vlan level (role = UNI)

See parameters for similiar UNI interfaces, such as for **`interface ont-ethernet`** with role = UNI.

Ethernet interface parameters > vlan level (role = ENNI)

See the following parameters:

CLI Parameter	SMx Parameter	Descrption
shutdown / no shutdown		(CLI only) Administrative state Valid values: • shutdown (disabled, default) • no shutdown
Ingress		
	Ingress Meter	(SMx only) To set the ingress limit, this field must be set to Enable. Valid values: • Enable • Disable (default)
ingress meter eir	EIR (kbps)	Ingress Meter EIR value (Kbps in 64K increments).
ingress meter ebs-bytes	Excess Burst Size (MTU Multiple)	The EBS provisioned as a factor of the MTU size configured on the interface (N*MTU), where the selected valid value = N. EBS is the maximum number of bytes available for temporary bursts above the CIR, plus EIR. Note: If the EIR is provisioned to a value greater to 0, the EBS must be provisioned to a value greater or equal to the maximum MTU in all services to which this bandwidth profile is applied.
ingress meter ebs-nxmtu	Excess Burst Size (Bytes)	The EBS provisioned as a fixed byte value. EBS is the maximum number of bytes available for temporary bursts above the CIR, plus EIR.
ingress pcp-map	PCP Map	Select an existing PCP Map to use.
Match VLAN		
match-vlan <vlan id>	Match VLAN	Match on a VLAN. Valid values • A valid VLAN
match-vlan <vlan id> **[remove-vlan <vlan id>]**	Remove Matched VLAN	Remove the matched VLAN.

Configuring Tunable DWDM SFP+ Optics

This topic describes how to configure tunable DWDM SFP+ optics via the "dwdm-channel" parameter of an Ethernet interface.

Calix AXOS systems support tunable DWDM SFP+ optics, which allow multiple 10G links to be active on the same fiber, each with a different operating wavelength. Calix supports 96 tunable channels with a supported channel range of 13.5-61.0.

Note: Only Calix keyed modules are supported. Third party (non-keyed) modules will raise a "module fault" alarm.

On SFP+ ports, the "dwdm-channel" parameter is used to specify the channel for the module to transmit on. The module can receive traffic on any of the 96 configurable channels. The operator must ensure the appropriate far end signal is delivered to the SFP+ module via the northern fiber DWDM Multiplexer.

Note: Calix recommends that you use the same channel on both sides of the link for easily identifying paired interfaces; however this is not a requirement.

To view the channels supported by an interface:

Use the following command to view the channels supported by an interface:

```
Calix-1# show interface ethernet <interface name> dwdm-map
```

Note that this is reported by the module and displayed by the E3-2, E7-2, or E9-2.

To configure a channel:

Use the following command to configure a channel:

```
Calix-1(config-ethernet-1/2/x12)# dwdm-channel <channel setting>
```

Note that any value between 1 and 72.5 may be entered, but only 13.5 – 61 are supported by Calix DWDM SFP+ optics.

To view the configuration:

Use the following commands to view information related to the configuration:

```
Calix-1# show interface ethernet 1/2/x12 status
 ...
 cfg-dwdm-channel            60.0
 oper-dwdm-channel           60.0

Calix-1# show interface ethernet 1/2/x12 module
 ...
 laser-first-frequency   " 191.350 THz"
 laser-last-frequency    " 196.100 THz"
 laser-grid-spacing      " 50.0 GHz"
 laser-dithering         " Tunable by wavelength; Tunable by channel
number; Tx Dither supported; (0x7)"
 channel-idx-set         " 94"
 wavelength-set          " 1529.55 nm"
```

Configuring Transport Service Features

This topic describes how to configure transport service features via the "transport-service" parameter of an Ethernet interface.

For Layer 2 ethernet interfaces in the INNI role, the following transport service features are available (per VLAN specified):

- C-VLAN list: Specifies a range or list of C-VLANs.
- IGMP mode: Configures an IGMP host or router instance on the specified service VLAN.
- MEP: Specifies a MEG name, MEP ID (1-8191)
- MIP: Specifies a MEG name, MEP ID (1-8191)
- sampling-point: Specifies a previously configured sampling point name.

IGMP mode considerations

If an ethernet interface is carrying MVR video traffic (via the video VLAN specified in the transport service profile), Calix recommends the following IGMP mode settings:

- For an Ethernet uplink (facing the upstream router), IGMP mode = router
- For an Ethernet downlink, IGMP mode = host

Example (IGMP mode)

```
!!Assumptions:
!!Ethernet uplink interface 1/2/x1 is carrying MVR video traffic via
VLAN !!400 specified in the transport-service-profile that is
already applied.

!!To set the IGMP mode setting of 1/2/x1 to router, do the
following:

Calix-1(config-ethernet-1/2/x1)# transport-service 400
Calix-1(config-transport-service-400)# ?
Description: Configure transport Service features
Possible completions:
  igmp   Configure a IGMP Host or Router instance on this Service
VLAN
  mep    MEP reference (MEG-name MEP ID)
  mip    MIP reference (MEG-name MIP ID)
  ---
  exit   Exit from current mode
  no     Negate a command or set its defaults
  pwd    Display current mode path
  top    Exit to top level and optionally run command
  <cr>
```

```
Calix-1(config-transport-service-400)# igmp mode
Possible completions:
  HOST     Host facing interface
  ROUTER   Multicast router facing interface
Calix-1(config-transport-service-400)# igmp mode ROUTER
```

Configuring LAG Interface Parameters

This topic describes how to configure a Link Aggregation Group (LAG), and is organized as follows:

- Procedures | Parameters

Procedures

To configure an LAG (via CLI)

1. Create a LAG with a unique name, or navigate to an existing LAG.
2. Enter parameter values as required.

Example

```
configure
interface lag la1
...
no shutdown
```

Parameters

You can configure the following parameters for a LAG interface:

LAG interface parameters > top level

Parameter	Description
interface lag <LAG group name>	A name for the LAG. Valid values: • la<n> (For example, la1). Note: The group name does not need to be the same on both nodes.
alarm-suppression	Suppress all alarms associated with the interface. Valid values: • ENABLED • DISABLED (default)
arp	Interface arp configuration. Valid values: • arp-accept <disable (default)|enable> • arp-announce {any|prefer primary|source-ip-in-target-subnet} • arp-filter <disable (default)|enable> • arp-ignore {any|do-not-reply|source-ip-in-target-ip-subnet|target-ip-on-received-interface|target-ip-scope-not-local} • arp-notify <disable (default)|enable> • drop-gratuitous-arp <disable (default)|enable> • proxy-arp <<disable (default)|enable> • proxy-arp-pvlan <disable (default)|enable>

Parameter	Description
description	Description of this LAG, consisting of up to 255 characters.
dscp-map	Binds a DSCP to PCP map profile to this interface.
ethertype	LAG group ethertype. Valid values: • 0x88a8: IEEE 802.1AD S-Tag • 0x88ab: Ethernet Powerlink • 0x8100(default): IEEE 802.1Q C-Tag
erps-ring <domain-id> role	ERPS ring associations and primary/secondary lag group role assignment. ERPS domain node interface role. Valid values: • none(default): ERPS domain node interface role none • primary: ERPS domain node interface role primary • secondary: ERPS domain node interface role Secondary
g8032-ring	G.8032 ring associations and LAG group rpl-mode assignment Valid options: • ring-instance-id • rpl-mode:G.8032 ring instance LAG group RPL mode Valid options rpl-mode: • inter-connect: G.8032 ring instance port role sub-ring inter-connect • neighbor: G.8032 ring instance port role neighbor • none (default): G.8032 ring instance port role none • owner: G.8032 ring instance port role owner
hash-method	[Applicable to E9-2 CLX systems only. For other AXOS systems, this field is located at the global level (load-balance hash-method).] Individual traffic flows use a single link in the group. The link used for each packet is based on a hash algorithm. Valid values: • dst-ip: Destination IP address • dst-mac: Destination MAC address • enhanced (default): MAC, VLAN, Ethertype for non-ip packets; source and destination ip address, source and destination port, protocol for ip packets • src-dst-ip: Source and destination IP address • src-dst-mac: Source and destination MAC address • src-dst-mac-ip: • src-ip: Source IP address • src-mac: Source MAC address
icl-active-protect	(Applicable to E9 ICL LAGs only) ICL LAG active-protect mode (or "active-standby" mode). **Note:** The non-default mode (disabled) should only be considered for Layer 2 Open Access use cases. Valid values: • enabled (default): ICL links work in active-standby mode • disabled: ICL links work in active-active mode
ip	IPv4 related configuration.

Parameter	Description
ip ospf	Configure OSPF. (Applicable to the E3-2 only, when switchport = disabled) Valid values: • area: OSPF area ID in IP address format. IPv4 address. • authentication: OSPF authentication configuration. • authentication keychain: Md5 keychain • authentication md5: MD5 Authentication • authentication text: Plain Text Authentication • cost: Interface cost (default = 1) • dead-interval: Interval after which a neighbor is declared dead (default = 40) • graceful-restart: OSPF Graceful restart • graceful-restart helper-disable: OSPF helper disable (default = false) • graceful-restart helper-strict-lsa-check-disable: OSPF helper strict lsa check disable (default = false) • hello-interval: Time between HELLO packets (default = 10) • mtu-ignore: MTU ignore (default = false) • network: Broadcast or point-to-point (default = broadcast) • passive-interface: Interface set to Passive state • enable • disable (default)
ipv6	(Applicable to the E3-2 only, when switchport = disabled)
isis	(Applicable to the E3-2 only, when switchport = disabled) IS-IS interface configuration instance. Valid values: • 1-99
l2transport	L2 Transport Information. Valid values: • bridge-domain: Bridge-domain instances for VLAN L2Transport • point-to-point: P2P instances for VLAN L2Transport • rewrite-ingress: tag(TAG information of rewriting), translate(Translate the ingress tag), dot1q(Value to be written)
lacp-actor-key	LAG group lacp actor-key
lacp-mode	Sets the LACP mode. Valid values: • none(default) • active • passive; For a static LAG, select: • none: LACP is disabled on the member ports. For a dynamic LAG, select: • active: LACP is enabled, and the LAG member ports always send LACPDUs • passive: LACP is enabled, and the LAG member ports only respond to LACPDUs. Note: For a dynamic LAG, at least one side of the LAG must be configured as LACP Mode = Active.
max-port	Configure the maximum number of member ports in the LAG at any given time. Valid values: • 1–8; (default = 8)

.

Parameter	Description
min-port	Configure the minimum number of member ports required for the LAG to remain up. Valid values: • 1–8; (default = 1)
mtu	Configure the Maximum Transmission Unit (MTU) for the LAG, specified in byte. LAG interfaces will discard any packets larger than the MTU size. Valid values: • 1500–9600; (default = 2000) The AXOS system support the ability to set the MTU size on a LAG interface to a maximum of 9600 bytes, not including the Ethernet header, two VLAN tags for Q-in-Q, and the frame check sequence (32-bit CRC). Note: MEF specifications require a minimum MTU of 1522 for Ethernet Business Services.
native-vlan	Sets the native VLAN that will receive/transmit untagged frames on.
priority-map	Priority-map-profile for LAG interface
rmon-session	Creates a Remote Monitoring (RMON) session for monitoring traffic that flows through LAG interfaces. Calix recommends configuring up to two RMON sessions per LAG.
role	Configure the service role of the LAG. When upgrading from a previous release, the AXOS system retains the configured service role, if applicable. After reverting to the factory default startup configuration, the LAG defaults to no service role. To remove the configured service role, delete any services associated with the service role, and then delete the role. Valid values: • enni • icl • inni
rstp	Rapid spanning tree configuration
shutdown	Administrative state of the LAG interface. Valid values: • no shutdown (default) • shutdown
storm-control	Ingress storm control rate limits • **Note:** Storm-control parameters are the same as described in the top-level "storm cotrol" command in the "interface ethernet" topic
switchport	State of the switchport mode. Valid values: • ENABLED (default) • DISABLED
transport-service <vlan id>	(Only available if role = inni) Configures the following transport service features on the interface: • cvlan-list <range or list of vlans> • igmp mode {router|host} • mep <meg name MEP ID, 1-8191> • mip <meg name MIP ID, 1-8191> • sampling-point <previously configured sampling point name>

Parameter	Description
transport-service-profile	Attach a transport-service-profile to add VLAN membership
vlan	(For role = enni) Valide VLAN ID. Opens up a new level of provisioning.
vlan-l2transport	VLAN instances for L2Transport Valid values: • bridge-domain: Bridge-domain instances for VLAN L2Transport • point-to-point: P2P instances for VLAN L2Transport • priority-map: Priority-map-profile for VLAN L2Transport • rewrite-ingress: Explicit tag rewrite option for ingress • rewrite-ingress dot1q: value to be written
vlan-l3transport ip ip-unicast-rpf ipv6	VLAN information for L3Transport. Valid values: • ip address: The list of configured IPv4 addresses on the interface • ip vrf: Associates the VRF with the interface port vlan IP unicast rpf: Enable unicast rpf on the interface Valid values: • loose: loose uRPF mode • strict: strict uRPF mode IPv6: vlan port interface IPv6 address Valid values: • address: The list of configured IPv6 addresses on the interface

LAG interface parameters > vlan level (role = ENNI)

See the following parameters:

CLI Parameter	SMx Parameter	Descrption
shutdown / no shutdown		(CLI only) Administrative state Valid values: • shutdown (disabled, default) • no shutdown
Ingress		
	Ingress Meter	(SMx only) To set the ingress limit, this field must be set to Enable. Valid values: • Enable • Disable (default)
ingress meter eir	EIR (kbps)	Ingress Meter EIR value (Kbps in 64K increments).
ingress meter ebs-bytes	Excess Burst Size (MTU Multiple)	The EBS provisioned as a factor of the MTU size configured on the interface (N*MTU), where the selected valid value = N. EBS is the maximum number of bytes available for temporary bursts above the CIR, plus EIR. Note: If the EIR is provisioned to a value greater to 0, the EBS must be provisioned to a value greater or equal to the maximum MTU in all services to which this bandwidth profile is applied.
ingress meter ebs-nxmtu	Excess Burst Size (Bytes)	The EBS provisioned as a fixed byte value. EBS is the maximum number of bytes available for temporary bursts above the CIR, plus EIR.
ingress pcp-map	PCP Map	Select an existing PCP Map to use.
Match VLAN		
match-vlan <vlan id>	Match VLAN	Match on a VLAN. Valid values • A valid VLAN
match-vlan <vlan id> **[remove-vlan <vlan id>]**	Remove Matched VLAN	Remove the matched VLAN.

load-balance hash-method

Note: This field is for E3-2, E7-2, and E9-2 ASM systems only. For E9-2 CLX systems, this field is located at the LAG interface level.

For LAG and ECMP load balancing, global-level setting for the hash-method option (applied to all LAG configurations).

Syntax

```
load-balance hash-method <hash-method option>
```

Parameters

The parameters for the "load-balance hash-method" command are described below.

Parameter	Description
hash-method	Individual traffic flows use a single link in the group. The link used for each packet is based on a hash algorithm. Valid values: • dst-ip: Destination IP address • dst-mac: Destination MAC address • enhanced (default): MAC, VLAN, Ethertype for non-ip packets; source and destination ip address, source and destination port, protocol for ip packets • src-dst-ip: Source and destination IP address • src-dst-mac: Source and destination MAC address • src-dst-mac-ip: • src-ip: Source IP address • src-mac: Source MAC address

lacp actor-system-priority

This priority value + LACP system MAC (show lacp actor-system) is compared with that of the other system (on the other side of the link) to determine which system controls the LAG. The the system with the lower value controls the LAG.

Note: The lacp-port-priority of member ports controls which ports are active or standby *only if the current AXOS system is controlling the LAG.*

Syntax

```
lacp actor-system-priority <0-65535>
```

Parameters

The parameters for the "lacp actor-system-prority" command are described below.

Parameter	Description
actor-system-priority	(LAG only) Sets the system priority between two systems connected by a LAG to determine which system controls controls the LAG. This priority value + LACP system MAC (show lacp actor-system) is compared with that of the other system (on the other side of the link), and the system with the lower value controls the LAG. Valid values: • 0–65535 (default = 32768)

Configuring G.8032 Ring Parameters

You can provision the following parameters for a G.8032v2 ring instance:

CLI Parameter	SMx Parameter	Description
g8032-ring <instance-id>	Ring Instance ID	Index number of the G.8032v2 ring instance. Valid values: 1–16
ring-id	Ring ID	Sets the ring instance ring ID. The ring ID is inserted in the R-APS source MAC address in the 6th octet as a debug aid. This is NOT the index number of the ring instance. **Note:** Ring ID numbers may not be duplicated on different ring instances. For example, ring instance ID 3 may not be configured with ring ID number 1 if ring instance 1 has already been configured with ring ID number 1. Valid values: 1–239; default = 1
description	Ring Descriptor	(Optional) Description for the ring instance. Valid value: String of up to 255 letters
control-vlan	Control VLAN	Sets the control VLAN for the ring instance. The control VLAN assigned to the G.8032v2 ring instance passes R-APS packets between all nodes on the ring, allowing them to communicate. The 0 value means that the control vlan is "unset." If the ring instance is enabled with the control VLAN unset, a g8032-configuration-unresolved alarm posts until a valid control VLAN is set. Valid values: 0–4094; default = 0 (By default, 1002–1005 are reserved for AXOS operation.)
maintenance-entity-level	Maintenance Entity Level	Sets the ring instance maintenance entity to be inserted into R-APS control messages. Valid values: 0–7; default = 1
admin-state	Admin State	Sets the administrative state of the ring instance. Valid values: enable, disable (default)
guard-time		Sets the ring instance guard time to block out of date R-APS control messages during a topology change in milli-seconds. The guard time prevents unnecessary state changes. Valid values: 10-2000 milli-seconds; default =500
hold-off-time		Sets the ring instance hold off time in milli-seconds. Hold off timers are used by the link layer on the node to filter out intermittent link failures (this is to prevent bouncing of the ring). A fault is only reported to the ring protection controller on the node if the timer expires. Valid values: 0-10000 ms, in 100 ms steps; default = 0
monitor-fop-to		Sets the AXOS system to monitor Failure of Protocol —Time-out (FOP-TO) failures. A prolonged absence of expected R-APS packets may cause a FOP-TO signal to be triggered by nodes on a G.8032v2 ring. By default, the AXOS system monitors for FOP-TO failures. Disabling this parameter stops the system from monitoring for FOP-TO failures and reporting them as alarms. This option may be required when the AXOS system interoperates in a G.8032v2 ring with third party network elements that do not forward R-APS packets. Valid values: enable (default), disable

CLI Parameter	SMx Parameter	Description
non-revertive		Sets the ring instance revertive/non-revertive mode. When disabled, the ring reverts after the signal failure condition causing a ring switch clears. The traffic resumes use of the recovered ring link only after the RPL blocks the traffic. When enabled, the ring does not revert after the signal failure condition causing a ring switch clears. The traffic remains blocked on the recovered link and unblocked on the RPL. Valid values: enable, disable (default)
propagate-topology-change		Enable or disable the Propagate Topology Change setting: • When this parameter is enabled on a major ring, topology changes in the major ring induce flushing on intersecting subtended rings. • When this parameter is enabled on a subtended ring, topology changes induce flushing on the parent major ring. • If the Propagate Topology Change setting is disabled on the ring and there is a topology change, it may take until the next general query from the upstream router to resume video traffic. In a single ring, where the topology change does not affect the location of the router facing interface, video would continue to flow. But, if upstream router interfaces are learned and the upstream router changes locations (for example, via a VRRP change) then there could be an outage. In a dual ring, the upstream router could change locations to be on the other ring, which could result in a video outage. The topology change from the ring protocol to IGMP triggers query solicits on INNI interfaces, so a new router (if there is one) can be quickly detected. This assumes the upstream router responds to a query solicit with a general query, which not all do. Valid values: enable, disable (default)
ring-type		Specifies the ring type. Valid values: • major-ring (default) • sub-ring-non-virtual • sub-ring-virtual **Note**: E9-2 does not support sub-rings.
vlan-l2transport		Sets information for L2 transport. Valid values: • VLAN ID: 0–4094 • bridge-domain: Bridge-domain instances for VLAN L2Transport • point-to-point: P2P instances for VLAN L2Transport • priority-map: Priority-map-profile for ring interface • rewrite-ingress tag: Explicit tag rewrite option for ingress
wait-to-restore-time		Sets the ring instance wait to restore time in minutes. This timer determines how long to wait before reverting the ring after a signal failure condition is removed, where the ring is configured to operate in a revertive mode. Valid values: 1-12 minutes; default = 5

Configuring ERPS Ring Parameters

You can provision the following parameters for an ERPS ring instance:

CLI Parameter	SMx Parameter	Description
erps-ring <erps ring domain id>	Name	ERPS ring domain identifier. Valid values: • 1-16
admin-state	Admin State	ERPS ring domain administration state. Valid values: • enable • disable
control-vlan	Control VLAN	VLAN ID for ERPS ring domain control traffic. Valid values: • 0-4094 (minus reserved)
description	Description	Description for ERPS ring domain (up to 255 characters)
health-time	Health Time	ERPS ring domain health timer Valid values: • 1-10 seconds(default = 5)
recovery-time	Recovery Time	ERPS ring domain recovery timer Valid values: • 1-10 seconds(default = 1)
role	Role	ERPS ring domain node role. Valid values: • transit (default) • master
topology-monitor	Topology Monitor	ERPS ring domain topology monitor administration state Valid values: • enable(default) • disable

Creating VLANs

This topic describes how to describes how to create VLANs, and is organized as follows:

- Configuration guidelines | Procedures | Parameters

Configuration guidelines

- The VLAN mode and Layer 3 service attribute (l3-service = enabled/disabled) must be set before the VLAN is used or referenced in any other object.
- Once any interface (subscriber UNI or uplink NNI) is configured with a given VLAN, the VLAN mode and Layer 3 service attributes cannot be modified.
- Modifying the reserved VLAN range (1002-1005) is not supported.
- By default, VLANs are enabled for Layer 2 (switched) service, not Layer 3 (routed) service.
- Layer 2 VLANs
  - For Layer 2 applications, VLANs are used on both the uplink and the PON.
  - To enable a VLAN for Layer 2, ensure that the l3-service parameter is set to "disabled" (default).
- Layer 3 VLANs
  - For Layer 3 applications, VLANs are used to deliver traffic over the PON. However, ingress and egress traffic at the subscriber port and uplink is untagged.
  - To enable a VLAN for Layer 3, specifically set the l3-service parameter to "enabled" and create a corresponding Layer 3 VLAN interface.
  - A Layer 3 VLAN interface can only be configured for a VLAN with Layer 3 service enabled.
- AXOS systems support DHCP and PPPoE traffic simultaneously in the same Layer 2 VLAN. To configure this support, apply both an l2-dhcp-profile and pppoe-ia-profile to the VLAN, and enable mff and source-verify on N:1 VLANs (for security with DHCP).

Procedures

To create a VLAN (via CLI)

1. In the CLI configuration mode, enter the starting point command "vlan <vlan id>" and enter a unique name for the VLAN.

```
vlan <vlan id>
```

2. Reference the table below to configure other parameters as required.

Examples

Example (Layer 2 VLAN)

```
configure

vlan 100
mode ELINE
top
```

Example (Layer 3 VLAN)

```
configure

vlan 200
l3-service ENABLED
mode N2ONE
top
```

Parameters

You can configure the following parameters when creating a VLAN:

Parameter	Description
vlan <vlan id>	Creates the VLAN container with ID value. Valid values: • 1–4094
access-group direction <direction> <type> <access-list>	(only available when mode = N2ONE) Applies a previously configured ACL to the VLAN. Direction - valid values: • inni-ingress: Internal network to network interface • uni-ingress: User network interface Type - valid values: • ethernet • ipv4 • ipv6 Access list - valid values: • Previously created access-list for the type selected above

Parameter	Description
channel-map-profile	(E3-2 only) Attach a channel map profile. Valid options: • A valid channel map profile.
description	(Optional) Brief description of the VLAN. Valid values: • String (255 characters maximum)
egress flooding	(only available when mode = N2ONE) Enables or disables flooding out UNI interfaces. Valid values • ENABLED • DISABLED (default)
igmp-profile	(E3-2 only) Attach an igmp profile. Valid options: • A valid igmp profile.
ipv6-source-verify	(E3-2 only) For EPON service with L2 transport, Source Address Verification for IPv6, which enables UNI interfaces to drop of traffic from unknown IPv6 sources. Supported only for DHCPv6 hosts, not static. Supports DHCPv6 hosts and prefix delegations (PD). Supports addresses within the upstream routers prefix as learned via Router Advertisement. Valid options: • Enabled • Disabled (default)
l2-dhcp-profile	(only available when mode = N2ONE or ONE2ONE) Attach an L2 DHCP profile to the VLAN to enable DHCP v4 and v6 snooping. **Note:** AXOS systems support DHCP and PPPoE traffic simultaneously in the same Layer 2 VLAN. To configure this support, apply both an l2-dhcp-profile and pppoe-ia-profile to the VLAN, and enable mff and source-verify on N:1 VLANs (for security with DHCP). Valid values: • name of an L2 DHCP profile
l2-dhcpproxy-profile	(E3-2/E7-2 only) (only available when mode = N2ONE or ONE2ONE) Enable DHCP v4 L2 Proxy and v6 Snoop Valid values: • name of an L2 DHCP proxy profile
l3-service	(E3-2/E9-2 only) **Note:** Configure this parameter before all others listed below. Allows Layer 3 VLAN interfaces to be provisioned on this VLAN. Valid values: • DISABLED (default) • ENABLED

Parameter	Description
mode	**Note:** Configure this parameter before all others listed below. Determines the switching behavior and provisioning of this VLAN. Valid values: • ELAN: MEF E-LAN service. Single tag shared VLAN switching on S+MAC • ELINE: MEF E-LINE service. Single tag cross-connect VLAN switched on S-VLAN only • N2ONE (default): BBF N:1 service. Single tagged shared VLAN switching on S+MAC. • ONE2ONE: BBF 1:1 service. Double tagged VLAN cross-connected VLAN switching on S+C.
mac-learning	Enables or disables MAC learning. Valid values: • DISABLED • ENABLED (default)
mcast-bandwidth	(E3-2 only) Assign allowed multicast bandwidth to an mcast vlan. Valid values: • 50(default)
meg	(only available when mode = ELINE or ELAN) Valid values: • meg name
mff	(only available when mode = N2ONE) Enables or disables UNI interfaces enforcement of MAC Forced Forwarding. MACFF provides a method for securing end-user traffic on an Ethernet access network, even if subscribers share the same IP subnetwork. In VLAN per Service applications, MACFF ensures that subscriber Ethernet frames sent upstream are only forwarded to the MAC address of a known IP gateway (Access Router or AR), and ensures that traffic from one subscriber interface cannot be sent directly to another, because the IP gateway provides IP-layer connectivity between these hosts, reducing the chance that malicious traffic can be transmitted between ports. Valid values: • DISABLED (default) • ENABLED
pppoe-ia-id-profile	**Note:** This command is deprecated. Use "pppoe-ia-profile" instead. (only available when mode = N2ONE or ONE2ONE) Enable PPPoE IA by referring to an ID profile or pppoe-ia-profile. The circuit ID string in this ID profile is used by the PPPoE IA application. Valid value: • Name of an ID profile or pppoe-ia-profile
pppoe-ia-profile	(only available when mode = N2ONE or ONE2ONE) Enable PPPoE IA by referring to a pppoe-ia-profile. The circuit ID string in this ID profile is used by the PPPoE IA application. **Note:** AXOS systems support DHCP and PPPoE traffic simultaneously in the same Layer 2 VLAN. To configure this support, apply both an l2-dhcp-profile and pppoe-ia-profile to the VLAN, and enable mff and source-verify on N:1 VLANs (for security with DHCP). (E7-2 and E3-2 systems only) For configurations where the service VLAN is configured to support both DHCP and PPPoE traffic, PPPoE frame blocking may be configured per subscriber (on ont-eth, RG, ont-ua and FB interfaces. Valid value: • Name of a pppoe-ia-profile

Parameter	Description
proxy-interface vlan-if	(only available when mode = N2ONE or ONE2ONE) Specifies the VLAN interface to use for upstream DHCP Server communication. Valid values: • 1-4094
ripv2-mode	(E7-2 and E3-2 systems only) Defines how to forward RIPv2 packets upstream. Value values: • Filter: Filters RIPv2 packets. • Flood: Floods RIPv2 packets. Allows RIPv2 to be passed from subscribers to upstream routers, even in the presence of L2 security features.
service-attributes	Free form string of Service Attributes associated with this VLAN. Valid values: • string, 1-64 chars
source-verify	(only available when mode = N2ONE) Enables or disables UNI interfaces dropping of traffic from unknown sources. IP Source Verification (IPSV) ensures that only data from IP addresses learned by DHCP snooping or static provisioning are allowed to ingress ONT Ethernet ports. This binds the IP address and MAC address to the physical ONT Ethernet port, preventing subscribers from assigning an IP address to a device and passing traffic on it. IP Source Verification for Static IP hosts requires MAC FF be enabled. Valid values: • DISABLED (default) • ENABLED
switch-mode	(E9-2 only, when mode = ONE2ONE or ELINE) Determines if frames are switched based on MAC learning (with flooding on some occasions) or based on VLAN tags only (no flooding). **Valid values:** • CROSS-CONNECT: Switching based on VLAN tags only (no flooding). • MAC-BRIDGE (default): Switching based on MAC learning. **Notes:** • The switch-mode cannot be changed while any VLAN memberships exist. • If switch-mode = CROSS-CONNECT, the mac-learning setting is not applicable.

Configuring Management VLAN ACLs with Layer 2 Transport

For Layer 2 in-band management configurations, an IPv4 or IPv6 access-list can be applied to the Layer 2 VLAN for management.

Follow these rules when applying access lists:

- For Layer 2 configurations, apply the access-list to the Layer 2 VLAN.
- For Layer 3 configurations, apply the access-list to the Layer 3 VLAN interface.

To apply an IP access-list to the Layer 2 VLAN for management, see the following configuration example:

```
[config mode]

access-list ipv4 mgmt-vlan-acl
top

vlan 999
access-group direction inni-ingress ipv4 mgmt-vlan-acl
top

[operational mode]

show running-config vlan 999
vlan 999
 access-group direction inni-ingress
  ipv4 mgmt-vlan-acl
 !
!
```

Configuring the VLAN Switch Mode (E9-2)

For VLANs in the 1:1 (ONE2ONE) or E-Line (ELINE) mode, the switching behavior can be refined even further by selecting the "MAC-BRIDGE" or "CROSS-CONNECT" switch mode.

See the table below for the description of each mode, and the impact on applications where the same VLAN spans multiple access cards.

Switch mode (switch-mode)	Description	If the same S-Tag spans multiple access cards...
MAC-BRIDGE (default)	Switching is based on MAC learning (S-Tag + MAC address). Flooding will occur for any unknown, multicast, or broadcast destination address.	Flooding will occur on all cards in the system where the S-Tag exists, regardless of the C-Tag. **NOTE: NOT supported** for NG-PON2 with wavelength mobility. You must use the CROSS-CONNECT mode to prevent flooding downstream traffic to all potential line cards that are part of the same channel partition.
CROSS-CONNECT	Switching is based on VLAN tags only (either single or double tagged), eliminating all flooding. MAC learning is also disabled on the aggregation card, resulting in increased MAC table capacity.	Frames are switched only to the access card where the C-Tag is provisioned.

Note: The switch-mode cannot be changed while any VLAN memberships exist.

Example configuration

```
!!recommended for all PON types
vlan 2000
 mode                ONE2ONE
 switch-mode         CROSS-CONNECT
!

!!supported for GPON/XGS-PON
vlan 2000
 mode                ONE2ONE
 switch-mode         MAC-BRIDGE
 mac-learning        ENABLED
!
```

Creating VLAN Interfaces

This topic describes how to describes how to create VLAN interfaces, and is organized as follows:

- Overview | Configuration guidelines | Procedures | Parameters

Overview

VLAN interfaces are used to put local IP addresses on VLANs—for Layer 3 applications (Layer 3 service VLANs) or Layer 2 in-band management (on a single Layer 2 VLAN dedicated for this purpose).

Note: VLAN interfaces should not be created for Layer 2 service VLANs.

Configuration guidelines

- Relationship to other profiles and objects:
  - IPv4 or IPv6 ACL > **VLAN interface** > Layer 3 service VLAN
  - Layer 3 DHCP profile > **VLAN interface** > Layer 3 service VLAN
  - **VLAN interface** > Layer 2 VLAN for in-band management
- For a given Layer 3 VLAN, a VLAN interface is used for the following:
  - Establish connectivity to the AXOS system router
  - Define subscriber subnets
  - Apply an ACL
  - Apply a Layer 3 DHCP profile (enabling Layer 3 DHCP relay/proxy)
  - For IPv6 subscribers, configure IPv6 neighbor discovery
- For a given Layer 2 VLAN, one Layer 2 VLAN interface may be configured as management-interface for Layer 2 in-band management.
- You must configure an IPv4 or IPv6 address for the VLAN interface before a Layer 3 DHCP profile can be applied.
- Support for DHCPv6 messaging with prefix delegation:
  - To support IPv6 RGs that request an address and prefix delegation from a DHCPv6 server, set the ND RA managed-flag to "true" and do not specify an ND RA prefix for host self-assignment.
  - Per VLAN, the hosts in a deployment must all follow the same behavior for getting an IP address—self-assignment or assignment by a DHCPv6 server (for addresses and prefix delegation).

Procedure

To create a VLAN interface (via CLI)

1. In the CLI configuration mode, enter the starting point command "interface vlan" and enter a unique name for the VLAN interface.

```
interface vlan <vlan id>
```

2. Reference the table below to configure other parameters as required.

Example

```
config

interface vlan 100
access-group ipv4-acl ACL_L3HSI
ip address 172.16.1.1/24
l3-dhcp-profile l3-fn-dhcp-prof
top
```

Parameters

You can configure the following parameters when creating a VLAN interface:

VLAN interface > top-level

Parameter	Description
interface vlan <vlan id>	VLAN ID for the interface. Valid values: • valid VLAN ID
access-group ipv4-acl	Applies an IPv4 access list to the interface. Valid values: • <name of an ipv4 access list>
access-group ipv6-acl	Applies an IPv6 access list to the interface. Valid values: • <name of an ipv6 access list>
arp	Interface arp configuration. Valid values: • arp-accept <disable (default)|enable> • arp-announce {any|prefer primary|source-ip-in-target-subnet} • arp-filter <disable (default)|enable> • arp-ignore {any|do-not-reply|source-ip-in-target-ip-subnet|target-ip-on-received-interface|target-ip-scope-not-local} • arp-notify <disable (default)|enable> • drop-gratuitous-arp <disable (default)|enable> • proxy-arp <<disable (default)|enable> • proxy-arp-pvlan <disable (default)|enable>

Parameter	Description
igmp-profile	Attach an IGMP profile to the VLAN interface. Valid value: • <Name of previously configured IGMP profile>
ip	IPv4 related configuration. (For sub-objects, see table below.)
ip	IPv4 related configuration.
ip ospf	Configure OSPF. (Applicable to the E3-2 only, when switchport = disabled) Valid values: • area: OSPF area ID in IP address format. IPv4 address. • authentication: OSPF authentication configuration. • authentication keychain: Md5 keychain • authentication md5: MD5 Authentication • authentication text: Plain Text Authentication • cost: Interface cost (default = 1) • dead-interval: Interval after which a neighbor is declared dead (default = 40) • graceful-restart: OSPF Graceful restart • graceful-restart helper-disable: OSPF helper disable (default = false) • graceful-restart helper-strict-lsa-check-disable: OSPF helper strict lsa check disable (default = false) • hello-interval: Time between HELLO packets (default = 10) • mtu-ignore: MTU ignore • network: Broadcast or point-to-point • passive-interface: Interface set to Passive state • enable • disable (default)
ip-unicast-rpf	(E3-2 only) Filters ingress packets to prevent the use of forged source IP addresses as per RFC 2827 and RFC 3704. Valid values: • ip-unicast-rpf loose • ip-unicast-rpf strict • no ip-unicast-rpf (disabled, default)
ipv6	IPv6 related configuration. (For sub-objects, see table below.)
isis	IS-IS interface configuration. (For sub-objects, see table below).
l3-dhcp-profile	(Only available if an IPv4 or IPv6 address has been configured.) Attach a Layer 3 DHCP profile to enable Layer 3 DHCP proxy. Valid values: • Name of a Layer 3 DHCP profile
mtu	MTU value Valid values: • 1500-9600 (E3-2 default = 2000, E9-2 default = 9390, E7-2 default = 9390)

Parameter	Description
mpls	Valid values: • discovery-hello Configure mpls ldp interface discovery-hello timers • keep-alive:Configure mpls ldpinterface keepalive timers • state:Enable/Disable mpls ldp on interface vlan Valid options for discovery-hello: • hold-time: Default(45)Configure mpls ldp interfacekeep-alive hold-time in seconds Valid options for keep-alive: • hold-time: Default(40)Configure mpls ldp interfacekeep-alive hold-time in seconds
proxy-arp	(E3-2 only) Layer 3 VLAN proxy ARP state Valid values: • DISABLED • ENABLED (default)
proxy-arp-vlan	L3 proxy ARP per VLAN (RFC 3069) state. Valid values: • DISABLED (default) • ENABLED
shutdown	Enables or disables the administrative state of the interface. Valid values: • shutdown (default) • no shutdown

VLAN interface > IP

Parameter	Description
address	Configured IPv4 address on the interface. Valid values: • <IPv4 address in CIDR notation> **Multinetting support:** For supported systems (E3-2 and E9-2 ASM), up to 8 addresses in different subnets are allowed for subscriber-facing multinetting support. One (1) primary and seven (7) secondary addresses are allowed, where the lowest address is the primary address. (E3-2 only) If the E3-2 is configured to operate acts as a DHCP proxy agent in the context of multinetting: • GIADDR is always populated with primary address • A newly configured lowest address will become new primary address
ospf	Configure OSPF on supported systems (when switchport = disabled). Valid values: • area: OSPF area ID in IP address format. IPv4 address. • authentication: OSPF authentication configuration. • authentication keychain: Md5 keychain • authentication md5: MD5 Authentication • authentication text: Plain Text Authentication • cost: Interface cost (default = 1) • dead-interval: Interval after which a neighbor is declared dead (default = 40) • graceful-restart: OSPF Graceful restart • graceful-restart helper-disable: OSPF helper disable • graceful-restart helper-strict-lsa-check-disable: OSPF helper strict lsa check disable • hello-interval: Time between HELLO packets • mtu-ignore: MTU ignore • network: Broadcast or point-to-point • passive-interface: Interface set to Passive state • enable • disable (default)
pim	Configure PIM
rip	Configure RIP
vrf	Associates the VRF with the interface Valid options: • forwarding:Enables VRF for interface • ip:VRF interface IP Address and Gateway Valid options for ip : • addres: The list of configured IPv4 addresses on the interface • ospf: Configure OSPF

VLAN interface > IPv6

Parameter	Description
address	IPv6 address of the interface. Valid values: • ipv6 address in CIDR notation
	Multinetting support: For supported systems (E3-2), up to 8 addresses in different subnets are allowed for subscriber-facing multinetting support. One (1) primary and seven (7) secondary addresses are allowed, where the lowest address is the primary address. (E3-2 only) If the E3-2 is configured to operate acts as a DHCP proxy agent in the context of multinetting: • GIADDR is always populated with primary address • A newly configured lowest address will become new primary address
nd	Configuration of IPv6 Neighbor Discovery protocols. • **dad:** Enables or disables the IPv6 Neighbor Discovery Duplicate Address Detection (DAD) parameters. accept (DAD) = <true | false> transmits = number of DAD probes to send • **ra:** Configuration of IPv6 Router Advertisements. (For sub-objects, see table below.)
redirects	Enables or disables the processing of ICMPv6 redirects. False = do not process ICMPv6 redirects. Valid values: • true (default) • false
unreachables	Enables or disables the transmission of ICMPv6 unreachables. False = do not generate ICMPv6 unreachable PDUs. Valid values: • true (default) • false

VLAN interface > IPv6 nd ra

Parameter	Description
cur-hop-limit	The value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the router. A value of zero means unspecified (by this router). If this parameter is not configured, the value specified in IANA Assigned Numbers that was in effect at the time of implementation is used. Valid values: • 0-255, (default = 64)
default-lifetime	The value to be placed in the Router Lifetime (in seconds) field of Router Advertisements sent from the interface It MUST be either zero or between max-rtr-adv-interval and 9000 seconds. A value of zero indicates that the router is not to be used as a default router. These limits may be overridden by specific documents that describe how IPv6 operates over different link layers. If this parameter is not configured, a a value of 3 * the value configured for the max-rtr-adv-interval field is used. Valid values: • 0-9000
link-mtu	The value to be placed in MTU options sent by the router. A value of zero indicates that no MTU options are sent. Valid values: • 0-4294967295, (default = 0)
managed-flag	The value to be placed in the 'Managed address configuration' flag field in the Router Advertisement. Valid values: • true • false (default)
max-rtr-adv-interval	The maximum time(in seconds) allowed between sending unsolicited multicast Router Advertisements from the interface Valid values: • 4-1800, (default = 600)
min-rtr-adv-interval	The minimum time(in seconds) allowed between sending unsolicited multicast Router Advertisements from the interface The default value tobe used operationally if this leaf is not configured is determined as follows: • if max-rtr-adv-interval >= 9 seconds, the default value is 0.33 * max-rtr-adv-interval; • otherwise it is 0.75 * max-rtr-adv-interval
other-config-flag	The value to be placed in the 'Other configuration' flag field in the Router Advertisement Valid values: • true • false (default)

Parameter	Description
prefix	Configuration of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from the interface. Prefixes that are advertised by default but do not have their entries in the child 'prefix' list are advertised with the default values of all parameters. The link-local prefix SHOULD NOT be included in the list of advertised prefixes. Example: ipv6 nd ra prefix 2000::0/64 Possible completions: **advertise:** Enable or disable the advertising of this prefix. Valid values: • false • true (default). **autonomous-flag:** The value to be placed in the Autonomous Flag field in the Prefix Information option. Valid values: • false • true (default). **on-link-flag:** The value to be placed in the on-link flag ('L-bit') field in the Prefix Information option. Valid values: • false • true (default). **preferred-lifetime:** The value to be placed in the Preferred Lifetime in the Prefix Information option. Valid values: • 0–4294967295, (default = 604800). **valid-lifetime:** The value to be placed in the Valid Lifetime(in seconds) in the Prefix Information option. Valid values: • 0–4294967295, (default = 2592000).
reachable-time	The value to be placed in the Reachable Time(in milliseconds)field in the Router Advertisement messages sent by the router. A value of zero means unspecified (by this router). Valid values: • 0-3600000, (default = 0)
retrans-timer	The value to be placed in the Retrans Timer(in milliseconds)field in the Router Advertisement messages sent by the router. A value of zero means unspecified (by this router). Valid values: • 0-4294967295, (default = 0)
send-advertisements	A flag indicating whether or not the router sends periodicRouter Advertisements and responds to Router Solicitations Valid values: • true • false(default)

Configuring Management Ports

This section describes how to modify or view the default parameters of system management ports.

For the location of each management port (per system), see the table below:

Management Port	E3-2 Location (1)	E7-2 Location	E9-2 Location (2)
*RJ-45 Ethernet (MGT-1)	RJ-45 port inside the case. • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1 • For local/temporary management access.	RJ-45 port on the front panel • interface craft 1/1/1 • interface craft 1/2/1 • For local/temporary management access.
RJ-45 Ethernet (MGT-3)	N/A	RJ-45 port on the rear panel • interface craft 2 • For a permanent out-of-band connection.	RJ-45 ports on the rear panel, labeled MGT-3A and MGT-3B. • interface craft 1/1/2 • interface craft 1/2/2 • For a permanent out-of-band connection • For use with interface system-craft
*RS-232 Serial (MGT-4)	RJ-11 port inside the case • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 port on the front panel • Always enabled with fixed connection settings. • For local/temporary management access.	RJ-11 ports on the rear panel, labeled MGT-4A and MGT-4B • Always enabled with fixed connection settings. • For local/temporary management access.
*USB (MGT-5)	External • interface wifi wlan1 • Requires a compatible, user-supplied USB Wi-Fi adapter. • For local/temporary management access.	N/A	N/A

Note: Ports marked with an * are typically considered for local/temporary management access.

Other notes:

(1) If supported by the installed E3-2 control module.

(2) Only E9-2 aggregation shelf locations are shown in this table.

(3) E9-2 access shelf locations:

- RJ-45 Ethernet (MGT-3A and MGT-3B) on the rear panel of access shelves
- interface craft x/1/1 and interface craft x/2/1, where x is greater than 1
- For local/temporary management access

Configuring the RJ-45 (MGT-1) Ethernet Management Port

This topic describes how to configure the RJ-45 (MGT-1) Ethernet management port, and is organized as follows:

- Configuration guidelines | Procedures | Parameters

Configuration guidelines

- You may wish to use this port without any configuration changes, with its following default settings:
  - Admin state: Enabled
  - Static IP: 192.168.1.1/24
  - DHCP Server: Enabled (allowing a PC connected to the port to obtain an IP address in the same subnet automatically)
  - DHCP Server Lease time: 10 minutes.
- If you wish to modify the the configuration of this port, note how it is identified by AXOS systems:
  - E3-2/E7-2: **`interface craft 1`**
  - E9-2: **`interface craft 1/x/1`** (aggregation shelf 1, card 1 or 2, and port 1)

Procedure

Examples

```
!!E3-2/E7-2 example
config
interface craft 1
...
top

!!E9-2 examples
config
interface craft 1/1/1
...
top

config
interface craft 1/2/1
...
top
```

Parameters (E3-2/E7-2)

You can configure the following parameter values for the front craft port:

Note: The following table covers both front and rear craft ports.

Parameter	Description
interface craft {1|2}	Specifies the craft interface index. Valid values: • craft 1 (MGT-1) • craft 2 (MGT-3, E7-2 rear panel)
access-group ipv4-acl	(E7-2 only) Valid values: • <valid IPv4 access list>
cosq	(E7-2 only) Valid values: • <cosq profile >
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. Valid values: • dhcp • <IP address>/<mask> Craft 1 default = 192.168.1.1; craft 2 default = 192.168.1.2. If you change the factory default address, the current value becomes the default.
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable (default for craft 1) • disable (default for craft 2) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)
ipv6 address	Valid values: • <IPv6 address>
ipv6 redirects	Valid values: • true (default) • false
ipv6 unreachables	Valid values: • true (default) • false

Parameter	Description
shutdown	Administrative state of the craft management port. Valid values: • no shutdown (default for craft 1) • shutdown (default for craft 2)

Parameters (E9-2)

You can configure the following parameter values for the front craft port:

Note: The following table covers both front and rear craft ports.

Parameter	Description
interface craft <shelf>/<slot>/<port>	Specifies the craft interface index. For example, 1/1/1. Valid values: • 1/x/1: located on the faceplate, labeled MGT-1 • 1/x/2: located on the shelf rear, labeled MGT-3A or MGT-3B An aggregation shelf supports one 'system-craft 1' port, which is logical port that rides over a pair of back craft ports (to route packets from the logical interfaced). Each access line card supports a 'craft 1' port located on the rear of the shelf, labeled MGT-3A or MGT-3B.
access-group	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates an access list with the interface Valid options: • ipv4-acl: Apply an Ipv4 Access Control List • ipv6-acl: Apply an Ipv6 Access Control List
cosq	(Only present for aggregation shelf rear craft 1/x/2 interfaces.) Associates a cosq profile with the interface Valid options: • <profile name>
description	Description for the interface Valid values: • String (255 char)
ip address	IP address of the craft management port. Valid values: • dhcp • <IP address>/<mask> • (1/x/1 default = 0.0.0.0/0)

Parameter	Description
ip dhcp server	Administrative state of the DHCP server. Valid values: • enable • disable • (craft 1/x/1 default = enable) • (all other craft ports default = disable) When enabled, the AXOS system looks for an existing DHCP server on the network for five seconds. If a DHCP server is not detected, the internal DHCP server on the port creates a pool of (3) IP addresses. If an external DHCP server is detected, the internal DHCP server is automatically disabled. Disabling the DHCP server causes the pool of IP addresses to be deleted.
ip dhcp client dhcp-lease-time	Specifies the DHCP lease time in seconds (Option 51). Valid values: • 0–4294967295 (default = 0)
ip gateway	(Only present for E9-2 access shelves craft x/y/1; not aggregation shelves.) Default gateway IP address. Valid values: • <IP address> (default = 0.0.0.0) • <fully qualified domain name, 1–253 alpha numeric characters>
ip vrf forwarding ip vrf forwarding ipv6 address	Associates a VRF with the interface Valid options: • <VRF name> • ipv6-address: The list of configured IPv6 addresses on the interface
ipv6	Craft interface IPv6 address and vrf configuration Valid values: • address: The list of configured IPv6 addresses on the interface • redirects: Enable or disable the processing of ICMPv6 redirects Valid values: • true (default) • false • unreachables: Enable or disable the transmission of ICMPv6 unreachables Valid values: • true(default) • false
mtu	Interface maximum transmission unit Valid value: • 1500-9600
shutdown	Administrative state of the craft management port. Valid values: • no shutdown • shutdown • (craft 1/x/1 default = no shutdown) • (all other craft ports default = shutdown)

Configuring the RJ-45 (MGT-3) Ethernet Management Port

For the E7-2: See *Configuring Out-of-Band Management (E7-2)* (on page 217)

For the E9-2: *Configuring Out-of-Band System Management (E9-2)* (on page 221)

Configuring the RS-232 Serial (MGT-4, MGT-4A, MGT-4B) Management Port

AXOS systems are equipped with one more more RS-232 serial ports (RJ-11 connectors) for establishing local console connections to the CLI only.

Note: You cannot modify the serial port connection settings.

Configuration guidelines

The serial port is always enabled and uses the following fixed connection settings:

- Baud Rate: 115200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

System notes:

- E9-2: Two RJ-11 ports located on the recessed rear panel, labeled MGT-4A and MGT-4B.
  - MGT-4A is assigned to card slot 1 (bottom).
  - MGT-4B is assigned to card slot 2 (top).
  - Use the serial port of the active aggregation card to establish a local console connection to the CLI only.
- E7-2: RJ-11 port located on the front panel.
- E3-2: RJ-11 port located inside the case.
- E3-2/E7-2 only: Show command to view the craft serial port:
  - **`show interface craft-serial`**

Configuring the USB (MGT-5) Ethernet Management Port

Note: This topic only applies to the E3-2.

This topic describes how to configure the USB Ethernet management port, and is organized as follows:

- Configuration guidelines | Parameters

Configuration guidelines

- The USB Ethernet management port is enabled by default, with a non-configurable link local IPv4 address of 169.254.42.1.
- The port is identified as **wlan1** in the CLI.
- An internal DHCP server runs on the port and provides a pool of (3) IPv4 local link addresses for devices connecting to the port; the DHCP server cannot be modified.

Parameters

You can configure the following parameters for this interface:

Parameter	Description
wifi	Name for the WiFi interface. For example, wlan1.
channel	The wireless access point channel number. • Channels 1–11 are available in North America. • Channels 1–13 are available in Europe generally, with variations between different countries. Valid values: • 1–14; default 1
inactivity-timer	Specifies the time in minutes for disabling the access point with no wireless client (PC or mobile device) connected. The timer starts when: • A compatible USB adapter is inserted in the USB port, *or* • The last wireless client (PC or mobile device) disconnects. The timer stops when a client successfully authenticates. If the timer expires, the access point is disabled. To reactivate the wireless access point: • Remove and reinsert the WiFi adapter with five second delay in between, *or* • Shutdown and then no shutdown the WiFi port administrative state. Re-activation is immediate. Valid values: • 1–1000; default 30 Entering 0 disables the timer.
max-clients	Specifies the maximum number of wireless clients allowed. Note: The USB port cannot be expanded using a USB hub. Valid values: • 1-2; default 1

Parameter	Description
shutdown *OR* no shutdown	Enables or disables the WiFi port administrative state Valid values: • shutdown, no shutdown; default is no shutdown
passphrase	Specifies a passphrase for the wireless access point. The passphrase uses Advanced Encryption Standard (AES) privacy protocol to encrypt the data. To securely enter the passphrase, type passphrase [enter key], and then enter the passphrase at the next prompt. **Note**: If you type passphrase <passphrase>, the passphrase echoes back in clear text. Enter a unique string of 8–16 characters, including a minimum of: • one lowercase, • one uppercase, and • one numeric character Default: Calix_XXXX, where XXXX is the last four digits of the AXOS system serial number
ssid	Specifies the access point Service Set Identifier (SSID). The SSID is the network name used to identify this AXOS system for connection to other wireless devices. Valid value: • A unique string of 1–32 characters, including lower case letters, upper case letters or numbers Default: CalixCraft-XXXX, where XXXX is the last four hex digits of the AXOS system starting MAC address
ssid-broadcast	Sets the administrative state of the SSID broadcast. When set to DISABLED, the AXOS system SSID does not display in the list of available wireless networks from your PC or mobile device. However, you can still connect to the SSID manually. Valid values: • ENABLED or DISABLED; default is ENABLED

•

Chapter 14

Managing AXOS Configuration Files

This chapter provides an overview of how to manage Calix AXOS platform configuration files.

This chapter describes how to manage Calix AXOS platform configuration files.

Topics covered

- Creating a configuration file
- Copying and pasting a configuration file
- Transferring files between the running configuration and startup configuration
- Transferring configuration files to/from a server
- Saving a configuration file to the node
- Applying a configuration file saved on the node
- Reverting to the factory default startup configuration
- Viewing the status of a copy operation
- Deleting a configuration file from the node
- Viewing configuration files
- Comparing configuration files
- Locking/Unlocking a datastore

About Configuration Management

Calix AXOS configurations contain the software commands used to customize the functionality of your device. Calix AXOS systems use the following configuration types:

- **Startup configuration**: An XML file containing the software configuration to be used during system boot up, which is persistent (stored in NVRAM).
- **Running configuration**: Reflects the currently running software configuration, and is not persistent (stored in RAM).

Supported Actions

You can perform the following actions for configuration files:

- Accept the running configuration
- Transfer files to or from an external server, including:
  - Uploading a file from an AXOS system configuration folder to a server
  - Downloading a file from a server into an AXOS system configuration folder
- Copy a source file to a destination location

  The destination location may be the startup configuration, running configuration or a configuration file stored in an AXOS system configuration folder. The result of the copy function varies based on the type and combination of source and destination locations provided. You can perform the following actions using the copy operation:
  - Save the running configuration as the current startup configuration file, to be applied on system boot up
  - Reapply the current startup configuration file, and make it the running configuration
  - Reapply a configuration file stored in an AXOS system configuration folder, and make it the running configuration or current startup configuration
  - Save a copy of the running configuration or startup configuration file to an AXOS system configuration folder
- View the status of a file transfer operation
- Delete configuration files
- View configuration files
- Compare two configuration files stored in an AXOS system configuration folder
- Lock and unlock a datastore

Note: For E9-2 systems, perform all procedures from the active aggregation card.

Creating a Configuration File (E3-2/E7-2)

You can manually create an Calix AXOS platform configuration file in XML format. Calix recommends that you create this file on a lab/spare system via the CLI, save it locally and then push it to a TFTP server.

The XML file should include the following minimum configuration:

- A configured management VLAN
- A transport service profile that includes all VLANs used by other nodes and traversing the new node
- Configuration for the transport (point to point or G.8032/ERPS ring)
- Configuration for Auto MEP feature to support Connectivity Fault Management (CFM) on G.8032v2 rings, if applicable
- A hostname

You may opt to create a generic configuration file intended for all nodes in your network. You can then download the configuration file to the Calix AXOS platform running configuration during manual node turn-up or via zero touch provisioning, manually configure the node as needed, and save the running configuration to the startup configuration.

Alternatively, you may create a configuration file for each node in your network containing the complete node-specific configuration. You can download the configuration file to the Calix AXOS platform running configuration during manual node turn-up or via zero touch provisioning, and then save the running configuration to the startup configuration. When changes in services occur, you can make the necessary changes to the running configuration via the user interface, and then save the updates to the corresponding configuration file.

Related topic:

- *Copying and Pasting a Configuration File* (on page 349)

Creating a Configuration File (E9-2)

You can manually create an AXOS system configuration file in XML format. Calix recommends that you create this file on a lab/spare system via the CLI, save it locally and then push it to a TFTP server.

The XML file should include the following minimum configuration:

- Front craft port (craft 1/1/1 or craft 1/2/1) on the active aggregation card configured with the desired IP address
- A hostname
- Configuration for the transport, including VLAN(s) and a transport service profile

You may opt to create a generic configuration file intended for all E9-2 systems in your network, and download the configuration file to either:

- the active configuration folder, and then copy the configuration from the folder into the running-configuration.
- the active configuration folder as a 'startup-config' file and then reboot the system to load the configuration into the running-configuration.

You can then manually configure the E9-2 as needed, and save the running configuration to the startup configuration.

Alternatively, you may create a configuration file for each E9-2 system in your network containing the complete OLT-specific configuration, and download the file as described above. When changes in services occur, you can make the necessary changes to the running configuration via the user interface, and then save the updates to the startup configuration file.

Copying and Pasting a Configuration File

AXOS systems support copying sections of the running configuration text file from one system and pasting it into an open terminal session onto another system. This feature is useful if you have a preferred configuration on one system and wish to quickly copy parts of it to another.

1. Using a console, SSH or Telnet connection, log in to the CLI on the system that has the source configuration. Enable session logging on the terminal program, if possible (Session > Logging).
2. At the CLI prompt, issue the **paginate false** or **terminal screen-length 0** command. This causes the system to display the entire configuration at once rather than a screen length at a time. This allows you to capture the configuration without "more" prompts being generated when the system displays one screen at a time.

   ```
   Calix-1# terminal screen-length 0
   ```
3. Issue the following command to display the active configuration in memory (stored in RAM), including saved configuration changes.

   ```
   Calix-1# show running-config
   ```

   Note: You can view default parameters by adding '|details' or by enabling show-defaults in the configuration mode ('cli show-defaults enable').
4. Open the saved log via a text editor program (for example, Notepad or Wordpad):
   - If you have enabled session logging on the terminal program, open the saved log by using a text editor program.
   - Otherwise, copy the output from the **show running-config** command into a text editor program.

   Note: When copying and pasting the output of the **show running-config** command, from one system (source) to another (destination), the two systems must have the same ONT profiles loaded. If they do not, the past operation fails.
5. If necessary, update parts of the configuration (for example, IP addresses) to be appropriate for the destination system.
6. Using a console, SSH or Telnet connection, log in to the CLI on the destination system.
7. Enter configuration mode:

   ```
   Calix-1# configure
   Enter configuration commands, one per line. End with CNTL/Z.
   Calix-1(config)#
   ```
8. Copy the updated text configuration file from the text editor program.
9. At the CLI prompt, paste the configuration into the system.
10. Exit configuration mode:

    ```
    Calix-1(config)# exit
    ```

11. Accept the new running configuration on this destination system as the current startup configuration.

```
Calix-1# copy running-config startup-config
```

Transferring Files between the Running Configuration and Startup Configuration

This topic describes how to:

- Copy the running configuration to the current startup configuration.
- Reapply the current startup configuration file, and make it the running configuration.

Configuration guidelines

- For an AXOS platform to boot up with the running configuration, you must copy the running configuration to the startup configuration.
- For E9-2 SMm systems with active subscribers, clear the subscribers by disabling the DHCP pool before reapplying the startup configuration file as the running configuration.
- The length of time required to copy a configuration varies, depending on the file size.
- When copying the running configuration to the startup configuration as a backup, an AXOS system:
  - Saves the running-config file with the name 'startup-config.xml'.
  - Appends a time stamp to the current startup configuration file name in the format "yyyymmdd.hhmmss."
  - Automatically stores up to 12 backup configuration files with dates in the configuration folder, after which the oldest file is rotated out.
- If a 'running-config-suspect' is present on the system, refer to the *AXOS Monitoring and Troubleshooting Guide* and follow the additional repair steps in the order presented.

Procedures

To copy the running configuration to the startup configuration

Note: You cannot perform the following operation if a 'running-config-suspect' is present on the system.

Use the following CLI command:

```
Calix-1# copy running-config startup-config
```

To reapply the current startup configuration file as the running configuration

Warning: The configuration file that you apply takes effect immediately (however the length of time required to copy the file varies). Verify that the configuration file is correct before proceeding.

1. (E9-2 with active subscribers only) Set the administrative state of the DHCP pool to disable.

```
Calix-1(config)# dhcp-v4-server-pool <name> admin-state disable
Calix-1(config-dhcp-v4-server-pool-<name>)# exit
Calix-1(config)# exit
```

2. Reapply the current startup configuration file as the running configuration.

```
Calix-1# copy startup-config running-config
```

3. (E9-2 with active subscribers only) Re-enable the DHCP pool.

```
Calix-1# config
Calix-1(config)# dhcp-v4-server-pool <name> admin-state enable
```

Transferring Configuration Files To/From an External Server

This topic describes how to perform the following operations:

- Upload a file from an AXOS system configuration folder to a server
- Download a file from a server into an AXOS system configuration folder

Configuration guidelines

- Configure your server as a server for one of the supported transport protocols: HTTP, HTTPS, FTP, TFTP, SFTP, or SCP.

  Note: For uploads, HTTP and HTTPS are not supported.

- Only one upload or download operation can be on-going at any given time.
- You must specify at least one file stored on the AXOS system (using the *from-file* or *to-file* parameters); URI-to-URI copy operations are not supported.
- The length of time required to upload or download a file varies, depending on the file size.
- AXOS systems support the following characters in the URI password field for upgrade, upload and download commands, as noted:
  - Special characters **~$&*()-+=:',.** are supported.

  Note: Passwords starting with "1" or "4" are not encrypted, and display as plain text.

  - Special characters **!;** are supported when escaped. To escape, precede the character with \. For example to escape ! enter **\!**.
  - All other characters, including special characters, are supported when encoded with %xx, where xx is the hex value of the ASCII character (for example, enter the @ symbol as %40). Refer to http://en.wikipedia.org/wiki/ASCII#ASCII_printable_code_chart for the hex values of all special characters.

  Note: Spaces are not supported in the URI password field.

Parameters

You can configure the following parameters when uploading or downloading a file to/from an external server:

Parameter	Description	Valid Options
Uploads		
To URI	URI for the destination file location on the server, formatted as follows[1]: <protocol>://[<user>:<password>]@<host>[:<port>]/<uri-path>/[<file>] where: protocol = the transport method user = username on the server password = password on the server host = IPv4 address or host name port = logical port number on the server[2] url-path = the directory where the configuration files reside on the server; the path requires a trailing '/' if it is a directory name file = filename.xml, if you are renaming the source file. If you do not specify the file, then the source file name is used for the destination file name. **Note**: With SFTP and SCP URLs, the path name given is the absolute name on the server. To access a file relative to the remote user's home directory, prefix the file with /~/ , such as: sftp://user:password@home.example.com/~/startup-config.xml	Text string of 1–255 characters Protocols: FTP (passive mode), TFTP, SFTP, or SCP **Note**: HTTP and HTTPS are not supported for the "to-URI" parameter.
from-file (CLI only)	Source file name **Note**: The .xml extension must be specified, if it exists.	Any configuration file saved to the Calix AXOS platform configuration folder
Downloads		
From URI	The complete uniform resource identifier (URI) for the source file location on the external server, formatted as follows[1]: <protocol>://[<user>:<password>]@<host>[:<port>]/<uri-path>/<file.xml> where: protocol = the transport method user = username on the server password = password on the server host = IPv4 address or host name port = logical port number on the server[2] url-path = the directory where the configuration files reside on the server file = filename.xml; the .xml extension must be specified, if it exists. **Note**: With SFTP and SCP URLs, the path name given is the absolute name on the server. To access a file relative to the remote user's home directory, prefix the file with /~/ , such as: sftp://user:password@home.example.com/~/startup-config.xml	Text string of 1–255 characters Protocols: HTTP, HTTPS, FTP (passive mode), TFTP, SFTP, or SCP

Parameter	Description	Valid Options
To File	Destination file name **Note**: Calix recommends using an .xml extension.	Name of the configuration file to be saved in the AXOS system configuration folder

[1] The server username and password are required for SFTP and SCP; all other parameters in brackets [] are optional. If you do not provide the username/password or provide an invalid username/password for SCP, the Calix AXOS platform displays a generic error message rather than a permissions error (for example "Error in the SSH Layer" or "Login denied").

[2] The port parameter is only needed if the server is running a protocol on a non-default port.

Procedures

To upload a file from an AXOS system configuration folder to a server

```
Calix-1# upload file config from-file <source file name> to-URI <destination
file URI>
```

- **TFTP Example:**

  ```
  Calix-1# upload file config from-file startup-config_5614.xml to-URI
  tftp://172.21.34.15/startup-config_5614.xml
  ```

- **FTP Example:**

  ```
  Calix-1# upload file config from-file startup-config_5614.xml to-URI
  ftp://node:node@172.23.35.18/startup-config_5614.xml
  ```

To download a configuration file from a server into an AXOS system configuration folder

```
Calix-1# download file config from-URI <source file URI> to-file <destination
file name.xml>
```

To verify the file transfer, use the following command:

```
Calix-1# show file transfer-status
```

Saving a Configuration File

This topic describes how to save a copy of the running configuration or startup configuration file to the configuration folder.

To save a configuration file

- **Calix-1# copy config from running-config to <file.xml>**
- **Calix-1# copy config from startup-config to <file.xml>**

NETCONF example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="m-
10">
<copy-configuration xmlns="http://www.calix.com/ns/exa/base">
  <to>running-config</to>
  <from>startup-config</from>
</copy-configuration>
</rpc>]]>]]>
```

Note: The 'copy-config' RPC is not supported. Use the Calix 'copy-configuration' RPC instead.

Related command:

- **Calix-1# copy config from <file.xml> to <file.xml>**

To save a configuration file to an external location

This section describes how you can save your startup configuration file to an external location.

Syntax:

Use the following command syntax for uploading the startup configuration file to an external location.

```
upload file config from-file <file name> to-URI <protocol>://<server
name>:<server password>@<server ip address or URI>/<file name>
```

Example

upload file config from-file startup-config.xml to-URI ftp://user123:pwd456@172.20.101.54/startup-config.xml

Applying a Configuration File Saved on the Node

This topic describes how to apply a configuration file saved in an AXOS system configuration folder, and make it the running configuration or current startup configuration.

To apply a configuration file saved on an AXOS system

Use the following command to apply a configuration file to the running configuration, to take effect immediately:

Note: For E9-2 SMm systems with active subscribers, use the 'dhcp-v4-server-pool <name> admin state' CLI command to disable the DHCP pool *before* applying a configuration file to the running configuration.

```
Calix-1# copy config from <file.xml> to running-config
```

Use the following command to reapply a configuration file into the startup configuration, to take effect at reboot:

```
Calix-1# copy config from <file.xml> to startup-config
```

Reverting to the Factory Default Startup Configuration

Calix AXOS systems initially boot up with the factory default startup configuration file shipped on the system. This topic describes how to return an AXOS system to the default startup configuration, if needed. Alarm and event archives and the card boot count are retained.

Note: For information about how to revert E9-2 aggregation and access cards to the factory default settings (erase all persistent data and logs and reload with factory default configuration), please refer to the topic *Reverting an E9-2 Card to Factory Default Startup Settings* (on page 360).

Configuration guidelines

- Calix recommends that you collect all technical logs and upload them to a file server (via the command "**generate techlog include-core YES**) before you perform a factory reset. Refer to the *AXOS Monitoring and Troubleshooting Guide* for more information.
- To revert the startup config to its previous state upon bootup (via the '**upgrade switch revert-config**' CLI command), refer to the *AXOS Upgrade Guide*.
- For a standalone system, revert to the factory default startup configuration via a console connection.
- E9-2 configuration guidelines:
  - Issue the commands described in this topic on the active aggregation card in an E9-2 system.
  - Only the active and standby aggregation cards in an E9-2 system contain the startup-config.xml file. This file is not stored on the access line cards. For this reason, do not use the shelf/slot parameter when issuing the '**delete file config filename startup-config.xml**' command. (For example, do not issue the command '**delete file config filename startup.xml 2/1**')
  - When the '**delete file config filename startup-config.xml**' and '**reload all**' commands are issued on the E9-2 active aggregation card, both aggregation cards (active and standby) and all active line cards in the E9-2 system reboot running the default startup configuration.

To revert to an AXOS system factory default startup configuration

1. Delete the startup configuration file:

   ```
   Calix-1# delete file config filename startup-config.xml
   ```

2. Enter the reload command:

   - E9-2:

     ```
     Calix-1# reload all
     ```

   - All other AXOS systems:

     ```
     Calix-1# reload
     ```

3. Confirm the reload:

   ```
   Proceed with reload? [Y/N] Y
   ```

Reverting an E9-2 Card to Factory Default Startup Settings

This topic describes how to revert aggregation and access line cards in an E9-2 platform to the factory default settings.

When E9-2 cards are reverted to factory default settings, all configuration files (including backup config files), core files, techlogs, and persistent checkpoints are deleted. The currently running image is then copied to the standby image, so that both images in partitions imgx and imgy contain the factory default configuration.

ALERT! When you restore an E9-2 aggregation or line card to the factory default configuration you erase all data that may help to debug the software.

Prerequisites

Prior to performing a factory reset Calix recommends that you do the following:

- Collect all technical logs and upload them to a file server. To generate all technical logs simultaneously, use the command "**generate techlog include-core YES**" from Operational mode.
- Backup your startup configuration file and upload it to a file server. Refer to *Saving a Configuration File* (on page 356)for information about how to back up your configuration files.

Configuration guidelines

To revert aggregation and access line cards in an E9-2 platform to factory default settings:

- Access the E9-2 active aggregation and access line cards via a local console connection. Refer to the *Calix E9-2 Installation Guide* for information about how to connect to an active aggregation or access line card via a console connection via an RS-232 management port.
- Log into the E9-2 platform under a user account with the 'calixsupport' role.
  - The E9-2 software includes a predefined system user account called "calixsupport". This is a special user account, meant to be used only by Calix support personnel and other authorized personnel.

    To access the default "calixsupport" user account, enter the following when logging into the E9-2:
    - login name: calixsupport
    - password: calixsupport
  - If you do not wish to use the default "calixsupport" user account, you may configure and use another user account with the 'calixsupport' role. For information about how to configure user accounts on the E9-2, refer to the *Calix AXOS Turn-Up and Transport Guide (E9-2)*.

Procedures

To revert the active and standby aggregation cards to the factory default settings

1. Login under the "calixsupport" user role to the active aggregation card via a console connection.
2. Issue the command "**show system-equipment**"to determine if the standby card is in slot 1/1 or 1/2, as shown in the following example

```
Calix-1# show system-equipment
system-equipment
 equipment-type     "Multi Card"
 active-controller  "card 1/1 (this card)"
 standby-controller "card 1/2 (mate card)" <---
```

3. SSH to the standby aggregation card under the "calixsupport" user role. Use the output from the "**show system-equipment**" command to determine the internal IP address:
   - card 1/1: 192.168.6.17
   - card 1/2: 192.168.6.18

For example:

```
Calix-1# ssh calixsupport@192.168.6.18
The authenticity of host '192.168.6.18 (192.168.6.18)' can't be
established.
ECDSA key fingerprint is
SHA256:Hei2QDh6gQlBrG4h83hTknPku05gnNif4NDTEApP4ac.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.6.18' (ECDSA) to the list of
known hosts.
calixsupport@192.168.6.18's password:
DISPLAY "(null)" invalid; disabling X11 forwarding
**** STANDBY AGG CARD ****
Welcome to CLI
calixsupport connected from 192.168.6.17 using ssh on Calix-1
```

4. Issue the command **upgrade factory-reset** from Operational mode to revert the standby aggregation card to the factory default settings.

```
Calix-1# upgrade factory-reset
Warning! Factory-reset will wipe out all configuration data
(including running
        configuration and all saved configuration files), all
checkpointed states,
        and all persistent files. The card will reset to factory
settings, and will
        reload immediately. Do not interrupt this process. Do not
power down the
        card during this process.
        It is strongly recommended that:
        1. You perform this operation using a console connection.
        2. You perform a configuration backup as needed.
        3. You collect and upload a techlog as needed.
        There is no UNDO !!
```

5. Confirm that you wish to proceed with the factory reset on the standby aggregation card, as shown in the following example. The standby aggregation card reloads and powers up with the factory default configuration on the active and standby image. When the standby aggregation card reloads you lose your SSH connection to it and are redirected back to the active aggregation card.

```
Proceed with factory-reset? [Y/N] Y
Factory reset in progress. This will take a few moments. Please be patient.
..............
Broadcast message from root@Calix-1 (pts/1) (DATE):
The system is going down for reboot NOW!
Factory reset finished. The system will reload now.
Calix-1# Connection to 10.202.11.119 closed.
```

6. Revert the active aggregation card to the factory default settings.

```
Calix-1# upgrade factory-reset
```

7. Confirm that you wish to proceed with the factory reset on the active aggregation card.

```
Proceed with factory-reset? [Y/N] Y
```

8. The active aggregation card reloads and powers up with the factory default configuration on the active and standby image.

To revert a line card to the factory default configuration

1. Login under the "calixsupport" user role to the line card via a console connection.
2. Issue the command **upgrade factory-reset** to revert the line card to the factory default settings.

```
E9_line_card-1# upgrade factory-reset
Warning! Factory-reset will wipe out all configuration data
(including running
         configuration and all saved configuration files), all
checkpointed states,
         and all persistent files. The card will reset to factory
settings, and will
         reload immediately. Do not interrupt this process. Do not
power down the
         card during this process.
         It is strongly recommended that:
         1. You perform this operation using a console connection.
         2. You perform a configuration backup as needed.
         3. You collect and upload a techlog as needed.
         There is no UNDO !!
```

3. Confirm that you wish to proceed with the factory reset on the line card.

```
Proceed with factory-reset? [Y/N] Y
```

4. The line card reloads and powers up with the factory default configuration on the active and standby image.

Viewing the Status of a File Transfer Operation

This topic describes how to view the status of the most recent file transfer operation via the CLI, either: Idle, In progress, Success or Aborted.

To view the status of a file transfer operation

Use the following command to view the status of the most recent file transfer operation:

show file transfer-status

CLI Example Outputs:

```
Calix-1# show file transfer-status
file transfer-status
 status Idle

Calix-1# show file transfer-status
file transfer-status
 status In progress

Calix-1# show file transfer-status
file transfer-status
 status Success

Calix-1# show file transfer-status
file transfer-status
 status Aborted
```

Deleting a Configuration File from the Node

This topic describes how to delete a configuration file from an AXOS system configuration folder.

To delete a configuration file from the system

```
Calix-1# delete file config filename <string>
```

Note: The file name must be an exact match.

For example, to remove the startup config file, issue the following command:

Calix-1# **delete file config filename startup-config.xml**

NETCONF example:

```
<rpc message-id="101"
          xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <delete-config>
          <target>
            <startup/>
          </target>
        </delete-config>
      </rpc>

       <rpc-reply message-id="101"
            xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <ok/>
      </rpc-reply>
```

Related topic

- Viewing Configuration Files

Viewing Configuration Files

This topic describes how to view all configuration files saved on an AXOS system, or the contents of a specific configuration file.

To view configuration files

Use the following command to view the contents of the configuration folder:

show file contents config

Example output:

```
Calix-1# show file contents config
file contents config
 number-of-files 12
 total-size      211113
FILENAME                              FOLDERNAME  SIZE   LAST
MODIFICATION TIME
-----------------------------------------------------------------------
startup-config.xml                    config      24274  Thu Jun 26
17:57:32 2014
startup-config.20140626.175732.xml    config      22865  Thu Jun 19
10:37:12 2014
startup-config.20140619.103712.xml    config      21974  Mon Jun 16
13:33:06 2014
startup-config.20140616.133306.xml    config      21863  Mon Jun 16
13:21:32 2014
startup-config.20140616.122132.xml    config      17455  Fri Jun 13
15:22:27 2014
startup-config.20140613.142226.xml    config      16429  Thu Jun 12
17:42:14 2014
startup-config.20140612.234214.xml    config      16429  Thu Jun 12
17:25:14 2014
startup-config.20140612.232514.xml    config      16321  Thu Jun 12
17:17:27 2014
startup-config.20140612.231727.xml    config      16318  Thu Jun 12
15:42:14 2014
startup-config.20140612.214214.xml    config      15520  Wed Jun 11
10:32:47 2014
startup-config.20140611.163247.xml    config      16043  Wed Jun 11
03:26:35 2014
startup-config.20140611.092635.xml    config      5622   Wed Jun 11
03:24:22 2014
```

Use the following command to view the contents of a configuration file:

show file contents config filename <file>

Note: You must include .xml in the file name.

Comparing Configuration Files

From the CLI, you can compare two files stored in an AXOS system configuration folder. To compare the running configuration to a saved configuration file, you must first save the running configuration to an AXOS system configuration folder.

AXOS systems use the unified output format to display differences between two files, where:

- The output begins with a header:
  - --- from-file
  - +++ to-file
- The lines common to both files begin with a space character. The lines that differ between the two files have one of the following characters to the left:
  - '+' indicates that a line was added here to the first file.
  - '-' indicates that a line was removed here from the first file.
- The output includes one or more hunks of differences; each hunk shows one area where the files differ. The first line of a hunk is formatted as @@ -l,s +l,s @@ where *l* is the starting line number, and *s* is the number of lines the hunk applies to. The hunk for *file1* is preceded by a minus sign. The hunk for *file2* is preceded by the plus sign.

To compare two configuration files

show file diff config file1 <file> **file2** <file>

Example:

```
Calix-1# show file diff config file1 startup-config.20140422.133248.xml
file2 startup-config.20140422.135514.xml
--- /.folders/config/startup-config.20140422.133248.xml
+++ /.folders/config/startup-config.20140422.135514.xml
@@ -3240,12 +3240,6 @@
       <override />
     </service-instance>
     <service-instance>
-      <service-name>vlan600</service-name>
-      <vlan>600</vlan>
-      <service-profile-name>tag60</service-profile-name>
-      <override />
-    </service-instance>
-    <service-instance>
       <service-name>vlan666</service-name>
       <vlan>666</vlan>
       <service-profile-name>smax2</service-profile-name>
```

```
@@ -3426,26 +3420,13 @@
     <ethernet>
       <port>g5</port>
       <storm-control />
+      <service-role>enni</service-role>
       <inni>
         <transport-service-profile>all</transport-service-profile>
         <rstp />
         <lldp />
       </inni>
       <enni>
-        <service>
-          <service-name>vlan600</service-name>
-          <match>
-            <vlan>600</vlan>
-          </match>
-          <shutdown>false</shutdown>
-        </service>
-        <service>
-          <service-name>vlan700</service-name>
-          <match>
-            <vlan>700</vlan>
-          </match>
-          <shutdown>false</shutdown>
-        </service>
         <rstp />
         <lldp />
       </enni>
```

Related topic:

- Saving a Configuration File to the Node

Locking/Unlocking a Datastore

Calix AXOS systems support the ability to lock candidate and running datastores.

When running and candidate datastores are locked, they are only modifiable for the given session. This is typically intended to be a short period of time but there is no time limit. If a session with a lock is lost, the lock is freed and any changes revert to the configuration prior to the lock.

The CLI only supports the ability to lock the running datastore; the candidate datastore may not be locked via the CLI.

A lock is not granted if any of the following conditions is true:

- The target configuration is <candidate>, it has already been modified, and these changes have not been committed or rolled back.
- The target configuration is <running>, and another NETCONF session has an ongoing confirmed commit.

To lock/unlock a running datastore

- To lock a running datastore, issue the following command:

```
Calix-1# lock datastore running
```

- To unlock a running datastore, issue the following command:

```
Calix-1# unlock datastore running
```

To display locked datastores

- To view information about all locked datastores:

```
Calix-1# show locks
```

- To view information about locked candidate datastores:

```
Calix-1# show locks candidate
```

- To view information about locked running datastores:

```
Calix-1# show locks running
```

The output displays the following information:

locked-time	The time the lock occurred
session-id	Session identifier of the NETCONF session that has the lock
session-ip	IP of the session that has the lock
session-login	User login of the session that has the lock
session-manager	Type of user agent session that has the lock (for example, CLI or netconf)

Example:

```
Calix-1# show locks
locks
 running
  session-id      12
  session-login   sysadmin
  session-manager cli
  session-ip      10.204.32.12
  locked-time     2016-05-10T19:11:36-0800
```

To display user sessions

To display information about all of the user sessions on the system, issue the following command:

```
Calix-1# show user-sessions
```

The output displays the following information:

has-candidate-lock	True/false statement that displays if the session has the candidate datastore locked
has-running-lock	True/false statement that displays if the session has the running datastore locked
is-our-session	True/false statement that displays if the session is the source of retrieval request
login-time	Login time for this session
session-id	NETCONF session identifier
session-ip	IP of the session
session-login	User login of the session

session-manager	Type of UA session that has the lock (for example, CLI or netconf)

Example:

```
Calix-1# show user-sessions
user-sessions
 session display-index 1
  session-id         10
  session-login      root
  session-manager    netconf
  session-ip         191.167.45.140
  login-time         2016-05-19T12:57:09-0700
  is-our-session     FALSE
  has-running-lock   FALSE
  has-candidate-lock FALSE
 session display-index 2
  session-id         18
  session-login      sysadmin
  session-manager    cli
  session-ip         171.20.102.14
  login-time         2016-05-23T10:45:54-0700
  is-our-session     TRUE
  has-running-lock   FALSE
  has-candidate-lock FALSE
```

Locking/Unlocking a Datastore (E9-2)

Calix AXOS systems support the following types of configuration datastores (databases):

- Running: Stores current configuration data. Running is available via both the CLI and NETCONF interfaces.
- Candidate: Stores configuration data that can be manipulated without impacting the current configuration. Candidate is only available via the NETCONF interface.

You can perform the following types of lock operations on a configuration datastore:

- Session lock: A lock that follows a specific session, and can be freed by the session or when the session ends. An administrator can free the lock by terminating the session.

  If a session with a lock is lost, the lock is freed and:

  - If in the middle of a two-phase commit, the configuration reverts.
  - Any changes made to the running configuration that have been accepted remain.
  - The lock being freed does not control the rollback but is managed via the two-phase commit feature, which may or may not make use of the lock.
- User lock: A lock that follows the specific user, and clears when the user or an administrator unlocks the datastore. This type of lock allows the datastore to remain locked when the session(s) end. For example, use this type of lock to block provisioning during an upgrade or card switchover.

Guidelines

- When a running or candidate datastore is locked, it is only modifiable for the given session or user. This is typically intended to be a short period of time but there is no time limit.
- The unlock command releases a configuration datastore lock previously obtained via a lock operation. A user cannot unlock a configuration datastore that the user did not lock. However, a system administrator can do the following:
  - Kill the operation to terminate a session lock acquired by any user.
  - Specifically free a user lock via the unlock command.
- A lock is not granted if any of the following conditions is true:
  - The target configuration is <candidate>, it has already been modified, and these changes have not been committed or rolled back.
  - The target configuration is <running>, and another User Agent (UA) session has an ongoing confirmed commit.

To lock a running datastore

Issue the following CLI command:

```
Calix-1# lock datastore running [type (user|session)]
```

Note: If the type is not provided, it defaults to a per session lock.

NETCONF example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
  <lock-rpc xmlns="http://www.calix.com/ns/exa/base">
    <datastore>running</datastore>
    <type>user</type>
  </lock-rpc>
</rpc>
]]>]]>
```

To unlock a running datastore

Issue the following CLI command:

```
Calix-1# unlock datastore running
```

NETCONF example to free any lock by a user:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">
  <unlock-rpc xmlns="http://www.calix.com/ns/exa/base">
    <datastore>running</datastore>
  </unlock-rpc>
</rpc>
]]>]]>
```

To end a session

Issue the following CLI command:

```
Calix-1# logout session <ID>
```

CLI example:

```
Calix-1# logout session ?
Possible completions:
  15   networkadmin@192.26.34.21 cli 13:01:14
  16   sysadmin@192.26.116.37 cli 14:06:14 (*)
```

NETCONF example:

```
<rpc message-id="101"
          xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <kill-session>
          <session-id>4</session-id>
        </kill-session>
      </rpc>

      <rpc-reply message-id="101"
           xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <ok/>
      </rpc-reply>
```

To log out a user

Issue the following CLI command:

```
Calix-1# logout user <name>
```

CLI example:

```
Calix-1# logout user ?
Possible completions:
  networkadmin   networkadmin@192.26.34.21 cli 13:01:14
  sysadmin   sysadmin@192.26.116.37 cli 14:06:14 (*)
```

To display locked datastores

- To view information about all locked datastores:
  `Calix-1# **show locks**`
- To view information about locked candidate datastores:
  `Calix-1# **show locks candidate**`
- To view information about locked running datastores:
  `Calix-1# **show locks running**`

The output displays the following information:

locked-time	The time the lock occurred
session-id	Session identifier of the NETCONF session that has the lock
session-ip	IP of the session that has the lock
session-login	User login of the session that has the lock
session-manager	Type of user agent session that has the lock (for example, CLI or NETCONF)

CLI Examples:

```
Calix-1# show locks
locks
 running
  session-id      14
  session-login   root
  session-manager cli
  session-ip      192.23.116.80
  locked-time     2017-12-08T15:12:17-0800
  type            user

Calix-1# show locks
locks
 running
  session-id      14
  session-login   root
  session-manager cli
  session-ip      192.23.116.80
  locked-time     2017-12-08T15:12:36-0800
  type            session
```

NETCONF example for retrieving locks:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="xpath" select="/status/system/locks" />
  </get>
</rpc>
]]>]]>
```

NETCONF output:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-
id="101"><data><status
xmlns="http://www.calix.com/ns/exa/base"><system><locks><running><se
ssion-id>15</session-id><session-login>root</session-login><session-
manager>cli</session-manager><session-ip>172.23.116.37</session-
ip><locked-time>2018-04-06T15:10:19-0700</locked-
time><type>user</type></running></locks></system></status></data></r
pc-reply>]]>]]>
```

To display user sessions

To display information about all of the user sessions on the system, issue the following command:

```
Calix-1# show user-sessions
```

The output displays the following information:

has-candidate-lock	True/false statement that displays if the session has the candidate datastore locked
has-running-lock	True/false statement that displays if the session has the running datastore locked
is-our-session	True/false statement that displays if the session is the source of retrieval request
login-time	Login time for this session
session-id	UA session identifier
session-ip	IP of the session
session-login	User login of the session
session-manager	Type of UA session that has the lock (for example, CLI or netconf)

CLI Example:

```
Calix-1# show user-sessions
user-sessions
 session display-index 1
  session-id          10
  session-login       root
  session-manager     netconf
  session-ip          191.167.45.140
  login-time          2016-05-19T12:57:09-0700
  is-our-session      FALSE
  has-running-lock    FALSE
  has-candidate-lock FALSE
 session display-index 2
  session-id          18
  session-login       sysadmin
  session-manager     cli
  session-ip          171.20.102.14
  login-time          2016-05-23T10:45:54-0700
  is-our-session      TRUE
```

```
  has-running-lock   FALSE
  has-candidate-lock FALSE
```

Note: If the lock is per user ID, all sessions logged in by that user show a lock.

NETCONF example for retrieving sessions:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="xpath" select="/status/system/user-sessions" />
  </get>
</rpc>
]]>]]>
```

NETCONF output:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-
id="101"><data><status
xmlns="http://www.calix.com/ns/exa/base"><system><user-
sessions><session><display-index>1</display-index><session-
id>14</session-id><session-login>root</session-login><session-
manager>netconf</session-manager><session-ip>172.23.116.37</session-
ip><login-time>2018-04-06T15:02:56-0700</login-time><is-our-
session>TRUE</is-our-session><has-running-lock>TRUE</has-running-
lock><has-candidate-lock>FALSE</has-candidate-
lock></session><session><display-index>2</display-index><session-
id>15</session-id><session-login>root</session-login><session-
manager>cli</session-manager><session-ip>172.23.116.37</session-
ip><login-time>2018-04-06T15:03:24-0700</login-time><is-our-
session>FALSE</is-our-session><has-running-lock>TRUE</has-running-
lock><has-candidate-lock>FALSE</has-candidate-lock></session></user-
sessions></system></status></data></rpc-reply>]]>]]>
```

Appendix A

Reference Information

This appendix provides reference information that may be useful during the turn-up of an AXOS system.

Physical Port to CLI Interface Mapping: E9-2

The E9-2 system supports different line interface types (ports) across its various line cards. All line ports use pluggable optic transceiver modules for fiber termination, where the actual line interface speed depends on the type of module used in the port socket. (For example, you can use a 1GE or 2.5GE SFP module in a 10GE SFP+ port socket, and the rate auto-detects.) However, for provisioning purposes, all port types only have one identifier convention in the AXOS CLI, regardless of module type used. This topic provides a mapping between the physical port types on hardware and the corresponding interface identifiers in the AXOS CLI.

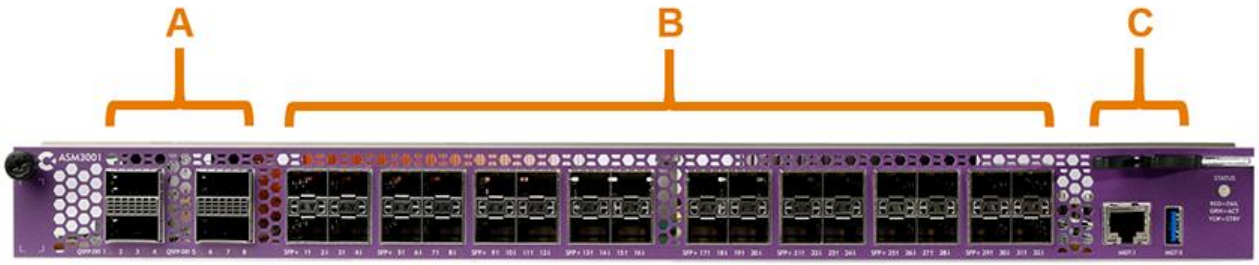
The following table lists the general CLI port identifiers for each port type.

E9-2 Line Interfaces	400GE (4x100GE)	200GE, 100GE, 40GE	10GE	1GE
Port socket types	CDFP	QSFP-DD, QSFP28	SFP+, DWDM SFP+	SFP
CLI Port identifier	c#	q#	x#	g#
Example port ID	1/1/c1	1/1/q1	1/1/x1	1/1/g1

E9-2 Line Interfaces	10G PON	GPON
Port socket types	XGS-PON XFP, NG-PON2 XFP	GPON SFP
CLI Port identifier	xp#	gp#
Example port ID	2/1/xp1	5/1/gp1

The following tables lists the specific ports to CLI interface mapping for each E9-2 card type.

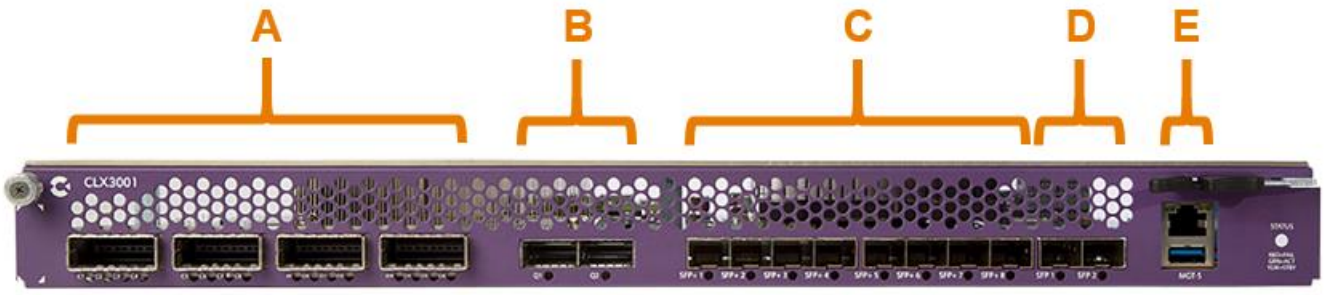
ASM3001



Key	Port Descriptions	Port IDs in CLI
A	**QSFP-DD:** (4) QSFP-DD sockets for 200GE uplink connections per port	q1-q4
B	**SFP+:** (32) SFP+ 10GE ports for uplink / downlink / aggregation (support 10G/2.5G/1G Ethernet SFP+ modules)	x1-x32
C	**RJ-45 Ethernet:** (1) 100/1000 Ethernet 'walk up' Craft port for *temporary* local management [1] **USB 2.0:** (1) USB Craft management port; connects to a USB-to-Wi-Fi adapter for temporary local Craft access [2]	craft */*/1

Notes: Not shown are the E9-2 rear shelf Craft Ethernet (craft */*/2) and serial management ports.
[1] Use the rear Ethernet management port(s) for *permanent* out-of-band management connections.
[2] Management via the USB port is not yet supported in software as of R20.x

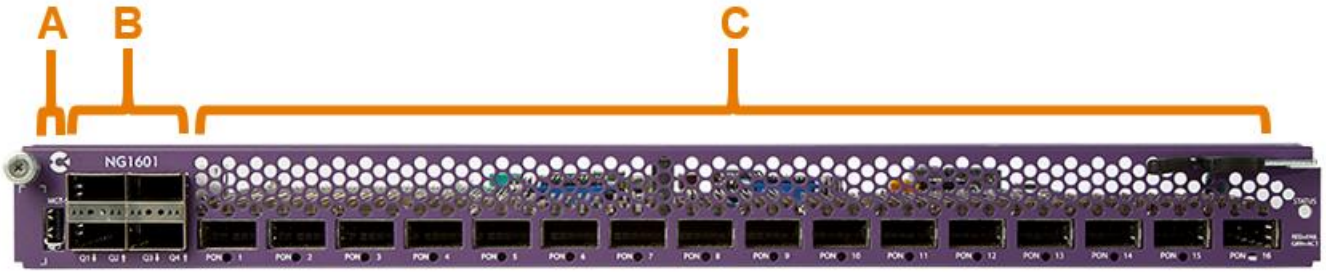
CLX3001



Key	Port Descriptions	Port IDs in CLI
A	**CDFP:** (4) CDFP sockets, each terminating (4) QSFP interfaces via CDFP copper connectors to support 4x100GE interconnection links to access line cards (Use CDFP-4x/QSFP-28 fan out cables to interconnect the aggregation card to access line cards)	c1-c16 (c1-c4, c5-c8, c9-c12, c13-c16)
B	**QSFP28:** (2) QSFP-28 sockets for 100GE uplink connections	q1-q2
C	**SFP+:** (8) SFP+ 10GE uplink, aggregation, or service ports	x1-x8
D	**SFP:** (2) SFP 1GE aggregation or service ports	g1-g2
E	**RJ-45 Ethernet:** (1) 100/1000 Ethernet 'walk up' Craft port for *temporary* local management [1] **USB 2.0:** (1) USB Craft management port; connects to a USB-to-Wi-Fi adapter for temporary local Craft access [2]	craft */*/1

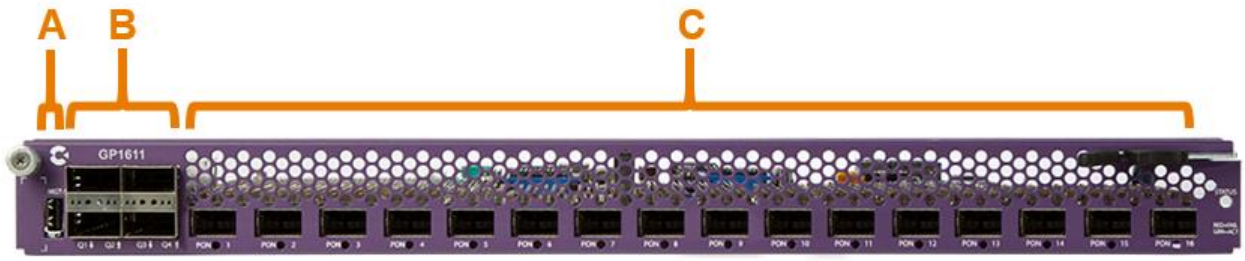
Notes: Not shown are the E9-2 rear shelf Craft Ethernet (craft */*/2) and serial management ports.
[1] Use the rear Ethernet management port(s) for permanent out-of-band management connections.
[2] Management via the USB port is not yet supported in software as of R20.x

NG1601



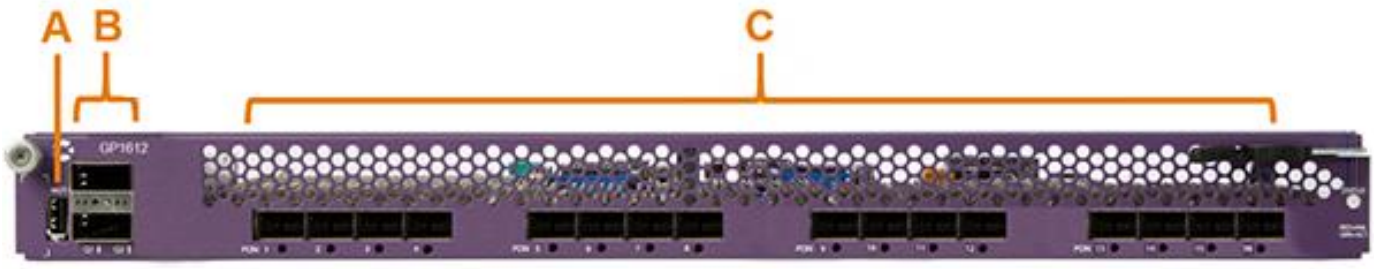
Key	Port Descriptions	Port IDs in CLI
A	**USB 2.0:** (1) Craft management port; connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access	1
B	**QSFP-28:** (4) QSFP-28 sockets for 4x100GE or 4x40GE uplink inter-connections to the aggregation shelf (two active, two standby)	q1-q4
C	**PON XFP:** (16) XFP PON OLT access ports (XGS-PON or NG-PON2 optics)	xp1-xp16

GP1611



Key	Port Descriptions	Port IDs in CLI
A	**USB 2.0:** (1) Craft management port; connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access	1
B	**QSFP-28:** (4) QSFP-28 sockets for 4x100GE or 4x40GE uplink inter-connections to the aggregation shelf (two active, two standby)	q1-q4
C	**GPON SFP:** (16) SFP GPON OLT access ports	gp1-gp16

GP1612



Key	Port Descriptions	Port IDs in CLI
A	**USB 2.0:** (1) Craft management port; connects to a USB Wi-Fi or Ethernet adapter for temporary local Craft access	1
B	**QSFP-28:** (2) QSFP-28 sockets for 2x100GE or 2x40GE uplink inter-connections to the aggregation shelf (one active, one standby)	q1-q2
C	**GPON SFP:** (16) SFP GPON OLT access ports	gp1-gp16

Physical Port to CLI Interface Mapping: E7-2

The E7-2 system supports different line interface types (ports) across its various line cards. All line ports use pluggable optic transceiver modules for fiber termination, where the actual line interface speed depends on the type of module used in the port socket. (For example, you can using a 2.5GE module in a 1GE port socket, and the rate auto-detects.) However, for provisioning purposes, all port types only have one identifier convention in the AXOS CLI, regardless of module type used. This topic provides a mapping between the physical port types on hardware and the corresponding interface identifiers in the AXOS CLI.

The following table lists the general CLI port identifiers for each port type.

E7-2 Line Interfaces	40GE	10GE	1GE	10G PON	GPON
Port socket types	QSFP-DD	XFP, SFP+, DWDM SFP+	CSFP, SFP	XGS-PON XFP, NG-PON2 XFP	GPON SFP
CLI Port identifier	q#	x#	g#	xp#	gp#
Example port ID	1/1/q1	1/1/x1	1/1/g1	1/1/xp1	1/1/gp1

The following tables lists the specific ports to CLI interface mapping for each E7-2 card type.

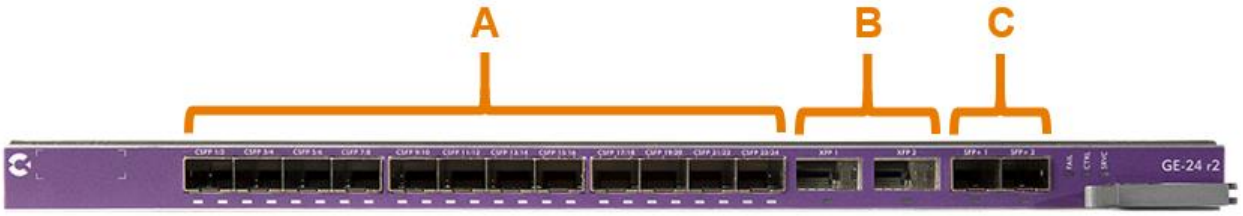
CE201

Key	Port Descriptions	Port IDs in CLI
A	**SFP+:** (12) SFP+ 10GE aggregation or service ports	x1-x12
B	**QSFP-DD:** (2) QSFP-DD socket for 100GE / 40GE uplink connections	q1-q2

10GE-12

Key	Port Descriptions	Port IDs in CLI
A	**SFP+:** (12) SFP+ 10GE aggregation or service ports	x1-x12
B	**XFP:** (2) XFP 10GE uplink or transport ports	x13-x14
C	**QSFP-DD:** (1) QSFP-DD socket for 40GE uplink connections	q1

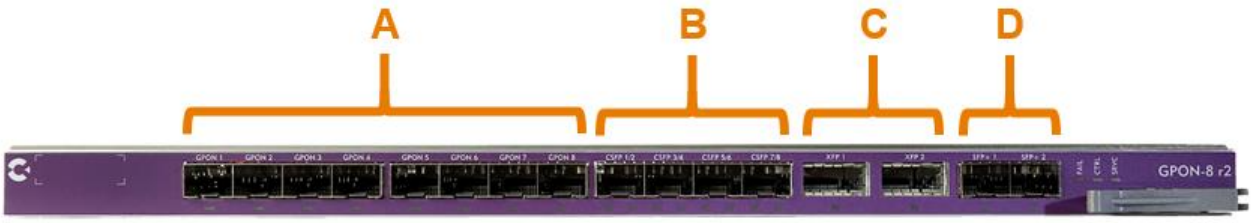
GE-24 r2



Key	Port Descriptions	Port IDs in CLI
A	**CSFP:** (12) two-port CSFP sockets, providing (24) 1GE aggregation or service ports; also support SFP modules (reduces capacity to 12 ports*)	g1-g24
B	**XFP:** (2) XFP 10GE uplink / transport ports	x1-x2
C	**SFP+:** (2) SFP+ 10GE uplink / transport ports	x3-x4

***Note:** When SFP modules are used in the CSFP sockets, capacity reduces to (12) 1GE ports, where only the odd-numbered ports are used: g1, g3, g5 ... g21, g23 in CLI.

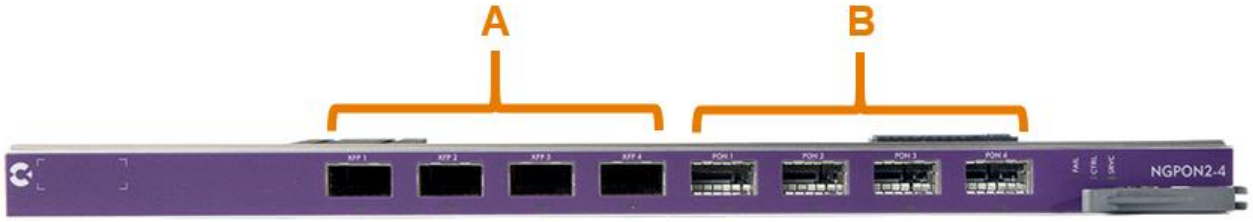
GPON-8 r2



Key	Port Descriptions	Port IDs in CLI
A	**GPON SFP:** (8) SFP GPON OLT ports	gp1-gp8
B	**CSFP:** (4) two-port CSFP sockets, providing (8) 1GE aggregation or service ports; also support SFP modules (reduces capacity to 4 ports*)	g1-g8
C	**XFP:** (2) XFP 10GE uplink / transport ports	x1-x2
D	**SFP+:** (2) SFP+ 10GE uplink / transport ports	x3-x4

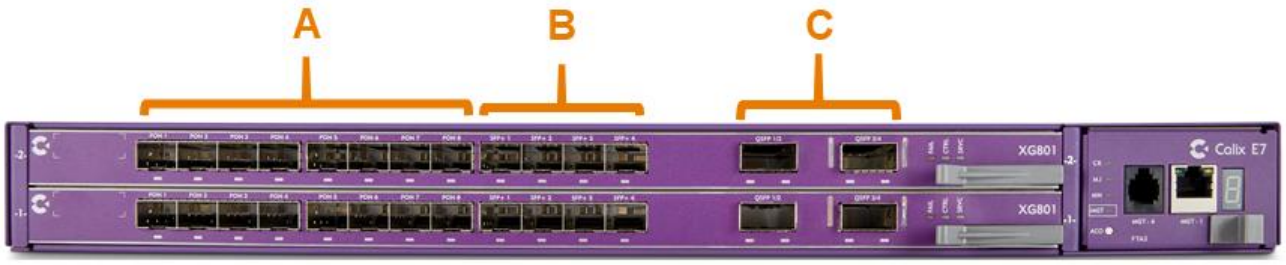
***Note:** When SFP modules are used in the CSFP sockets, capacity reduces to (4) 1GE ports, where only the odd-numbered ports are used: g1, g3, g5, g7.

NG-PON2-4



Key	Port Descriptions	Port IDs in CLI
A	**XFP:** (4) XFP 10GE uplink / transport ports	x1-x4
B	**PON XFP:** (4) XFP PON OLT ports (XGS-PON or NG-PON2 optics)	xp1-xp4

XG801



Key	Port Descriptions	Port IDs in CLI
A	**PON SFP:** (8) SFP PON OLT ports (XGS-PON or GPON optics)	xp1-xp8
B	**SFP+:** (4) SFP+ 10GE aggregation or service ports	x1-x4
C	**QSFP-DD:** (2) QSFP-DD socket for 100GE / 40GE uplink connections	q1-q2

Note: The PON port description in the CLI will always be xp regardless of whether the port is set to GPON or XGS-PON>

Physical Port to CLI Interface Mapping: E3-2

The E3-2 system supports various line interface modules, with all ports using pluggable optic transceiver modules for fiber termination. For provisioning purposes, each port type has a common identifier convention in the AXOS CLI. This topic provides a mapping between the physical port types on hardware and the corresponding interface identifiers in the AXOS CLI.

The following table lists the general CLI port identifiers for each port type.

E3-2 Line Interfaces	10GE	10G PON	GPON
Port socket types	XFP, SFP+, DWDM SFP+	10G EPON XFP, XGS-PON XFP	GPON SFP
CLI Port identifier	x#	xp#	gp#
Example port ID	1/1/x1	1/1/xp4	1/1/gp8

The following tables lists the specific ports to CLI interface mapping for each E3-2 interface module type.

XE401 WAN module

Key	Port Descriptions	Port IDs in CLI
A	**XFP:** (4) XFP 10GE uplink or transport ports	x1-x4

XE401S WAN module

Key	Port Descriptions	Port IDs in CLI
A	**SFP+:** (4) SFP+ 10GE uplink or transport ports	x1-x4

XEP201 interface module (10G EPON)

Key	Port Descriptions	Position	Port IDs in CLI
A	**PON XFP:** (2) XFP PON OLT ports (10G EPON optics) per interface module; up to two modules.	IM 1	xp1-xp2
		IM 2	xp3-xp4

NG201 interface module (NGPON2 / XGS-PON)

Key	Port Descriptions	Position	Port IDs in CLI
A	**PON XFP:** (2) XFP PON OLT ports (XGS-PON or NG-PON2 optics) per interface module; up to two modules.	IM 1	xp1-xp2
		IM 2	xp3-xp4

GP401 interface module (GPON)

Key	Port Descriptions	Position	Port IDs in CLI
A	**PON SFP:** (4) SFP GPON OLT ports, per interface module; up to two modules.	IM 1	gp1-gp4
		IM 2	gp5-gp8

E9-2 LED Behavior

Active CLX3100 card status indicators

Each active CLX3100 card has a status LED to indicate the card's operational status.

Color	Status	Description
Blue	On	Indicates the card is in the process of collecting a log during a core dump
Red	On	Indicates either: • A card is in the early boot process (on a power cycle) • A fault has occurred that should be addressed
	Blinking (50/50)	Indicates either: • Local host booting in process • A card is reloading
	Blinking (87/17)	A very short off indicates a card is missing Board ID (BID) data; at boot time, the product model and "version" are determined from the BID data
Green	On	Indicates normal operation Aggregation card is up and operational
Amber	Blinking	Indicates normal operation A software upgrade is in progress

Standby CLX3100 card status indicators

Each standby CLX3100 card has a status LED to indicate the card's operational status.

Color	Status	Description
Blue	On	Indicates the card is in the process of collecting a log during a core dump
Red	On	Indicates either: • A card is in the early boot process (on a power cycle) • A fault has occurred that should be addressed
	Blinking (50/50)	Indicates either: • Local host booting in process • A card is reloading
	Blinking (87/17)	A very short off indicates a card is missing Board ID (BID) data; at boot time, the product model and "version" are determined from the BID data
Green	On	Indicates normal operation Aggregation card is up and operational
Amber	On	Indicates normal operation Software image has been copied from the active CLX3100 and installed on the standby CLX3100; card is STBY HOT
	Blinking	Indicates normal operation, either: • Software image is being copied from the active CLX3100 card to the standby CLX3100 card • Card is in the process of booting

Line card status indicators

Each access line card has a status LED to indicate the card's operational status.

Color	Status	Description
Blue	On	Blue is the default color on boot initiation, before it changes to red during the boot process. If an LED is stuck in Blue, an early process failure likely occurred where the boot process never fully began before getting stuck.
Red	On	Indicates a card is in the process of early booting or a fault has occurred that should be addressed
	Blinking (50/50)	Indicates the card is about to reboot or the local host booting is in process
	Blinking (87/17)	A very short off indicates a card is missing Board ID (BID) data; at boot time, the product model and "version" are determined from the BID data
Green	On	Indicates normal operation Line card is connected to the active aggregation card; a software load is installed on the card
	Blinking	Indicates normal operation Line card is connecting to the active aggregation card
Amber	Blinking	Indicates normal operation Line card is connected to the active aggregation card; a software upgrade is in progress

Port status indicators

Each PON interface port on a line card has a LED located below its module socket to indicate port status.

Color	Status	Description
Green	On	Indicates that at least one ONT is in service on the PON
	Blinking	After module insertion, blinks (3) times to indicate the inserted module is recognized and allowed to operate Blinks steadily while the first ONT on the port is ranging
	Off	Socket is vacant or an invalid module is inserted

Fan module status indicators

Each E9-2 fan module has a LED visible inside the fan.

Color	Status	Description
Green	On	Inserted module is recognized and allowed to operate
	Off	No power present
Red	On	A fault has occurred that should be addressed
	Off	No power present

Reserved and Designated VLANs

The following table shows a list of reserved and default VLANs on the AXOS system.

VLAN ID	Usage
Reserved VLANs	
1002-1005 4095	These VLANs are reserved for internal management.
Default VLANs	
85	This VLAN ID may be used for management of CPE devices. If so, it must be plumbed through the access network (for example, added to the transport profile).
999	By default, the uplink interface references a transport service profile (SYSTEM_TSP) that contains VLAN 999. This VLAN is used by the auto-provisioning feature during turn-up when the system initially boots up; it will try to acquire a DHCP lease on this VLAN. Calix strongly recommends that you dedicate a VLAN for management traffic only and do not use it for traffic related to services. The default transport service profile may be modified to include the management VLAN used by your network or a new one may be created.

Interfaces with a Reserved Subnet/VRF

The following table lists AXOS interfaces that use a reserved subnet or the internal VRF.

AXOS System	Interface Name	Reserved Subnet or VRF
E3-2/E7-2/E9-2	craft	192.168.1.x/24*
E9-2	multibind0	169.254.3.x/24
E9-2	dhcpsrv	169.254.4.x/24
E3-2/E7-2/E9-2	net2	internal VRF
E3-2/E7-2/E9-2	eth2/bond0	internal VRF
E9-2	eth5	169.254.7.x/24
E9-2	mvlan	192.168.8.x/24#

* This default subnet is configurable.

This default subnet is configurable; see 'Layer 3 Video Service VLANs' guidelines in the *AXOS everyPON Services Guide*.

To display internal interfaces, use the '**show ip system interface**' CLI command.

Subnet Table

Class address ranges:

- Class A = 1.0.0.0 to 126.0.0.0
- Class B = 128.0.0.0 to 191.255.0.0
- Class C = 192.0.1.0 to 223.255.255.0

Reserved address ranges for private (non-routed) use:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Note: Refer to *E9-2 Reserved Subnet Masks* (on page 395) for more information.

- Other reserved addresses:
- 127.0.0.0 for loopback and IPC on the local host
- 224.0.0.0 – 239.255.255.255 for multicast addresses

Class A

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/8	255.0.0.0	0	16777214
/9	255.128.0.0	2 (0)	8388606
/10	255.192.0.0	4 (2)	4194302
/11	255.224.0.0	8 (6)	2097150
/12	255.240.0.0	16 (14)	1048574
/13	255.248.0.0	32 (30)	524286
/14	255.252.0.0	64 (62)	262142
/15	255.254.0.0	128 (126)	131070
/16	255.255.0.0	256 (254)	65534
/17	255.255.128.0	512 (510)	32766
/18	255.255.192.0	1024 (1022)	16382
/19	255.255.224.0	2048 (2046)	8190
/20	255.255.240.0	4096 (4094)	4094
/21	255.255.248.0	8192 (8190)	2046
/22	255.255.252.0	16384 (16382)	1022
/23	255.255.254.0	32768 (32766)	510
/24	255.255.255.0	65536 (65534)	254
/25	255.255.255.128	131072 (131070)	126
/26	255.255.255.192	262144 (262142)	62
/27	255.255.255.224	524288 (524286)	30
/28	255.255.255.240	1048576 (1048574)	14
/29	255.255.255.248	2097152 (2097150)	6
/30	255.255.255.252	4194304 (4194302)	2

Class B

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/16	255.255.0.0	0	65534
/17	255.255.128.0	2 (0)	32766
/18	255.255.192.0	4 (2)	16382
/19	255.255.224.0	8 (6)	8190
/20	255.255.240.0	16 (14)	4094
/21	255.255.248.0	32 (30)	2046
/22	255.255.252.0	64 (62)	1022
/23	255.255.254.0	128 (126)	510
/24	255.255.255.0	256 (254)	254
/25	255.255.255.128	512 (510)	126
/26	255.255.255.192	1024 (1022)	62
/27	255.255.255.224	2048 (2046)	30
/28	255.255.255.240	4096 (4094)	14
/29	255.255.255.248	8192 (8190)	6
/30	255.255.255.252	16384 (16382)	2

Class C

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/24	255.255.255.0	0	254
/25	255.255.255.128	2 (0)	126
/26	255.255.255.192	4 (2)	62
/27	255.255.255.224	8 (6)	30
/28	255.255.255.240	16 (14)	14
/29	255.255.255.248	32 (30)	6
/30	255.255.255.252	64 (62)	2

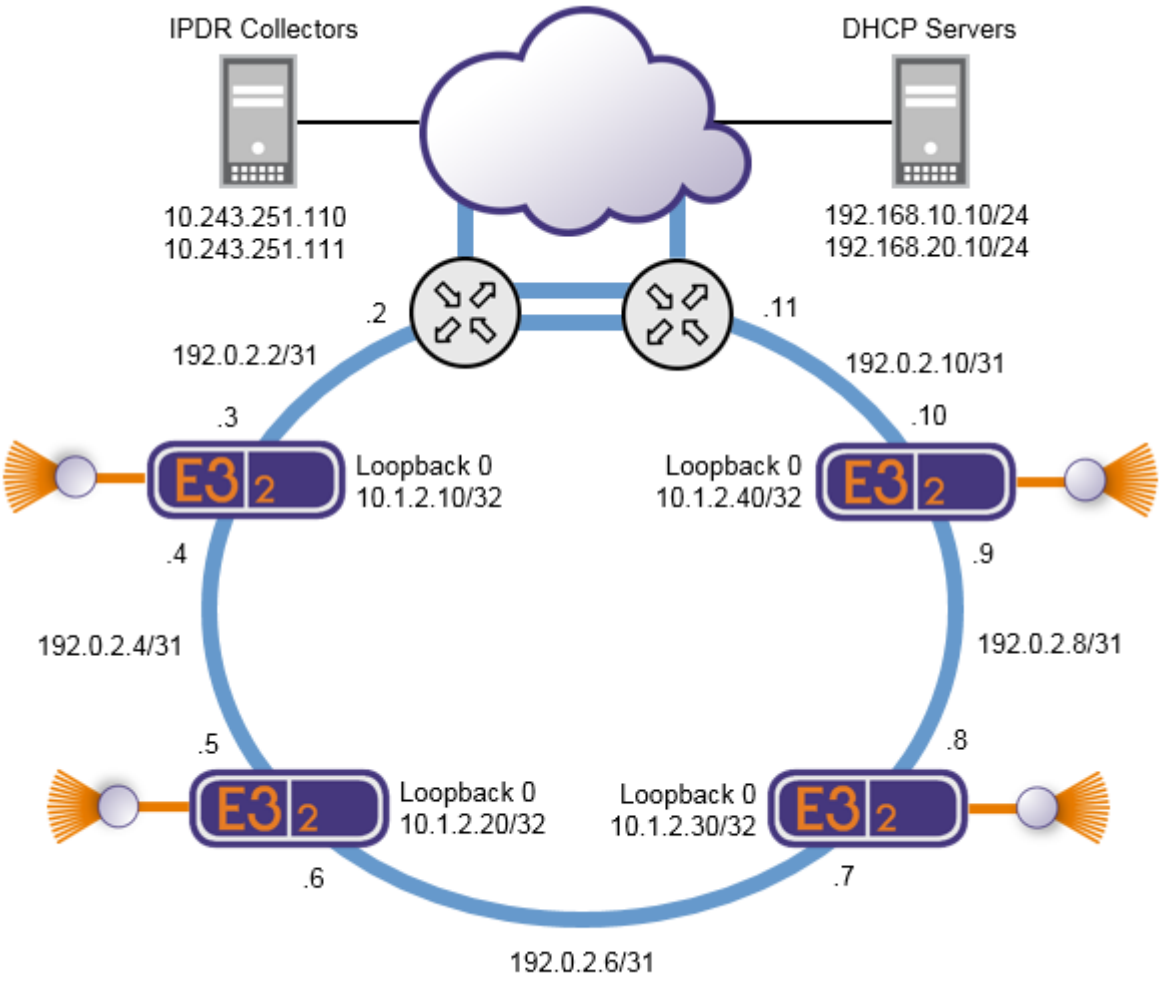
For information on subnetting, refer to the following:

- RFC 1878
- RFC 1817
- RFC 1812

Example IPv4 Network Addressing Scheme (E3-2)

For an example IPv4 network addressing scheme, see the following diagram.

Note: In this example, a /31 network is used for each link around the ring to conserve public IP addresses.



Built-In CPU Filters and Rate-Limiters

This topic describes the internal rate limiters and CPU filters that do not use ACL resources.

Traffic is throttled to the CPU to provide protection as shown below:

Queue Number	Bandwidth (kilo bits /sec)	Use
1	30,000	CPU port global limiter
2	2,600	Route to CPU
3	325	Neighbor Miss traffic
4	325	Classifier trap type "Host"
5	650	Classifier Trap type "DHCP"

The following packet types are dropped:

- Src IP Equals Destination Ip
- Destination Ip to zero
- Source Ip is Multicast
- Ipv4 version error
- Ipv4 Checksum error
- Ipv4 header length error
- Ipv4 Total Length error
- Ipv6 Version error
- Ipv6 Unspecified destination
- Ipv6 multicast source
- Ipv6 next header NULL
- Ipv6 unspecified source

The following DoS Controls are enabled and trapped to the CPU:

- Enable sip=dip checking
- Enable Minimum TCP header size checking
- Enable Tcp fragment Offset less than 8
- Enable Tcp Flag checking
  - TCP SN Flags zero trapped to CPU
- Enable L4 port checking
  - TCP_EQUAL_PORT trapped to CPU
- Enable Tcp fragment checking
  - TCP incomplete header trapped to CPU

- Enable Icmp checking
  - ICMP data greater than 576 trapped to CPU
- Enable IcmpPktOversize check
  - ICMP data greater than 576 trapped to CPU
- Enable MAC SA equals MAC DA check
  - SA == DA trapped to CPU
- Enable IcmpV6 Ping size check
  - ICMP data greater than 576 trapped to CPU
- Enable Icmp fragments check
  - ICMP fragmented data trapped to CPU
- Enable Tcp Ports Equal check
  - TCP_EQUAL_PORT trapped to CPU
- Enable Udp port check
  - UDP Equal ports trapped to CPU
- Enable Syn flood checking
  - Sync Flood trapped to CPU
- The following are trapped to CPU.
  - Ttl 0/1 packets

Configuring SNMP Management (E3-2/E7-2)

Note: Refer to the *AXOS SNMP MIBs Reference* for a list of supported MIBs.

This topic shows you how to configure Simple Network Management Protocol (SNMP).

SNMP is an application-layer protocol used for exchanging management information between managers and agents. The SNMP architecture consists of a manager, agent, and a MIB. The SNMP manager is a console through which network administrators perform network management functions. The SNMP agent and MIB reside on the AXOS system. To configure SNMP, you define how the manager and agent communicate.

Configuration guidelines

- AXOS systems support SNMPv2 and/or SNMPv3, where you can configure either version or both simultaneously.
- SNMPv1 is not supported.
- To allow an SNMP manager access to the SNMP agent, you must specify a trap host (IP address) to which the agent forwards traps.
- AXOS systems support up to eight trap hosts and up to eight SNMPv2c community strings.
- SNMPv3 users are distinct from other management interface users. The SNMP subsystem uses its own authentication mechanism in accordance with security standards defined by SNMPv3.
- Configurable SNMPv3 user security levels include:
    - **No Auth No Priv**: Does not check authentication protocol, or privacy protocol
    - **Auth No Priv**: Checks the authentication protocol and key, but does not check the privacy protocol
    - **Auth Priv**: Checks the authentication protocol and key, and checks the privacy protocol and key

Parameters

You can configure the following parameters for SNMP version 2 management:

Parameter	Description	Valid Options
Admin State	Enable/disable SNMPv2 support.	Enable Disable (default)
Community String		
Community String*	Name of the read-only SNMPv2 community, which acts as a password.	Alpha-numeric string, up to 32 characters
Access*	Sets the access level. The system supports read-only (Ro) for SNMP v2.	Ro
Trap Host		
Host*	Remote IP address of the trap destination to which traps are forwarded.	IPv4 address 0.0.0.0 (default)
Community*	A previously configured community string for the trap host.	Any configured community string
Trap Type	Sets the trap type: • **Trap**: Receives trap (SNMP message) only. • **Inform**: Receives traps and acknowledges receipt of traps. Unacknowledged traps are resent until they are acknowledged.	Trap (default) Inform
Retries	When the trap type is configured as "Inform", the number of times to retry may be configured.	1..6 1 (default)
Timeout	When the trap type is configured as "Inform", the timeout value in milliseconds may be configured.	100..500 200 (default)

* User input required

You can configure the following parameters for SNMP version 3 management:

Parameter	Description	Valid Options
Admin State	Enable/disable SNMPv3 support.	Enable Disable (default)
V3 Users		
Name*	Defines a user name for the account.	Alpha-numeric string, up to 32 characters
Authentication Protocol	Sets the authentication protocol: • Message-digest algorithm (MD5) • Secure hash algorithm (SHA)	NONE (default) MD5 SHA
Authentication Key	(Optional) Defines the user's authentication key (pass phrase). Authentication is performed via the user's key to sign the SNMP message being sent. The authentication key displays when you select authorization protocol MD5 or SHA.	Alpha-numeric string, 8–32 characters notvalid (default)
Privacy Protocol	(Optional) Sets the privacy protocol to encrypt the data portion of the SNMP message. • Advanced Encryption Standard (AES) • Data Encryption Standard (DES)	NONE (default) AES DES
Privacy Key	(Optional) Defines the user's privacy key. The privacy key displays when you select privacy protocol AES or DES.	Alpha-numeric string, 8–32 characters notvalid (default)
Trap Host		
Host*	Remote IP address of the trap destination to which traps are forwarded.	IPv4 address (0.0.0.0 ‡)
User*	A previously configured name for the SNMPv3 user account.	Any existing configured SNMPv3 user name
Security Level	Sets the security level to use for SNMP messages. For more information, see the Considerations section above.	No Auth No Priv (default) Auth No Priv Auth Priv
Trap Type	Sets the trap type: • **Trap**: Receives trap (SNMP message) only. • **Inform**: Receives traps and acknowledges receipt of traps. Unacknowledged traps are resent until they are acknowledged.	Trap (default) Inform
Retries	When the trap type is configured as "Inform", the number of times to retry may be configured.	1..6 1 (default)
Timeout	When the trap type is configured as "Inform", the timeout value in milliseconds may be configured.	100..500 200 (default)

* User input required

To configure SNMPv2 management

1. **Calix-1(config)# snmp**
2. **Calix-1(config-snmp)# v2 admin-state {enable|disable}**
3. **Calix-1(config-snmp)# v2 community <string> <ro>**
4. **Calix-1(config-snmp)# v2 trap-host <IPv4> <community string> [trap-type {inform <retries <number>>|timeout <number>>|trap}]**

To configure SNMPv3 management

1. **Calix-1(config)# snmp**
2. **Calix-1(config-snmp)# v3 admin-state {enable|disable}**
3. **Calix-1(config-snmp)# v3 user <username> authentication protocol <NONE>**

   or

   Calix-1(config-snmp)# v3 user <username> authentication protocol {MD5|SHA} [key {notvalid|string} privacy protocol <NONE>]

   or

   Calix-1(config-snmp)# v3 user <username> authentication protocol {MD5|SHA} [key {notvalid|string} privacy protocol {AES|DES} key {notvalid|string}]

```
Calix-1(config-snmp)# v3 trap-host <IPv4> <v3 username> security-level
{noAuthNoPriv|authNoPriv|authPriv} [trap-type {inform inform <retries
<number>>|timeout <number>>|trap}]
```