Engineering
Simplicity

Junos Fusion Enterprise User Guide

Published
2025-04-16

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos Fusion Enterprise User Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

About This Guide

Junos Fusion Enterprise enables enterprise switching networks to combine numerous switches into a single, port-dense system managed from a single point known as the aggregation device. Junos Fusion Enterprise simplifies network administration because the system is viewed as a single device by the larger network. Use the topics on this page to understand Junos Fusion Enterprise, configure the aggregation device, and manage satellite devices.

1

PART

Junos Fusion Enterprise

CHAPTER 1

Junos Fusion Enterprise Overview

IN THIS CHAPTER

Junos Fusion Enterprise Overview

Junos Fusion provides a method of significantly expanding the number of available network interfaces on a device—called an *aggregation device*—by allowing the aggregation device to add interfaces through interconnections with *satellite devices*. The entire system—the interconnected aggregation device and satellite devices—is called a *Junos Fusion*. A Junos Fusion simplifies network topologies and administration because it appears to the larger network as a single, port-dense device that is managed using one IP address.

Junos Fusion Enterprise brings the Junos Fusion technology to enterprise switching networks. In a Junos Fusion Enterprise, EX9200 switches act as aggregation devices while EX2300, EX3400, EX4300 or QFX5100 switches act as satellite devices.

Junos Fusion Enterprise provides the following benefits:

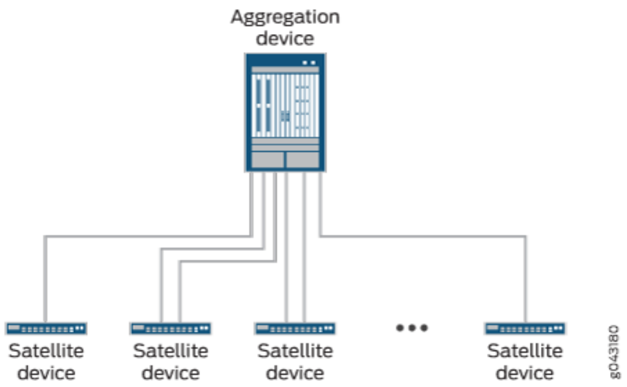
- Hides the complexity of managing a large campus network with a single point of management for up to 6,000 ports or 128 switches.

- Reduces operational costs with plug-and-play provisioning of access devices.
- Easy to scale by adding satellite devices for additional ports.

In a Junos Fusion Enterprise, each satellite device has at least one connection to the aggregation device. The aggregation device acts as the single point of management for all devices in the Junos Fusion Enterprise. The satellite devices provide network interfaces that send and receive network traffic.

Figure 1 on page 3 provides an illustration of a basic Junos Fusion Enterprise topology.

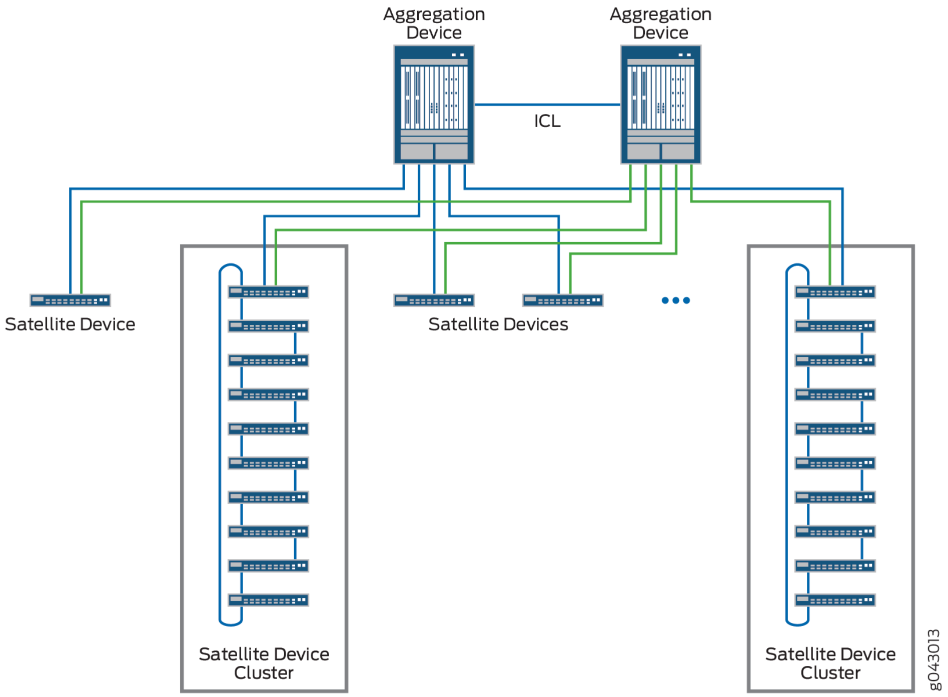
Figure 1: Basic Junos Fusion Enterprise Topology



Junos Fusion Enterprise supports up to two aggregation devices that can be multi-homed to each satellite device, as well as satellite device clustering, which allows multiple satellite devices to be clustered into a group and cabled into the Junos Fusion as a group instead of as individual satellite devices. A Junos Fusion Enterprise using two aggregation devices uses the ICCP protocol from MC-LAG to connect and maintain the Junos Fusion topology.

Figure 2 on page 4 illustrates an example of a more complex Junos Fusion Enterprise topology. This dual-aggregation topology includes both standalone and clustered satellite devices. The aggregation devices are multi-homed to each standalone satellite device and to each satellite device cluster.

Figure 2: Junos Fusion Topology with Dual Aggregation Devices and Satellite Device Clusters



An EX9200 switch acting as an aggregation device in a Junos Fusion Enterprise is responsible for almost all management tasks, including interface configuration for every satellite device interface in the topology. The aggregation device runs Junos OS software for the entire Junos Fusion Enterprise, and the network-facing interfaces on the satellite devices—called *extended ports*—are configured from the aggregation device and support features that are supported by the version of Junos OS running on the aggregation device.

The satellite devices and the aggregation device maintain the control plane for the Junos Fusion Enterprise using multiple internal satellite management protocols. Network traffic can be forwarded between satellite devices through the aggregation device. Junos Fusion Enterprise supports the IEEE 802.1BR standard.

Junos Fusion Enterprise provides the following benefits:

- Simplified network topology—You can combine multiple devices into a topology that appears to the larger network as a single device, and then manage the device from a single IP address.

- Port density—You can configure a large number of network-facing interfaces into a topology that operates as a single network device.

- Manageability—You can manage a Junos Fusion that supports a large number of network-facing interfaces from a single point. The single point of management, the aggregation device, runs Junos OS software for the entire Junos Fusion.

- Flexibility—You can easily expand the size of your Junos Fusion by adding satellite devices to the Junos Fusion as your networking needs grow.

- Investment protection—In environments that need to expand because the capabilities of the existing hardware are maximized, a Junos Fusion can be a logical upgrade option because it enables the network to evolve with minimal disruption to the existing network and without having to remove the existing, previously purchased devices from the network.

RELATED DOCUMENTATION

Network Configuration Example: Enabling Junos Fusion Enterprise on an Enterprise Campus Network

Understanding Junos Fusion Enterprise Components | 5

Understanding Junos Fusion Ports | 19

Understanding the Flow of Data Packets in a Junos Fusion Topology | 41

Configuring or Expanding a Junos Fusion Enterprise | 49

Understanding Junos Fusion Enterprise Components

IN THIS SECTION

This topic describes the components of a Junos Fusion Enterprise. It covers:

Junos Fusion Topology

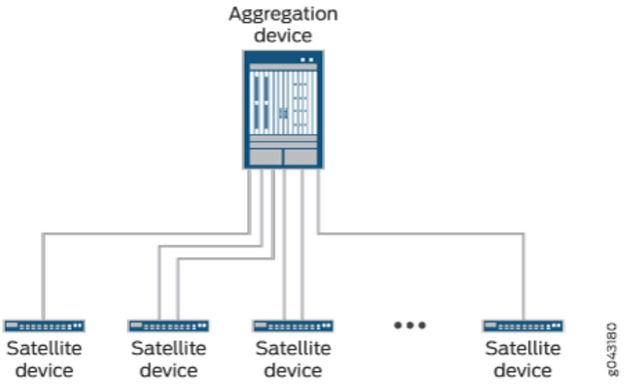
A basic Junos Fusion topology is composed of an aggregation device and multiple satellite devices. Each satellite device has at least one connection to the aggregation device. The satellite devices provide interfaces that send and receive network traffic. Network traffic can be forwarded over the aggregation device within the Junos Fusion.

The satellite devices and the aggregation device maintain the control plane for the Junos Fusion using multiple internal satellite management protocols. Junos Fusion supports the IEEE 802.1BR standard.

The aggregation device acts as the management points for all devices in the Junos Fusion. All Junos Fusion management responsibilities, including interface configuration for every satellite device interface in the Junos Fusion, are handled by the aggregation device. The aggregation device runs Junos OS software for the entire Junos Fusion, and the interfaces on the satellite devices are configured from the aggregation device and mostly support features that are supported by the version of Junos OS running on the aggregation device.

See Figure 3 on page 6 for an illustration of a basic Junos Fusion topology.

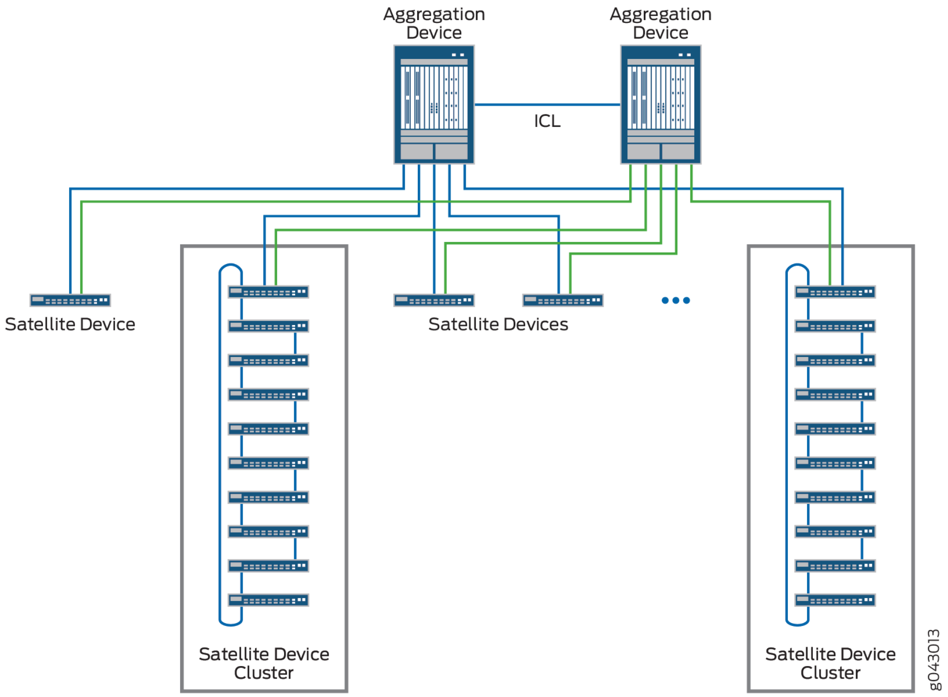
Figure 3: Basic Junos Fusion Topology



Junos Fusion Enterprise supports multihomed dual aggregation device topologies and satellite device clusters. A multihomed topology with two aggregation devices provides load balancing and redundancy to the Junos Fusion Enterprise topology. A satellite device cluster allows you to group multiple satellite devices into a single group, and connect the group to the Junos Fusion as a group instead of as single standalone devices. Dual aggregation device topologies and satellite device clustering are discussed in more detail in "Dual Aggregation Device Topologies" on page 8 and "Satellite Device Clustering" on page 9.

Figure 4 on page 7 shows a complex Junos Fusion Enterprise topology using dual aggregation devices and satellite device clusters.

Figure 4: Junos Fusion Topology with Dual Aggregation Devices and Satellite Device Clusters



Aggregation Devices

This section discusses aggregation devices and contains the following sections:

Aggregation Devices Overview

An aggregation device:

- Is an EX9200 switch in a Junos Fusion Enterprise.
- Has at least one connection to each satellite device or satellite device cluster.
- Runs Junos OS software.
- Manages the entire Junos Fusion. All Junos Fusion configuration management is handled on the aggregation device or devices, including interface configuration of the satellite device interfaces.

The hardware specifications for aggregation devices in a Junos Fusion Enterprise are discussed in greater detail in Understanding Junos Fusion Enterprise Software and Hardware Requirements.

Dual Aggregation Device Topologies

Junos Fusion Enterprise supports dual aggregation device topologies. The advantages of a dual aggregation device topology include:

- Load balancing. Traffic traversing the Junos Fusion Enterprise can be load balanced across both aggregation devices.

- Redundancy. The Junos Fusion Enterprise can pass traffic even in the unexpected event of an aggregation device failure.

A Junos Fusion Enterprise supports multiple aggregation devices using Multichassis Link Aggregation (MC-LAG) groups and the Inter-Chassis Control Protocol (ICCP).

A Junos Fusion Enterprise with dual aggregation devices is configured as an MC-LAG with one redundancy group. The redundancy group includes two peering chassis IDs—the aggregation devices—and all satellite devices in the Junos Fusion Enterprise. The aggregation devices are connected using an interchassis link (ICL) in the MC-LAG topology.

ICCP runs inside the Junos Fusion on all dual aggregation topologies. ICCP parameters are automatically configured in a Junos Fusion Enterprise by the automatic ICCP provisioning feature, which simplifies the ICCP configuration procedure. ICCP configuration can be customized, however.

Figure 4 on page 7 provides an illustration of a dual aggregation device topology.

Satellite Devices

Satellite Devices Overview

A satellite device:

- Is an EX2300, EX3400, EX4300, EX4600 or QFX5100 switch in a Junos Fusion Enterprise.

- Runs a version of satellite software after being converted into a satellite device.

- Has either a direct connection to an aggregation device, or is part of a satellite device cluster that is cabled to an aggregation device.

- Provides network interfaces to send and receive traffic for the Junos Fusion.

- Is managed and configured by the aggregation device.

The hardware specifications for satellite devices in a Junos Fusion Enterprise are discussed in greater detail in Understanding Junos Fusion Enterprise Software and Hardware Requirements.

Satellite Device Clustering

Satellite device clustering allows you to connect up to ten satellite devices into a single cluster, and connect the satellite device cluster to the aggregation device as a single group instead of as individual satellite devices.

Satellite device clustering is particularly useful in scenarios where optical cabling options between buildings are limited and in scenarios where you want to preserve optical interfaces for other purposes. If you have, for instance, two buildings that have limited optical interfaces between each other and you want to put an aggregation device in one building and ten satellite devices in the other building, you can group the ten satellite devices into a cluster and connect the cluster to the aggregation device with a single cable.

See "Understanding Satellite Device Clustering in a Junos Fusion" on page 14 for additional information on satellite device clustering.

Cascade Ports

A *cascade port* is a port on an aggregation device that sends and receives control and network traffic from an attached satellite device or satellite device cluster. All traffic passed between a satellite device or cluster and the aggregation device in a Junos Fusion traverses the cascade port.

The link that connects an aggregation device to a satellite device has an interface on each end of the link. The interface on the aggregation device end of the link is a cascade port. The interface on the satellite device end of the link is an uplink port.

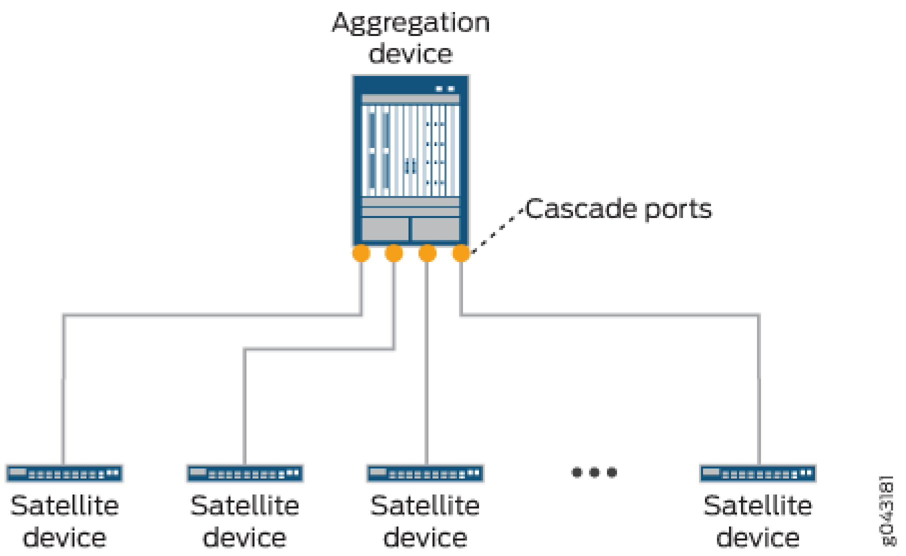
Satellite devices are added to a Junos Fusion by configuring the interface on the aggregation device end of a link into a satellite device.

A cascade port is typically a 10-Gbps interface with an SFP+ transceiver or a 40-Gbps interface with a QSFP+ transceiver, but any interface on the aggregation device that connects to the satellite device can be converted into a cascade port.

NOTE: Direct attach copper (DAC) cable connections cannot be configured as cascade ports.

The location of the cascade ports in a Junos Fusion are illustrated in Figure 5 on page 10.

Figure 5: Cascade Ports



The hardware specifications for cascade ports for a Junos Fusion Enterprise are discussed in greater detail in Understanding Junos Fusion Enterprise Software and Hardware Requirements.

Uplink Ports

An *uplink port* is a physical interface on a satellite device that provides a connection to an aggregation device. All network and control traffic on a satellite device that is transported to an aggregation device is sent or received on the satellite device's uplink port.

The link that connects an aggregation device to a satellite device has an interface on each end of the link. The interface on the aggregation device end of the link is a cascade port. The interface on the satellite device end of the link is an uplink port. Uplink ports are automatically created when a cascade port is configured on the aggregation device end of the link.

Each satellite device model (EX4300, EX2300, EX3400 and QFX5100) has a set of default uplink ports that the device uses to connect to the aggregation device and, in the case of a satellite device cluster, to other satellite devices. The set of uplink (and clustering) ports may be overridden by configuring an uplink port policy for the device. The uplink port policy must include at least one default uplink port. See "Configuring Uplink Port Policies on a Junos Fusion" on page 93 for more information on uplink port policies.

An uplink port is typically a 10-Gbps SFP+ interface or a 40-Gbps QSFP+ interface, but any 1-Gbps interface that connects a satellite device to an aggregation device can become an uplink port if it is included in an uplink port policy.

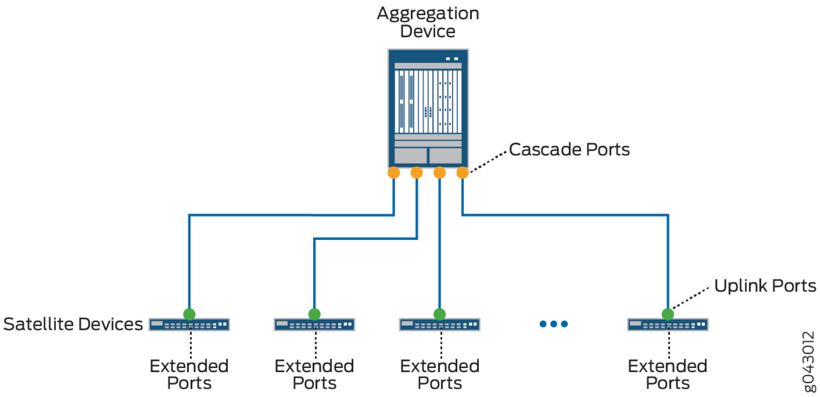
A single satellite device can have multiple uplink port connections to an aggregation device. The multiple uplink port connections to a single aggregation device provide redundancy and additional bandwidth for satellite device to aggregation device connections.

Satellite devices in a Junos Fusion with dual aggregation devices must have at least one uplink port connection to each aggregation device.

In a satellite device cluster, some cluster member satellite devices do not have uplink port connections to the aggregation device. Satellite devices in a satellite device cluster pass traffic to the aggregation device using another cluster member's uplink port.

Figure 6 on page 11 labels the uplink port location in a Junos Fusion Enterprise.

Figure 6: Junos Fusion Enterprise Ports



Extended Ports

An *extended port* is a network-facing port on a satellite device that transmits and receives network traffic for the Junos Fusion.

Network traffic received on an extended port is passed, when appropriate, to the aggregation device over the uplink port to cascade port link.

Each network-facing port on a satellite device in a Junos Fusion is also an extended port. A single cascade port is associated with multiple extended ports.

Figure 6 on page 11 labels the extended ports location in a Junos Fusion Enterprise.

Clustering Ports

Clustering ports are interfaces that interconnect satellite devices in the same satellite device cluster.

See "Understanding Satellite Device Clustering in a Junos Fusion" on page 14 for more information on clustering ports.

Understanding FPC Identifiers and Assignment in a Junos Fusion

In a Junos Fusion, each satellite device—including each member satellite device in a satellite device cluster—must have a Flexible PIC Concentrator identifier (FPC ID).

The FPC ID is in the range of 65-254, and is used for Junos Fusion configuration, monitoring, and maintenance. Interface names—which are identified using the *type*-*fpc* / *pic* / *port* format—use the FPC ID as the *fpc* variable when the satellite device is participating in a Junos Fusion. For instance, built-in port 2 on PIC 0 of a satellite device—a Gigabit Ethernet interface on a satellite device that is using 101 as its FPC ID— uses **ge-101/0/2** as its interface name.

A Junos Fusion provides two methods of assigning an FPC identifier:

- Unique ID-based FPC identification
- Connectivity-based FPC identification

In unique ID-based FPC identification, the FPC ID is mapped to the serial number or MAC address of the satellite device. For instance, if a satellite device whose serial number was **ABCDEFGHIJKL** was assigned to FPC ID 110 using unique ID-based FPC identification, the satellite device with the serial number **ABCDEFGHIJKL** will always be associated with FPC ID 110 in the Junos Fusion. If the satellite device with the serial number **ABCDEFGHIJKL** connects to the aggregation device using a different cascade port, the FPC ID for the satellite device remains 110.

In connectivity-based FPC identification, the FPC ID is mapped to the cascade port. For instance, connectivity-based FPC identification can be used to assign FPC ID 120 to the satellite device that connects to the aggregation device using cascade port **xe-0/0/2**. If the existing satellite device that connects to cascade port **xe-0/0/2** is replaced by a new satellite device, the new satellite device connected to the cascade port assumes FPC ID 120.

Unique ID-based FPC identification is configured using the *serial-number* or *system-id* statement in the [edit chassis *satellite-management fpc slot-id*] hierarchy.

Connectivity-based FPC identification is configured using the *cascade-ports* statement in the [edit chassis *satellite-management fpc slot-id*] hierarchy.

FPC ID configurations must be identical between aggregation devices in a Junos Fusion Enterprise with two aggregation devices. A satellite device that has two FPC IDs because of mismatched aggregation device configurations goes offline until the configuration issue is fixed.

If a prospective satellite device is connected to a Junos Fusion without having a configured FPC slot ID, the prospective satellite device does not participate in the Junos Fusion until an FPC ID is associated with it. The **show chassis satellite unprovision** output includes a list of satellite devices that are not participating in a Junos Fusion because of an FPC ID association issue.

Understanding Software in a Junos Fusion Enterprise

In a Junos Fusion, the aggregation device is responsible for all configuration and management within the Junos Fusion and runs Junos OS software.

The satellite devices, meanwhile, run satellite software that has the built-in intelligence to extend features on the Junos OS software onto the satellite device.

The role of Junos OS and satellite software is discussed in greater detail in "Understanding Software in a Junos Fusion Enterprise" on page 24.

You can see software version compatibility information for any Junos Fusion Enterprise using the Junos Fusion Hardware and Software Compatibility Matrices.

The software specifications for a Junos Fusion Enterprise are discussed in greater detail in Understanding Junos Fusion Enterprise Software and Hardware Requirements.

Understanding Interface Naming in a Junos Fusion

Network interfaces in Junos OS are specified as follows:

- *type*-*fpc* / *pic* / *port*

In a Junos Fusion, the interface names on the satellite devices follow this naming convention, where:

- The *type* does not change for the interface when it becomes part of a Junos Fusion. The *type* for a 10-Gbps interface, for instance, remains `xe` regardless of whether the interface is or is not in a Junos Fusion.

  You will see internally created `sd` interfaces in a Junos Fusion. The `sd` interfaces map to uplink ports and are used internally by the Junos Fusion to process some types of traffic.

- The *fpc* identifier in a Junos Fusion, which is user-configurable, is the FPC slot identifier. See " Understanding FPC Identifiers and Assignment in a Junos Fusion" on page 12.

  For instance, built-in port 2 on PIC 0—a Gigabit Ethernet interface that is acting as an extended port —on the satellite device numbered as FPC slot 101 would be identified as:

  ge-101/0/2

Understanding Feature Configuration in a Junos Fusion Enterprise

In a Junos Fusion, the aggregation device is responsible for all configuration and management within the Junos Fusion and runs Junos OS software.

In a Junos Fusion with one aggregation device, all configuration—whether it's a command that enables a feature globally or enables a feature on a specific extended port—is done on the lone aggregation device.

In a Junos Fusion with two aggregation devices, the configuration of any command must match between aggregation devices. If a command is enabled differently on the aggregation devices, the command might be implemented in an unpredictable manner or may not be implemented at all.

A Junos Fusion Enterprise with dual aggregation devices is an MC-LAG topology. MC-LAG topologies support commitment synchronization, a feature that allows users to configure commands on one device within a group and then share that group with other devices. In a Junos Fusion Enterprise with dual aggregation devices, commitment synchronization can be used to ensure identical configuration between aggregation devices by sharing configuration between aggregation devices.

See "Understanding Configuration Synchronization in a Junos Fusion" on page 27.

RELATED DOCUMENTATION

Configuring or Expanding a Junos Fusion Enterprise | 49

Network Configuration Example: Enabling Junos Fusion Enterprise on an Enterprise Campus Network

Junos Fusion Hardware and Software Compatibility Matrices

Understanding Satellite Device Clustering in a Junos Fusion

IN THIS SECTION

This topic describes satellite device clustering in a Junos Fusion. It covers:

Satellite Device Clustering Overview

Satellite device clustering allows you to connect up to ten satellite devices into a single cluster, then connect the satellite device cluster to the aggregation device as a single group instead of as individual satellite devices.

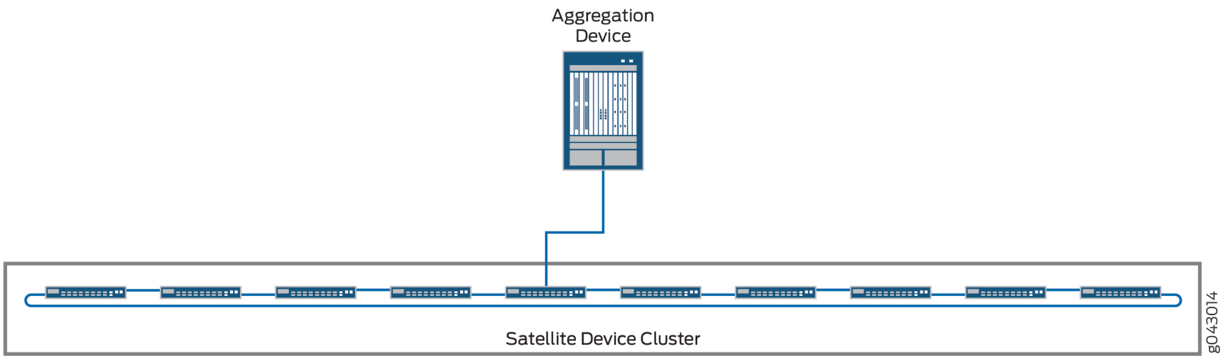
Satellite device clustering is particularly useful in scenarios where optical cabling options between buildings are limited and in scenarios where you want to preserve optical interfaces for other purposes. If you have, for instance, two buildings that have limited optical interfaces between each other and you want to put an aggregation device in one building and ten satellite devices in the other building, you can group the ten satellite devices into a cluster and connect the cluster to the aggregation device with a single cable.

Satellite Device Cluster Topology

A satellite device cluster must be cabled into a ring topology. No other cabling topologies are supported for a satellite device cluster.

Figure 7 on page 16 shows a picture of a sample satellite device cluster connected to a single aggregation device.

Figure 7: Satellite Device Cluster Topology



Satellite Device Cluster Names and Identifiers

In a Junos Fusion, each satellite device cluster is named and assigned a number. The number is called the *cluster identifier*, or *cluster ID*.

The cluster name and ID are used by the aggregation device to identify a cluster for configuration, monitoring, and troubleshooting purposes.

The cluster name and ID are set using the **set chassis satellite-management cluster *cluster-name* cluster-id *cluster-id-number*** statement.

Satellite Device Cluster Uplink Interfaces

A satellite device cluster must have at least one member with an uplink interface connection to the aggregation device.

In a dual aggregation device topology using satellite device clustering, each satellite device cluster must have at least one uplink interface connection to both aggregation devices. The uplink interfaces to the aggregation devices can be on any member satellite devices in each satellite device cluster.

NOTE: Junos Fusion Provider Edge supports only one aggregation device.

A satellite device cluster supports multiple uplink interfaces. The uplink interfaces can be on any satellite devices that are members of the satellite device cluster. The advantages of configuring multiple uplink interfaces for a satellite device cluster is resiliency—all traffic can be forwarded to another uplink interface if an uplink interface fails—and efficiency—multiple uplink interfaces can reduce the number of hops that traffic takes across a cluster before it is forwarded to an aggregation device.

Cluster Interfaces

Clustering ports are interfaces that interconnect satellite devices in the same satellite device cluster.

Traffic originating from an access device connected to an extended port travels over cluster interfaces to get to an uplink port. Traffic from an aggregation device travels to a satellite device uplink port then over cluster interfaces before it is delivered to an access device connected to an extended port.

Cluster interfaces are typically 10-Gbps SFP+ interfaces. 10-Gbps SFP+ and 40-Gbps QSFP+ interfaces can be used as cluster interfaces. Other interfaces cannot be used as cluster interfaces by default. To use other interfaces as cluster interfaces, you must configure a candidate uplink port policy. See Configuring Uplink Port Policies on a Junos Fusion for additional information on candidate uplink port policies.

NOTE: DAC cables are not supported on cluster interfaces.

Satellite Device Cluster Software Management

All satellite devices in a satellite device cluster are associated with a single satellite software upgrade group, which is automatically created when a satellite device cluster is configured as part of a Junos Fusion. The satellite software upgrade group is named after the satellite device cluster name, and ensures that all satellite devices in the cluster run the same version of satellite software.

See Understanding Software in a Junos Fusion Enterprise for additional information on software management for a satellite device cluster.

See Understanding Junos Fusion Enterprise Software and Hardware Requirements for information on software requirements for satellite devices in a satellite device cluster.

FPC Identifiers and Extended Port Interfaces in a Satellite Device Cluster

Each satellite device in a satellite device cluster has a unique *FPC* identifier (FPC ID), in the same way that a satellite device that is not part of a cluster has a unique FPC ID.

For this reason, all interface naming for satellite device cluster member switches is not impacted by cluster membership. If a switch is assigned FPC ID 103, for instance, the aggregation device views the satellite device as FPC 103 regardless of whether it is or is not part of a satellite device cluster.

The FPC ID is used in the FPC slot name for an extended port interface; for instance, ge-103/0/2. An extended port is any network-facing interface on a satellite device. As with FPC ID naming, extended port interface names are not impacted by satellite device cluster membership status.

NOTE: Satellite devices in a cluster are configured using the unique ID-based FPC identification method of FPC identifier assignment. For more information, see *Understanding FPC Identifiers and Assignment in a Junos Fusion* in Understanding Junos Fusion Enterprise Components.

Understanding 40-Gbps Interfaces with QSFP+ Transceiver Roles for Satellite Devices in a Satellite Device Cluster

40-Gbps QSFP+ interfaces on satellite devices in a satellite device cluster can be used as clustering ports to cable to other satellite devices in the cluster or as uplink ports to cable the satellite device cluster to the aggregation device.

40-Gbps QSFP+ interfaces on EX2300, EX3400, EX4300 and QFX5100 satellite devices are default uplink ports. Please see Table 1 on page 18for the default uplink ports for satellite devices. When these devices are part of a satellite device cluster, the default uplink ports cannot be configured as extended ports to pass network traffic unless they have a direct connection to the aggregation device or if there is an uplink port policy configured that excludes them from acting as uplink ports.

Table 1: Default Uplink Interfaces for Junos Fusion Enterprise Satellite Devices

Device Type	Default Uplink Interfaces
EX2300 (4 ports on PIC1)	1/0 through 1/3
EX3400 (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-24P (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-24T (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-32F (4 ports on PIC 0, 2 ports on PIC 1 and 8 ports on PIC 2)	0/32 through 0/35 1/0 through 1/1 2/0 through 2/7
EX4300-48P (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3

Table 1: Default Uplink Interfaces for Junos Fusion Enterprise Satellite Devices *(Continued)*

Device Type	Default Uplink Interfaces
EX4300-48T (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-48T-BF (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-48T-DC (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
EX4300-48T-DC-BF (4 ports each on PIC1 and PIC2)	1/0 through 1/3 and 2/0 through 2/3
QFX5100-48S-6Q (6 QSFP+ ports)	0/48 through 0/53
QFX5100-48T-6Q (6 QSFP+ ports)	0/48 through 0/53

RELATED DOCUMENTATION

Configuring or Expanding a Junos Fusion Enterprise

Understanding Junos Fusion Enterprise Components

Configuring Uplink Port Policies on a Junos Fusion

Understanding Junos Fusion Ports

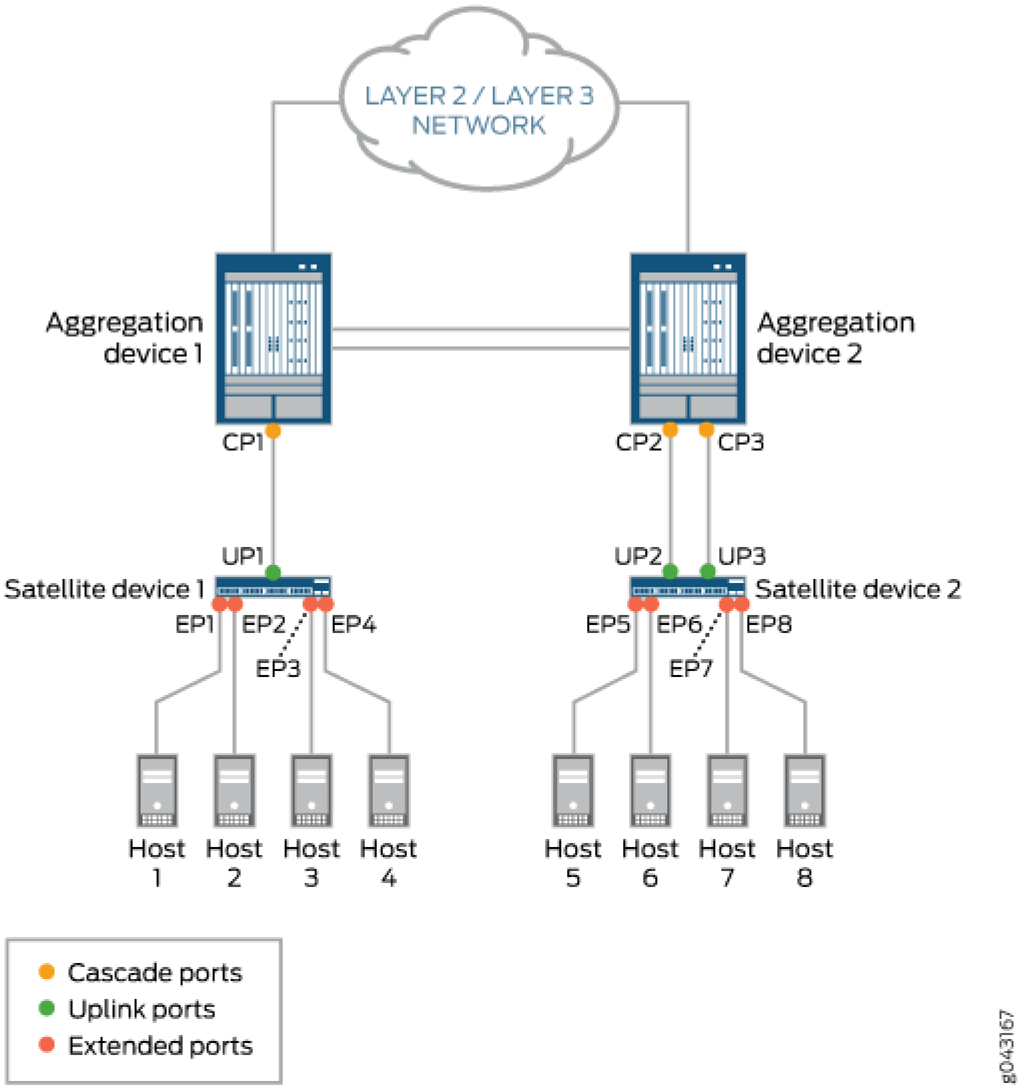
IN THIS SECTION

In a Junos Fusion topology, cascade, uplink, and extended ports are components that play key roles. Figure 8 on page 21 shows a sample Junos Fusion topology, which serves as a point of reference for this discussion of cascade, uplink, and extended ports.

In the Junos Fusion topology shown in Figure 8 on page 21, two aggregation devices and two satellite devices are deployed. The aggregation devices are connected to each other through a multichassis link aggregation group (MC-LAG). Each satellite device has a single-homed connection to its respective aggregation device through one or two links.

On the aggregation devices in each illustration, each link is connected to a cascade port (for example, CP1 on Aggregation device 1), while on the satellite devices, each link is connected to an uplink port (for example, UP1 on Satellite device 1). Hosts 1 through 4 are connected to Satellite device 1 through extended ports EP1 through EP4, and so on.

Figure 8: Cascade, Uplink, and Extended Ports in a Junos Fusion Topology With Two Aggregation Devices and MC-LAG



This topic provides the following information:

Understanding Cascade Ports

A *cascade port* is a physical interface on an aggregation device that provides a connection to a satellite device. A cascade port on an aggregation device connects to an uplink port on a satellite device.

On an aggregation device, you can set up one or more cascade port connections with a satellite device. For example, in the Junos Fusion topology shown in Figure 8 on page 21, Aggregation device 1 has one cascade port connection (CP1) to Satellite device 1, and Aggregation device 2 has two cascade port connections (CP2 and CP3) to Satellite device 2.

When there are multiple cascade port connections to a satellite device, as shown in Figure 8 on page 21, the traffic handled by the ports is automatically load-balanced. For a packet destined for a satellite device, the cascade port over which to forward the packet is chosen based on a per-packet hash that is computed using key fields in the packet. To select the key fields to be used, you can specify the `hash-key` statement in the `[edit forwarding-options]` hierarchy or the `enhanced-hash-key` statement in the `[edit forwarding-options]`, `[edit logical-systems` *`logical-system-name`* `routing-instances` *`instance-name`* `forwarding-options]`, and `[edit routing-instances` *`instance-name`* `forwarding-options]` hierarchies.

NOTE: The 802.1BR tag is not included in the load-balancing hash computation for cascade ports.

In addition, a cascade port can handle the traffic for all extended ports on a particular satellite device. However, you cannot specify that a particular cascade port handle the traffic for a particular extended port.

After you configure an interface as a cascade port (for example, by issuing `set interfaces xe-0/0/1 cascade-port`), you cannot configure the interface as a Layer 2 interface (for example, by issuing `set interfaces xe-0/0/1 unit 0 family bridge`) or a Layer 3 interface (for example, `set interfaces xe-0/0/1 unit 0 family inet`). If you try to configure a cascade port as a Layer 2 or Layer 3 interface, you receive an error message.

On a cascade port, you can configure class-of-service (CoS) policies.

Understanding Uplink Ports

An *uplink port* is a physical interface on a satellite device that provides a connection to an aggregation device. An uplink port on a satellite device connects to a cascade port on an aggregation device.

After a cascade port is configured on the aggregation device end of a link, a corresponding uplink port is automatically created on the satellite device. From the aggregation device, you can monitor port and queue statistics for uplink ports. However, we do not recommend that you configure Layer 2 or Layer 3 forwarding features on uplink ports.

On a satellite device, you can set up one or more uplink port connections to an aggregation device. For example, in the Junos Fusion topology shown in Figure 8 on page 21, Satellite device 1 has one uplink port (UP1) to Aggregation device 1, and Satellite device 2 has two uplink ports (UP2 and UP3) to Aggregation device 2.

When a satellite device has multiple uplink ports to an aggregation device, the traffic from the extended ports is automatically load-balanced among the uplink ports. For example, in the Junos Fusion topology shown in Figure 8 on page 21, the traffic from extended ports EP5 through EP8 is load balanced between uplink ports UP2 and UP3 to reach Aggregation device 2. In this situation, each packet is examined, and if an IPv4 or IPv6 header is found, a load-balancing algorithm chooses the uplink port based on the header (source and destination IP addresses, and source and destination TCP/UDP ports). If an IPv4 or IPv6 header is not found, the load-balancing algorithm chooses the uplink port based on the Layer 2 header (destination and source MAC addresses, Ethertype, and outer VLAN ID) of the packet.

Understanding Extended Ports

An *extended port* is a physical interface on a satellite device that provides a connection to servers or endpoints. To an aggregation device, a satellite device appears as an additional Flexible PIC Concentrator (FPC) and the extended ports on the satellite device appear as additional interfaces to be managed by the aggregation device.

On aggregation devices, you can configure extended ports by using the same Junos OS CLI and naming convention used for Junos OS interfaces on standalone routers and switches. The only difference is that when you specify an extended port name, the FPC slot number must be in the range of 100 through 254 in Junos OS Release 14.2 and in the range of 65 through 254 in Junos OS Release 16.1 and later.

For example, for the four extended ports shown on Satellite device 1 in Figure 8 on page 21, the FPC slot number could be 100, the PIC slot number could be 0, the first extended port could be 1, the second extended port could be 2, the third extended port could be 3, and the fourth extended port could be 4. The complete 10-Gigabit Ethernet extended port names could be as follows:

xe-100/0/1

xe-100/0/2

xe-100/0/3

xe-100/0/4

You can configure the following features on extended ports:

- Layer 2 bridging protocols
- Integrated routing and bridging (IRB)
- Firewall filters
- CoS policies

RELATED DOCUMENTATION

Understanding the Flow of Data Packets in a Junos Fusion Topology | 41

hash-key

enhanced-hash-key

Understanding Software in a Junos Fusion Enterprise

IN THIS SECTION

This topic discusses the role of software in a Junos Fusion Enterprise. It covers:

Understanding Junos OS for the Aggregation Device in a Junos Fusion

An aggregation device in a Junos Fusion always runs Junos OS software and is responsible for almost all management tasks, including configuring all network-facing ports—the *extended ports*—on all satellite devices in the Junos Fusion. The extended ports in a Junos Fusion, therefore, typically support features that are supported by the version of Junos OS running on the aggregation device.

An aggregation device in a Junos Fusion runs the same Junos OS software regardless of whether it is or is not part of a Junos Fusion. Hence, Junos OS software is acquired, installed, and managed on an aggregation device in a Junos Fusion in the same manner that it is acquired, installed, and managed on a standalone device that is not part of a Junos Fusion.

Understanding Satellite Software for the Satellite Devices in a Junos Fusion

The satellite devices in a Junos Fusion run satellite software that has the built-in intelligence to extend features on the Junos OS software onto the satellite device. The satellite software is a Linux-based operating system that allows the satellite devices to communicate with the aggregation device for control plane data while also passing network traffic.

All satellite devices in a Junos Fusion must run satellite software that is compatible with the Junos OS software running on the aggregation device. See Junos Fusion Hardware and Software Compatibility Matrices for software compatibility requirements and links to the satellite software.

You can run the same version of satellite software on satellite devices that are different hardware platforms. For instance, if your Junos Fusion included EX2300 and EX4300 switches as satellite devices, the EX2300 and EX4300 switches acting as satellite devices could install the satellite software from the same satellite software package.

You can download satellite software from the software center for any satellite device. See the Junos Fusion Hardware and Software Compatibility Matrices, which provides software requirements as well as links to satellite device and Junos OS software. Additionally, you have the option to order some switches with the satellite software preinstalled from the factory.

The satellite software packages are stored on the aggregation device after a satellite software package installation—which is typically managed from the aggregation device—has been executed. The satellite software packages remain in the file system even if the Junos OS on the aggregation device is upgraded. The satellite software on a satellite device can be updated individually or, more commonly, using satellite software upgrade-groups, which are discussed in more detail in this document.

A device cannot simultaneously run Junos OS and the satellite software. If you remove a satellite device from a Junos Fusion, you have to install the Junos OS onto the device before you can use it in your network as a standalone Junos switch.

Satellite software is sometimes referred to as satellite network operating system (SNOS) software in the command-line interface and in other documentation.

The satellite software requirements for a Junos Fusion Enterprise are discussed in Understanding Junos Fusion Enterprise Software and Hardware Requirements.

Understanding Satellite Software Upgrade Groups

A *satellite software upgrade group* is a group of satellite devices that are designated to upgrade to the same satellite software version. One Junos Fusion can contain multiple software upgrade groups, and multiple software upgrade groups should be configured in most Junos Fusions to avoid network downtimes during satellite software installations.

When a satellite device is added to a Junos Fusion, the aggregation device checks if the satellite device is using an FPC ID that is included in a satellite software upgrade group. If the satellite device is using an FPC ID that is part of a satellite software upgrade group, the device upgrades its satellite software to the version of software associated with the satellite software upgrade group - unless it is already running the defined version.

When the satellite software package associated with an existing satellite software group is changed, the satellite software for all member satellite devices is upgraded using a throttled upgrade. The throttled upgrade ensures that the aggregation device is not overwhelmed with providing satellite software simultaneously to many satellite devices.

When satellite devices of a satellite device cluster are upgraded, members of the same satellite device cluster download the software to be used and install the software at the same time as other members of the cluster. This ensures that cluster members run the same version of software as each other in case there are incompatibilities between satellite software versions.

The two most common methods of installing satellite software onto a Junos switch—autoconverting a device into a satellite device when it is cabled into an aggregation device and manually converting a device that is cabled into an aggregation device into a satellite device—require the presence of a configured satellite software upgrade group.

Software upgrade groups are configured and managed on the aggregation device.

Understanding Satellite Software Requirements for a Satellite Device Cluster

All satellite devices in a satellite device cluster are associated with a single satellite software upgrade group, which is automatically created when a satellite device cluster is configured as part of a Junos Fusion. The satellite software upgrade group uses the same name as the satellite device cluster name, and ensures that all satellite devices in the cluster run the same version of satellite software.

The automatically created software upgrade group for the satellite device cluster is managed like any other software upgrade group.

Understanding Satellite Software Requirements in a Dual Aggregation Device Topology

In a Junos Fusion with dual aggregation devices, you must ensure that only one version of satellite software is associated with each satellite software upgrade group.

When configuring a Junos Fusion into a dual aggregation topology, do one of the following to ensure satellite software is properly maintained:

- Configure all satellite software upgrade groups on one of the aggregation devices.
- Configure the exact same satellite software upgrade group—a satellite software upgrade group with the same name and same FPC ID associations—on both aggregation devices.

If there is a mismatch between satellite software upgrade group membership or satellite software version for a satellite software upgrade group, satellite software is not upgraded on any satellite devices in the upgrade group until the configuration and version association is addressed.

Understanding the Platform Specific Satellite Software Image

The platform specific satellite software package is required to install satellite software onto an EX2300, EX3400 or EX4300 switch that is not connected to an aggregation device. Use the platform specific satellite software package when you want to manually install satellite software on a switch using the **request chassis device-mode satellite** ***URL-to-satellite-software*** command before you interconnect that switch into a Junos Fusion Enterprise.

> **NOTE**: Platform specific satellite software is not required for QFX5100 switches.

You can identify the platform specific satellite software by looking for the satellite-ppc prefix in the satellite software image name; for example, satellite-ppc-3.0R1.1-signed.tgz. To find the image that is compatible with your satellite device, please refer to Junos Fusion Hardware and Software Compatibility Matrices.

RELATED DOCUMENTATION

Junos Fusion Hardware and Software Compatibility Matrices

Understanding Junos Fusion Enterprise Software and Hardware Requirements | **28**

Configuring or Expanding a Junos Fusion Enterprise | **49**

Understanding Configuration Synchronization in a Junos Fusion

All configuration and management for a Junos Fusion are done from the aggregation devices. which run Junos OS software.

In a Junos Fusion with one aggregation device, all configuration—whether it's a configuration statement that enables a feature globally or enables a feature on a specific extended port—is done from the lone aggregation device.

A Junos Fusion with multiple aggregation devices often requires that the configuration of a feature—for example, an extended port, and entities such as routing instances and VLANs that include the extended port—must match on all aggregation devices. If a configuration statement for the feature—in this case, the extended port—is specified differently on one aggregation device, the statement on that particular aggregation device might be implemented in an unpredictable manner or might not be implemented at all.

Junos Fusion supports configuration synchronization, a feature that allows users to specify configuration statements within a group on one aggregation device and then share that group with other aggregation devices.

We strongly recommend using configuration synchronization to configure software features in multiple aggregation device topologies. Configuration synchronization ensures configuration consistency by sharing the exact same configuration between aggregation devices. Configuration synchronization also simplifies administration of a Junos Fusion by allowing users to enter configuration statements once in a configuration group and apply the configuration group to all aggregation devices rather than repeating a configuration procedure manually on each aggregation device.

For more information about configuration synchronization, see "Enabling Configuration Synchronization Between Aggregation Devices in a Junos Fusion" on page 88, Understanding MC-LAG Configuration Synchronization, and Synchronizing and Committing MC-LAG Configurations.

See Enabling Junos Fusion Enterprise on an Enterprise Campus Network for a sample Junos Fusion Enterprise topology configured largely using configuration synchronization.

RELATED DOCUMENTATION

Enabling Configuration Synchronization Between Aggregation Devices in a Junos Fusion | 88

Understanding Junos Fusion Enterprise Software and Hardware Requirements

IN THIS SECTION

This topic describes the software and hardware requirements for a Junos Fusion Enterprise. For Junos Fusion Provider Edge software and hardware requirements, see Understanding Junos Fusion Provider Edge Software and Hardware Requirements. For Junos Fusion Data Center software and hardware requirements, see Understanding Junos Fusion Data Center Software and Hardware Requirements.

It covers:

Aggregation Device to Satellite Device Software Compatibility

A Junos Fusion Enterprise includes an aggregation device or devices running Junos OS and satellite devices running satellite software. The version of Junos OS running on the aggregation device must be compatible with the satellite software versions running on the satellite device in order for the Junos Fusion Enterprise to function.

See Junos Fusion Hardware and Software Compatibility Matrices for software compatibility information for any Junos Fusion Enterprise.

NOTE: When you upgrade the satellite software version to a release later than the recommend versions listed in the Junos Fusion Hardware and Software Compatibility Matrices, your Junos Fusion system will only benefit from the satellite software fixes. To acquire the full benefits of a satellite software release, including satellite software fixes and new features, we recommend you upgrade both the aggregation device software and its compatible satellite device software for a complete upgrade.

Aggregation Devices

This section details the hardware and software requirements for an aggregation device in a Junos Fusion Enterprise. It covers:

Aggregation Device Hardware Models

Table 2 on page 29 lists the hardware platforms that are supported as aggregation devices for a Junos Fusion Enterprise. It also lists the supported satellite devices for each Junos OS Release supporting Junos Fusion Enterprise.

Table 2: Supported Aggregation Device Hardware and Supported Satellite Devices by Junos OS Release

Aggregation Device Hardware	Supported Satellite Devices by Junos OS Release
EX9204 Switch	16.1R1 (EX4300) 17.1R1 (EX2300, EX3400, EX4300) 17.3R1 (EX2300, EX3400, EX4300, QFX5100) 18.2R1 (EX2300, EX3400, EX4300, QFX5100, EX4600)

Table 2: Supported Aggregation Device Hardware and Supported Satellite Devices by Junos OS Release *(Continued)*

Aggregation Device Hardware	Supported Satellite Devices by Junos OS Release
EX9208 Switch	16.1R1 (EX4300) 17.1R1 (EX2300, EX3400, EX4300) 17.3R1 (EX2300, EX3400, EX4300, QFX5100) 18.2R1 (EX2300, EX3400, EX4300, QFX5100, EX4600)
EX9214 Switch	16.1R1 (EX4300) 17.1R1 (EX2300, EX3400, EX4300) 17.3R1 (EX2300, EX3400, EX4300, QFX5100) 18.2R1 (EX2300, EX3400, EX4300, QFX5100, EX4600)
EX9251 Switch	18.1R1 (EX2300, EX3400, EX4300, QFX5100) 18.2R1 (EX2300, EX3400, EX4300, QFX5100, EX4600)
EX9253 Switch	18.2R1 (EX2300, EX3400, EX4300, QFX5100, EX4600)

NOTE: Tunable optics SFPs are not supported for wavelength tuning on QFX5110 satellite devices.

Maximum Number of Aggregation Devices

A Junos Fusion Enterprise supports one or two aggregation devices.

Cascade Ports

A *cascade port* is a port on an aggregation device that sends and receives control and network traffic from an attached satellite device.

Table 3 on page 31 provides a list of line cards on an EX9200 switch that have interfaces that can be converted into cascade ports, and the initial Junos OS release that introduced cascade port support for interfaces on the line card.

Direct attach copper (DAC) cable connections cannot be configured as cascade ports.

BEST PRACTICE: A cascade port is typically a 10-Gbps interface with an SFP+ transceiver or a 40-Gbps interface with a QSFP+ transceiver, although other interfaces on the aggregation device can be converted into a cascade port.

Table 3: Line Cards on EX9200 Switch Cascade Port Support

Line Card	Switch Model	Initial Junos OS Release
EX9200-6QS (6-port 40-Gigabit Ethernet QSFP+, 24-port 10-Gigabit Ethernet SFP+ line card)	EX9204	16.1R1
	EX9208	16.1R1
	EX9214	16.1R1
EX9200-32XS (32-port SFP+ line card)	EX9204	16.1R1
	EX9208	16.1R1
	EX9214	16.1R1
EX9200-40T (40-port 10/100/1000BASE-T RJ-45 line card)	EX9204	16.1R1
	EX9208	16.1R1
	EX9214	16.1R1
EX9200-MPC (modular line card) The following MICs are supported: • EX9200-10XS-MIC • EX9200-20F-MIC	EX9204	17.1R1
	EX9208	17.1R1

Table 3: Line Cards on EX9200 Switch Cascade Port Support *(Continued)*

Line Card	Switch Model	Initial Junos OS Release
- EX9200-40T-MIC	EX9214	17.1R1
EX9200-40F (40-port 100FX/1000BASE-X SFP line card)	EX9204	17.4R1
	EX9208	17.4R1
	EX9214	17.4R1
EX9200-40F-M (40-port 100FX/1000BASE-X SFP line card with MACsec)	EX9204	17.4R1
	EX9208	17.4R1
	EX9214	17.4R1
EX9200-40XS (40-port 10GbE SFP+ line card with MACsec)	EX9204	17.4R1
	EX9208	17.4R1
	EX9214	17.4R1
EX9200-12QS (12-port 10GbE/40GbE QSFP+ or 4-port 100GbE QSFP28 combo line card) **NOTE**: All ports can operate at 10-Gbps and 40-Gbps speeds. The ports are configured to operate at 10-Gbps speed by default.	EX9204	17.4R1
	EX9208	17.4R1
	EX9214	17.4R1

Table 3: Line Cards on EX9200 Switch Cascade Port Support *(Continued)*

Line Card	Switch Model	Initial Junos OS Release
EX9253-6Q12C (12-port QSFP28 40GbE/100GbE and 6-port QSFP+ 40GbE line card)	EX9253	18.2R1
EX9253-6Q12C-M (12-port QSFP28 40GbE/100GbE and 6-port QSFP+ 40GbE line card with MACsec)	EX9253	18.2R1

Satellite Devices

This section details the hardware and software requirements for satellite devices in a Junos Fusion Enterprise. It covers:

Satellite Device Hardware Models

Table 4 on page 33 lists the EX2300 switches that are supported as satellite devices for a Junos Fusion Enterprise.

To convert an EX2300 switch from Junos OS to satellite software, the switch must be running Junos OS Release 15.1X53-D55 or later.

To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

Table 4: Supported EX2300 Satellite Device Hardware and Initial Junos OS Release

Hardware	Initial Junos OS Release
EX2300-C-12P	15.1X53-D55
EX2300-C-12T	15.1X53-D55

Table 4: Supported EX2300 Satellite Device Hardware and Initial Junos OS Release *(Continued)*

Hardware	Initial Junos OS Release
EX2300-24P	15.1X53-D55
EX2300-24T	15.1X53-D55
EX2300-24T-DC	15.1X53-D55
EX2300-48P	15.1X53-D55
EX2300-48T	15.1X53-D55

Table 5 on page 34 lists the EX3400 hardware platforms that are supported as satellite devices for a Junos Fusion Enterprise.

To convert an EX3400 switch from Junos OS to satellite software, the switch must be running Junos OS Release 15.1X53-D55 or later.

To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

Table 5: Supported EX3400 Satellite Device Hardware and Initial Junos OS Release

Hardware	Initial Junos OS Release
EX3400-24P	15.1X53-D55
EX3400-24T	15.1X53-D55
EX3400-24T-DC	15.1X53-D55
EX3400-48P	15.1X53-D55
EX3400-48T	15.1X53-D55

Table 5: Supported EX3400 Satellite Device Hardware and Initial Junos OS Release *(Continued)*

Hardware	Initial Junos OS Release
EX3400-48T-AFI	15.1X53-D55

Table 6 on page 35 lists the EX4300 hardware platforms that are supported as satellite devices for a Junos Fusion Enterprise.

To convert an EX4300 switch from Junos OS to satellite software, the switch must be running Junos OS Release 14.1X53-D43 or later.

To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

Table 6: Supported EX4300 Satellite Device Hardware and Initial Junos OS Release

Hardware	Initial Junos OS Release
EX4300-24P	14.1X53-D43
EX4300-24T	14.1X53-D43
EX4300-32F	14.1X53-D43
EX4300-48P	14.1X53-D43
EX4300-48T	14.1X53-D43
EX4300-48T-BF	14.1X53-D43
EX4300-48T-DC	14.1X53-D43
EX4300-48T-DC-BF	14.1X53-D43

Table 7 on page 36 lists the QFX5100 hardware platforms that are supported as satellite devices for a Junos Fusion Enterprise.

To convert a QFX5100 switch from Junos OS to satellite software, the switch must be running Junos OS Release 14.1X53-D43 or later.

To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

Table 7: Supported QFX5100 Satellite Device Hardware and Initial Junos OS Release

Hardware	Initial Junos OS Release
QFX5100-48S-6Q	14.1X53-D43
QFX5100-48T-6Q	14.1X53-D43

Table 8 on page 36 lists the EX4600 hardware platforms that are supported as satellite devices for a Junos Fusion Enterprise.

To convert an EX4600 switch from Junos OS to satellite software, the switch must be running Junos OS Release 14.1X53-D47 or later.

To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

NOTE: The EX4600-EM-8F and QFX-EM-4Q expansion modules are not supported in a Junos Fusion Enterprise.

Table 8: Supported EX4600 Satellite Device Hardware and Initial Junos OS Release

Hardware	Initial Junos OS Release
EX4600-40F	14.1X53-D47

Satellite Device Firmware Requirements

Table 9 on page 37 lists the firmware requirements for satellite devices for a Junos Fusion Enterprise.

Table 9: Minimum Satellite Device Firmware Version Requirements

Satellite Device	Minimum U-boot Release	Minimum Loader Version	Minimum PoE Firmware
EX2300	1.3.2	NA	1.6.1.1.9
EX3400	1.3.0	NA	1.6.1.1.9
EX4300	NA	NA	2.6.3.9.2.1
EX4600	NA	NA	NA
QFX5100	NA	NA	NA

Satellite Device Software Requirements for Satellite Device Clustering

A standalone switch must be running the required satellite software before it can be added to a Junos Fusion Enterprise as a member of a satellite device cluster. A standalone switch running any version of satellite software below the minimum required version for that switch is not recognized by the aggregation device and cannot be added to a Junos Fusion Enterprise as a member of a satellite device cluster. To find the required satellite software version, see Junos Fusion Hardware and Software Compatibility Matrices.

If your switch is running a version of satellite or Junos OS software below the required minimum and you want to include the switch in a satellite device cluster, follow one of these procedures:

- if your switch is already cabled into a Junos Fusion and is able to upgrade to a version of satellite software that supports satellite device clustering, upgrade the satellite software on the switch before adding it to the satellite device cluster. See "Configuring or Expanding a Junos Fusion Enterprise" on page 49.

- If your switch is not cabled into a Junos Fusion, install a version of Junos OS that supports satellite device clustering using the procedure outlined in "Installing Junos OS Software on a Standalone Device Running Satellite Software" on page 128 before installing the switch into the satellite device cluster.

  Once the switch is running a version of Junos OS that supports satellite device clustering, you can install the required satellite software version manually or as part of the satellite software installation that occurs as part of the procedure for adding a satellite device to a Junos Fusion Enterprise.

Satellite Software to Junos OS Conversion Requirements

A satellite device can be removed from a Junos Fusion Enterprise and reinserted into a network as a switch running Junos OS. See Removing a Satellite Device from a Junos Fusion.

A device running satellite software must be converted to a version of Junos OS that supports satellite device conversion. The minimum Junos OS versions that support satellite device conversion are provided in this document.

The following list provides additional information for converting each type of switch from satellite software to Junos OS.

- EX2300 and EX3400 switches:
  - EX2300 and EX3400 switches must be converted to Junos OS Release 15.1X53-D55 or later.
  - EX2300 and EX3400 switches cannot be converted from satellite software to Junos from an aggregation device. To convert the satellite software, remove the satellite device from the Junos Fusion Enterprise and perform the upgrade manually. See Installing Junos OS Software on a Standalone Device Running Satellite Software
  - The target Junos OS image must be a signed version of Junos OS. The text string *-signed* text must be n the Junos OS image filename when the image is downloaded from the Software Center.
- EX4300 switches:
  - EX4300 switches must be converted to Junos OS Release 14.1X53-D43 or later.
  - The target Junos OS image must be a signed version of Junos OS. The text string *-signed* text must be n the Junos OS image filename when the image is downloaded.
- QFX5100 switches:
  - The QFX5100 switch must be converted to Junos OS Release 14.1X53-D43 or later.
  - The target Junos OS image must be a Preboot eXecution Environment (PXE) version of Junos OS. The PXE version of Junos OS includes *pxe* in the package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named *install-media-pxe-qfx-5-14.1X53-D43.3-domestic-signed.tgz*.
  - The target Junos OS image must be a signed version of Junos OS. The text string *-signed* text must be n the Junos OS image filename when the image is downloaded.
- EX4600 switches:
  - The EX4600 switch must be converted to Junos OS Release 14.1X53-D47 or later.

- The target Junos OS image must be a Preboot eXecution Environment (PXE) version of Junos OS. The PXE version of Junos OS includes *pxe* in the package name when it is downloaded from the Software Center—for example, *install-media-pxe-qfx-5-14.1X53-D47.<version>-domestic-signed.tgz*.

- The target Junos OS image must be a signed version of Junos OS. The text string *-signed* text must be n the Junos OS image filename when the image is downloaded.

Power over Ethernet Requirements for a Satellite Device

A satellite device must be running Power over Ethernet (PoE) controller software version as specified in Table 9 on page 37.

To check the PoE controller software version, enter the `show chassis firmware detail` command and view the `PoE firmware` output.

For information on checking and upgrading the PoE controller software, see *Upgrading the PoE Controller Software*.

NOTE: PoE is not supported for QFX5100 satellite devices.

Maximum Number of Satellite Devices or Extended Ports

A Junos Fusion Enterprise supports up to 128 satellite devices or 6,000 extended port access interfaces.

RELATED DOCUMENTATION

Junos Fusion Hardware and Software Compatibility Matrices

Configuring or Expanding a Junos Fusion Enterprise | 49

Understanding ICCP in a Junos Fusion using Dual Aggregation Devices

IN THIS SECTION

This topic describes the Inter-Chassis Control Protocol (ICCP) in a Junos Fusion. It covers:

ICCP in a Junos Fusion Overview

Inter-Chassis Control Protocol (ICCP) is used in MC-LAG topologies to exchange control information between the devices in the topology. See Multichassis Link Aggregation Features, Terms, and Best Practices for additional information on ICCP.

A Junos Fusion with two aggregation devices is an MC-LAG topology, and is therefore always running ICCP as the control protocol. A Junos Fusion using a single aggregation device is not an MC-LAG topology and does not run ICCP.

A dedicated ICCP link is highly recommended in a Junos Fusion deployment, but is not required. ICCP traffic is transmitted across the ICL when an ICCP link is not configured. An ICCP link can be one link or an aggregated ethernet interface. In most Junos Fusion deployments, we recommend using a 40-Gbps link or an aggregated ethernet interface as the ICCP link.

Automatic ICCP Provisioning

Junos Fusion supports automatic ICCP provisioning, which automatically configures ICCP in a dual aggregation device setup without any user action. Automatic ICCP provisioning is enabled by default and is often the preferred method of enabling ICCP for a Junos Fusion in greenfield deployments that are not being integrated into an existing network. If you are installing your Junos Fusion in an environment that doesn’t have to integrate into an existing campus network, you can usually ignore manual ICCP configuration processes and allow automatic ICCP provisioning to enable ICCP.

Many Junos Fusion installations occur in brownfield deployments and the Junos Fusion has to be integrated into an existing network. Brownfield deployments often have a need to maintain existing ICCP settings, in particular in scenarios where a Junos Fusion is replacing an MC-LAG topology or is supporting a network that includes other MC-LAG topologies. ICCP must be configured manually in these scenarios.

See Enabling Junos Fusion Enterprise on an Enterprise Campus Network for an example of a Junos Fusion Enterprise deployment that manually configures ICCP.

RELATED DOCUMENTATION

Multichassis Link Aggregation Features, Terms, and Best Practices

Configuring or Expanding a Junos Fusion Enterprise | 49

Understanding the Flow of Data Packets in a Junos Fusion Topology

All Ethernet data packets that are exchanged between aggregation devices and satellite devices in a Junos Fusion topology include an E-channel tag (ETAG) header that carries an E-channel identifier (ECID) value. The ECID value, which is assigned by the aggregation device, identifies the source or destination extended port on one of the connected satellite devices.

In a sample Junos Fusion topology, where an aggregation device is connected to two satellite devices, the following Layer 2 unicast data packet flow scenarios can occur:

- Scenario 1—A host on one satellite device sends a packet to another host on the same satellite device. For example, Host 2 sends a unicast packet to Host 4. Both hosts are connected to Satellite device 1. (See Figure 9 on page 42.)

- Scenario 2—A host on one satellite device sends a packet to another host on the other satellite device. For example, Host 2, which is connected to Satellite device 1, sends a unicast packet to Host 7, which is connected to Satellite device 2. (See Figure 10 on page 43.).

Figure 9: Layer 2 Unicast Data Packet Flow Through a Junos Fusion Topology—Scenario 1

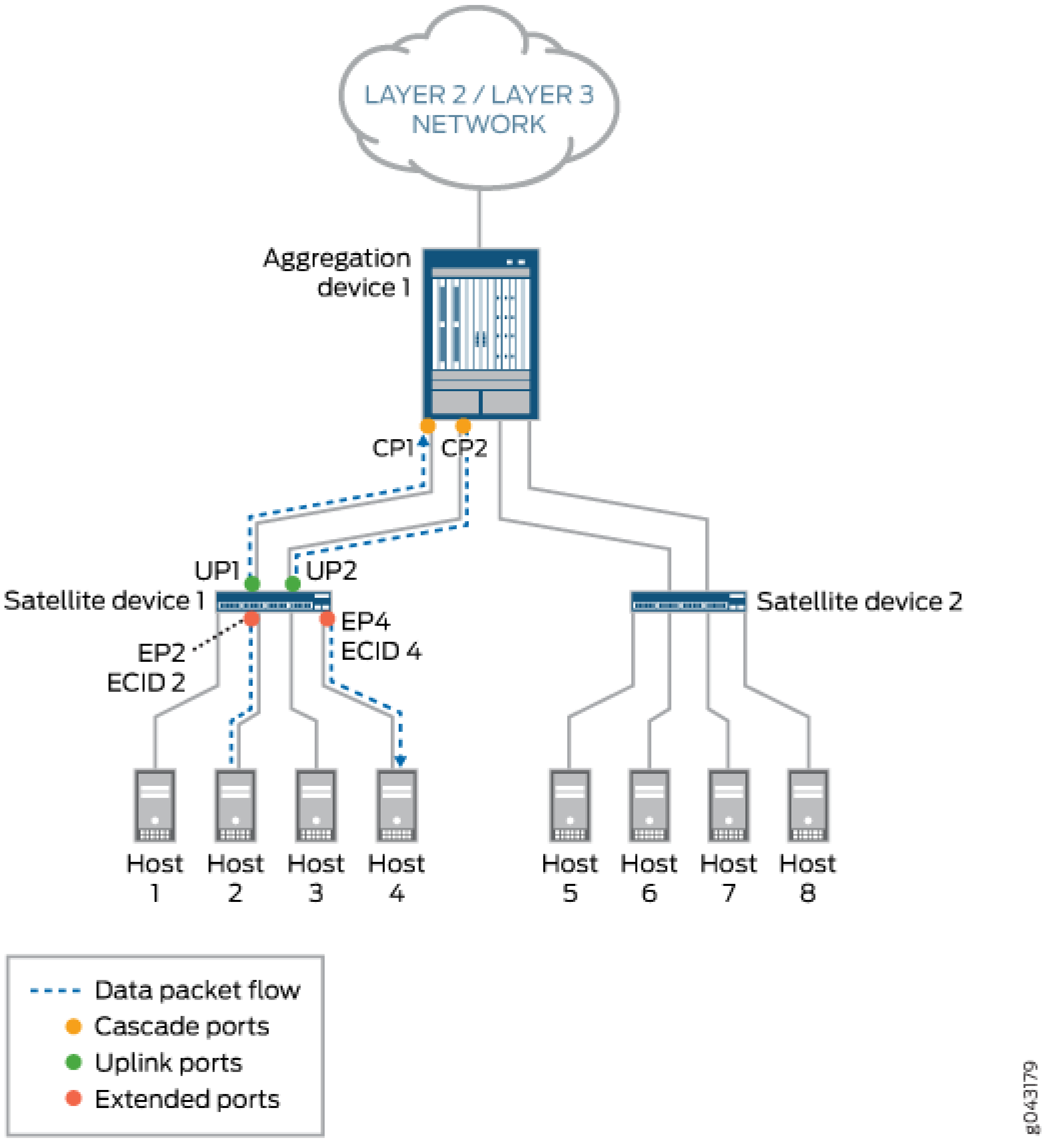
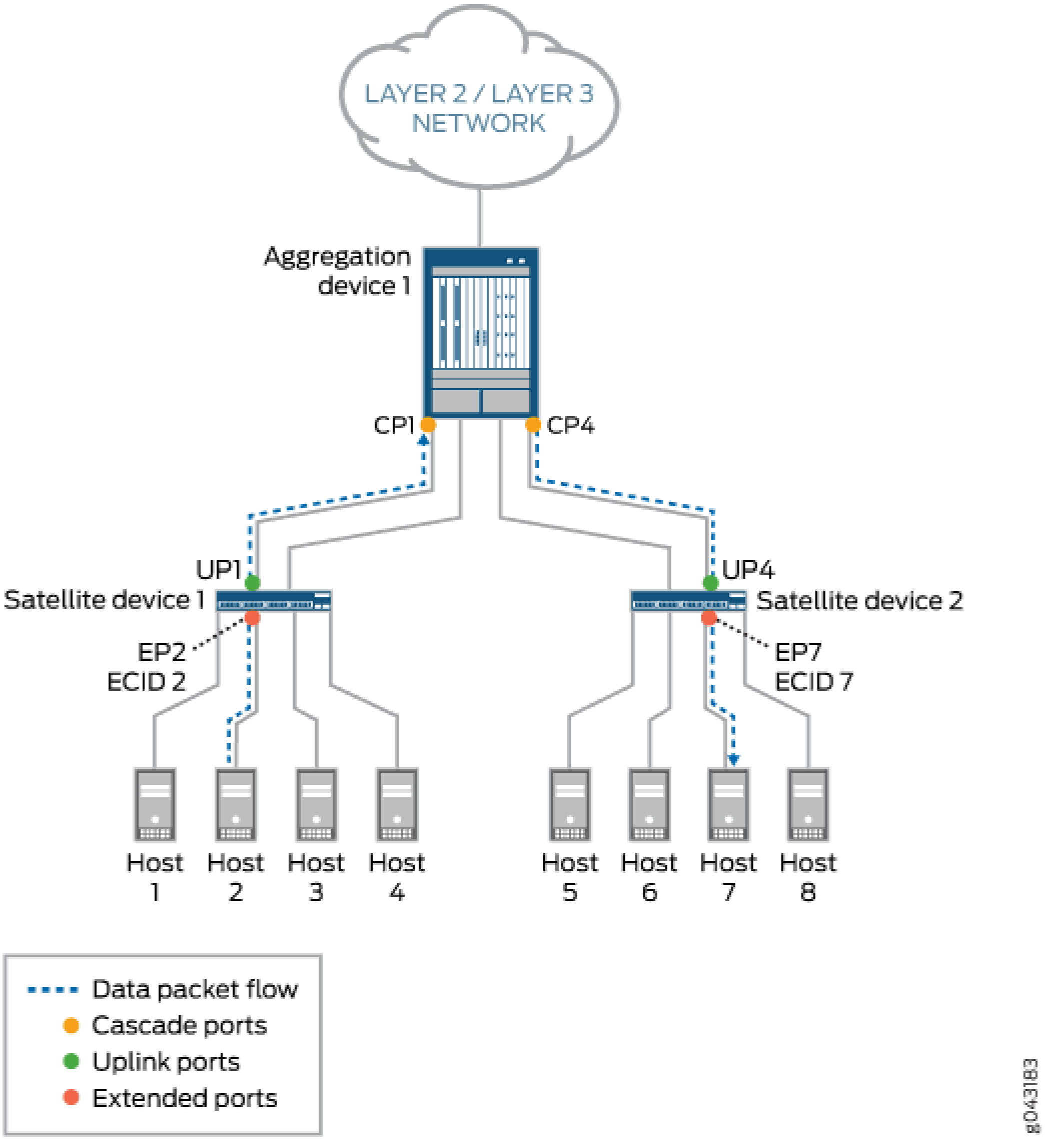


Figure 10: Layer 2 Unicast Data Packet Flow Through a Junos Fusion Topology—Scenario 2



In scenario 1, where Host 2 sends a unicast data packet to Host 4, the following events occur:

> **NOTE**: Only the events that are performed by Junos Fusion components are listed. Events handled by components that are not specific to the Junos Fusion topology are excluded.

1. Extended port EP2 on Satellite device 1 receives the packet from Host 2.

2. Satellite device 1 inserts an ETAG header in the packet. The ETAG header carries the ECID value (ECID 2), which is assigned by Aggregation device 1 to extended port EP2.

3. On Satellite device 1, two uplink ports (UP1 and UP2) are connected to Aggregation device 1. As a result, traffic between the devices can be load-balanced. In this case, uplink port UP1 is chosen to forward the packet to cascade port CP1 on Aggregation device 1.

4. On receiving the packet, Aggregation device 1 extracts the ECID value (ECID 2) from the ETAG header of the packet and learns that the packet is from extended port EP2 on Satellite device 1. Aggregation device 1 then removes the ETAG header from the packet.

5. Aggregation device 1 performs a lookup for Host 4. The result of the lookup is extended port EP4 on Satellite device 1.

6. On Aggregation device 1, two cascade ports (CP1 and CP2) are connected to Satellite device 1. As a result, traffic between the devices can be load-balanced. In this case, cascade port CP2 is chosen to forward the packet to uplink port UP2 on Satellite device 1.

7. The packet is forwarded to cascade port CP2, where a new ETAG header and ECID value (ECID 4), which is assigned by Aggregation device 1 to extended port EP4, is added.

8. The packet is received by uplink port UP2 on Satellite device 1.

9. Satellite device 1 extracts the ECID value (ECID 4) from the ETAG header of the packet, then maps ECID 4 to extended port EP4.

10. Host 4 receives the packet from extended port EP4.

In scenario 2, where Host 2 sends a unicast data packet to Host 7, the events that occur are the same as for scenario 1 except for the following:

- Event 5—Aggregation device 1 performs a lookup for Host 7. The result of the lookup is extended port EP7 on Satellite device 2.

- Event 6—On Aggregation device 1, two cascade ports (CP3 and CP4) are connected to Satellite device 2. As a result, traffic between the devices can be load-balanced. In this case, cascade port CP4 is chosen to forward the packet to uplink port UP4 on Satellite device 2.

- Event 7—The packet is forwarded to cascade port CP4, where a new ETAG header and ECID value (ECID 7), which is assigned by Aggregation device 1 to extended port EP7, is added.

- Event 8—The packet is received by uplink port UP4 on Satellite device 2.

- Event 9—Satellite device 2 extracts the ECID value (ECID 7) from the ETAG header of the packet, and then maps ECID 7 to extended port EP7.

- Event 10—Host 7 receives the packet from extended port EP7.

RELATED DOCUMENTATION

Understanding Junos Fusion Provider Edge Components

Understanding Junos Fusion Enterprise Components

Understanding Satellite Policies in a Junos Fusion

IN THIS SECTION

Satellite Policies Overview

Satellite policies are used in a Junos Fusion to define how certain features are configured for standalone satellite devices within a Junos Fusion. Satellite policies can be used to configure standalone satellite devices or all satellite devices in a satellite device cluster.

Environment monitoring of the satellite devices, uplink failure detection for satellite device uplink ports, and remapping uplinks—with port pinning, uplink selection, and local port mirroring—are configured using satellite policies.

Satellite policies are configured as independent policies on the aggregation device, and then associated with the Junos Fusion configuration.

Understanding Environment Monitoring Satellite Policies

You can configure an environment monitoring satellite policy in a Junos Fusion to configure how a Junos Fusion responds to link-down alarms on satellite devices.

In the environment monitoring satellite policy, you define how you want a link-down alarm from a satellite device to be handled by the Junos Fusion. The Junos Fusion can treat the link-down alarm as a yellow or red alarm, or it can be configured to ignore the alarm.

The environment monitoring policy provides the flexibility to define different alarm handling based on user preference. You can, for instance, assign environment monitoring policies to individual satellite devices based on FPC ID. You can also configure environment monitoring policies based on the product model of the satellite devices, if desired. You can, for instance, specify that all link-down alarms from

EX4300 switches acting as satellite devices are treated as yellow alarms, while all link-down alarms from QFX5100 switches acting as satellite devices are treated as red alarms.

Environment monitoring satellite policies are configured using the *environment-monitoring-policy* statement in the `[edit policy-options satellite-policies]` hierarchy level.

An environment monitoring policy is applied for a single satellite device in a Junos Fusion using the `environment-monitoring-policy` statement in the [edit chassis *satellite-management*] or the [edit chassis *satellite-management fpc slot-id*] hierarchy levels.

You can configure a different environment monitoring policy for a single satellite device in the **fpc *slot-id*** when an environment monitoring policy for all satellite devices is configured. The environment monitoring policy for the FPC is enabled in cases when both an individual and global environment monitoring policy is configured.

RELATED DOCUMENTATION

Configuring Junos Fusion Provider Edge

Configuring or Expanding a Junos Fusion Enterprise

Understanding Multicast Forwarding on a Junos Fusion Enterprise

IN THIS SECTION

Starting with Junos OS Release 17.1R1, multicast traffic forwarding is supported in Junos Fusion Enterprise. Multicast forwarding is supported only on the aggregation device (AD).

Overview of Multicast Forwarding

The AD performs ingress multicast replication to a set of extended ports. On the satellite device, multicast traffic is received for each of the extended ports. The following scenarios are supported for both IPv4 and IPv6 traffic:

- Layer 2 multicast with VLAN flooding—IGMP snooping and the Multicast Learner Discovery (MLD) protocol are configured on the AD to forward multicast traffic
- Layer 3 multicast—IGMP and PIM are configured on the AD to forward multicast traffic. Only versions 2 and 3 of IGMP are supported.

Configuring Layer 2 Multicast Forwarding in a Junos Fusion Enterprise

To configure Layer 2 multicast forwarding in a Junos Fusion Enterprise, configure IGMP snooping and MLD snooping on each VLAN. The following example shows the basic configuration required. Virtual router instances with integrated routing and bridging (IRB) interfaces are also supported.

```
protocols {
    igmp-snooping {
        vlan team-a {
            interface ge-101/0/0.0 {
                multicast-router-interface;
            }
            interface ge-101/0/1.0 {
                static {
                    group 233.252.0.1;
                }
            }
        }
        vlan team-b;
    }
}
```

Configuring Layer 3 Multicast Forwarding in a Junos Fusion Enterprise

To configure Layer 3 multicast forwarding in a Junos Fusion Enterprise, enable PIM and IGMP. The following example shows the basic configuration required. Note that an IRB interface are also required as the multicast traffic is forwarded through IRB interfaces.

```
protocols {
    igmp {
        accounting;
        interface all;
        interface irb.40 {
            version 2;
        }
        interface irb.50 {
            static {
                group 233.252.0.1;
            }
        }
    }
    pim {
        rp {
            auto-rp discovery;
            static {
                address 192.0.2.1;
            }
        }
        interface all {
            mode sparse;
        }
    }
}
```

RELATED DOCUMENTATION

Junos Fusion Enterprise Overview | 2

CHAPTER 2

Junos Fusion Enterprise Configuration

IN THIS CHAPTER

Configuring or Expanding a Junos Fusion Enterprise

IN THIS SECTION

This topic provides the instructions needed to configure a Junos Fusion Enterprise—a Junos Fusion using EX9200 switches as aggregation devices—and to add satellite devices or an aggregation device to an existing Junos Fusion Enterprise. It covers:

Preparing the Aggregation Devices

Ensure your aggregation devices are running a version of Junos OS software that is compatible with Junos Fusion Enterprise. Junos Fusion Enterprise support was introduced for EX9200 switches in Junos OS Release 16.1R1. See Junos Fusion Hardware and Software Compatibility Matrices to learn more about Junos OS software compatibility requirements and to obtain Junos OS and satellite software for your Junos Fusion Enterprise. See "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28 for additional information on Junos Fusion Enterprise hardware and software requirements.

If the aggregation device does not have the correct version of Junos OS installed, upgrade the Junos OS on both Routing Engines on your aggregation device.

> **NOTE**: If your aggregation device is part of an existing Junos Fusion Enterprise installation with satellite device clusters that is running Junos OS Release 16.1 and you wish to upgrade to Junos OS Release 17.1 or later, please refer to the upgrade instructions in the 17.1R1 release notes.

The following procedure shows one method of upgrading Junos OS software. The instructions assume that you know the basics of Junos OS image file management and have already acquired the target Junos OS image. The target Junos OS image can be obtained using the Junos Fusion Hardware and Software Compatibility Matrices. This upgrade procedure causes avoidable system downtime.

The number of Junos OS software upgrade options available for EX9200 switches is beyond the scope of this document. For information on Junos OS software installation options for EX9200 switches, see the Software Installation and Upgrade Guide.

To upgrade Junos OS software, enter the following commands on the aggregation device:

```
user@aggregation-device> request system software add aggregation-device-package-name re0
```

```
user@aggregation-device> request system software add aggregation-device-package-name re1
```

After performing the upgrade, reboot both Routing Engines to complete the software upgrade.

```
user@aggregation-device> request system reboot both-routing-engines
```

Preparing a Switch Running Junos OS to Become a Satellite Device

Use this procedure to prepare all switches running Junos OS software to become satellite devices. This procedure must be performed on all satellite devices, regardless of whether the satellite device will be converted into a standalone satellite device or be part of a satellite device cluster.

This section can be skipped if your satellite device or all satellite devices in your satellite device cluster are already running satellite software.

NOTE: The following conditions must be met before a Junos switch that is running Junos OS Release 17.1R1 can be converted to a satellite device when the action is initiated from the aggregation device:

- The Junos switch can only be converted to SNOS 3.0 and higher.
- The Junos switch must be either set to factory default configuration, or the following command must be included in the configuration: `set chassis satellite-management auto-satellite-conversion`.

To prepare a switch running Junos OS software to become a satellite device:

1. Log into the device that will become a satellite device through the console port.
2. Ensure the device is running a version of Junos OS that allows it to be converted into a satellite device. See Junos Fusion Hardware and Software Compatibility Matrices and "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28 for information on minimum Junos OS requirements for satellite devices.

   NOTE: In case of difficulty moving to the required versions of U-boot and JLOADER, please contact the Juniper Networks Technical Assistance Center.

   If you need to upgrade Junos OS on your satellite device before proceeding, see the Junos Fusion Hardware and Software Compatibility Matrices to obtain the software. Upgrade Junos OS before converting your switch into a satellite device.
3. (Satellite devices providing interfaces for PoE only) If you plan on using the satellite device interfaces to provide PoE, check the satellite device’s PoE firmware version:

   - Enter the **show chassis firmware detail** command to learn the PoE firmware version running on the device.

     ```
     user@sd1-ex4300> show chassis firmware detail
     FPC 0
        Boot SYSPLD             10
     ```

```
    PoE firmware            2.6.3.92.1
(additional output omitted)
```

- The satellite device must have the following minimum PoE versions to support PoE in a Junos Fusion Enterprise.

  Table 10: Minimum PoE Firmware Versions

Satellite Device Platform	Minimum PoE Firmware Version
EX2300	1.6.1.1.9
EX3400	1.6.1.1.9
EX4300	2.6.3.92.1
QFX5100	No minimum version requirement

  See Minimum Satellite Device Firmware Version Requirements table for additional information on firmware version requirements for devices in a Junos Fusion Enterprise.

- If your device meets the minimum PoE firmware requirement, proceed to the next step.

  If a PoE firmware update is required, upgrade the PoE firmware. See Upgrading the PoE Controller Software.

4. Zeroize the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for zeroizing the device.

If you are not logged into the device using the console port connection, your connection to the device is lost after entering the **request system zeroize** command.

If you lose your connection to the device, log in using the console port.

5. (EX3400 and EX4300 switch uplink ports only) After the reboot is complete, convert the built-in 40-Gbps interfaces with QSFP+ transceivers from Virtual Chassis ports (VCPs) into network ports:

   ```
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
   ```

   For example, to convert all four built-in 40-Gbps interfaces with QSFP+ transceivers on an EX4300-24P switch into network ports:

   ```
   user@satellite-device>request virtual-chassis vc-port delete pic-slot 1 port 0
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
   ```

   The number of built-in 40-Gbps interfaces with QSFP+ transceivers varies by switch model. See the hardware documentation for your switch.

   This step is required for the 40-Gbps interfaces with QSFP+ transceivers that will be used as uplink interfaces to directly connect to the aggregation device in a Junos Fusion Enterprise, because zeroizing the devices restores the default settings and 40-Gbps interfaces with QSFP+ transceivers on EX3400 and EX4300 switches are configured into VCPs by default. VCPs cannot be used as uplink ports to connect to aggregation devices in a Junos Fusion.

6. Commit the configuration.

   ```
   user@satellite-device# commit
   ```

Configuring the FPC Slot IDs, Cascade Ports, and Satellite Device Clusters on the Junos Fusion

IN THIS SECTION

Use this procedure to configure FPC slot IDs, cascade ports, and satellite device clusters.

For more information on FPC slot IDs, cascade ports, and satellite device clusters, see "Understanding Junos Fusion Enterprise Components" on page 5.

This section provides separate instructions for configuring FPC slot IDs and cascade ports for standalone satellite devices and satellite devices in a satellite device cluster. A Junos Fusion Enterprise can and often does support standalone satellite devices and satellite device clusters in the same Junos Fusion topology.

This section covers the following procedures:

Configuring the FPC Slot ID and Cascade Ports for a Standalone Satellite Device

Use this procedure to configure the FPC slot IDs and cascade ports for standalone satellite devices, which are satellite devices that are not part of a satellite device cluster:

1. Configure the cascade ports, and commit the configuration.

   A cascade port is a port on an aggregation device that connects to a satellite device or a satellite device cluster. Data and control traffic is passed between the aggregation device and the satellite devices over the cascade port link.

   To configure a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces interface-name cascade-port
   ```

   where *interface-name* in the cascade port interface on the aggregation device.

   For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces xe-0/0/1 cascade-port
   ```

   Commit the configuration on both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   or onto a single Routing Engine:

   ```
   [edit]
   user@aggregation-device# commit
   ```

2. Configure the FPC slot ID number of each satellite device.

   In a Junos Fusion Enterprise, each satellite device, including each satellite device in a satellite device cluster, must be mapped to an FPC identifier (FPC ID). The FPC ID is in the range of 65 through 255, and it is used for Junos Fusion Enterprise configuration, monitoring, and maintenance. Interface names—which are identified using the *type-fpc* / *pic* / *port* format—use the FPC ID as the *fpc* variable when the satellite device is participating in a Junos Fusion Enterprise.

   You can assign an FPC identifier to the satellite device based on either the satellite device's MAC address, serial number, or cascade port.

   - To map the FPC slot ID to a standalone satellite device's MAC address:

     ```
     [edit]
     user@aggregation-device# set chassis satellite-management fpc slot-id system-id mac-address
     ```

     where *slot-id* becomes the FPC slot ID of the satellite device and *mac-address* is the satellite device's MAC address. The FPC slot ID must be 65 or larger, and it functions as the FPC slot identifier.

     For example, to map FPC slot ID to the satellite device using MAC address 00:00:5E:00:53:00:

     ```
     [edit]
     user@aggregation-device# set chassis satellite-management fpc 110 system-id
     00:00:5E:00:53:00
     ```

     NOTE: To find out the system MAC of the satellite device, use the `show chassis mac-addresses` command on the satellite device.

   - To map the FPC slot ID to a standalone satellite device's serial number:

     ```
     [edit]
     user@aggregation-device# set chassis satellite-management fpc slot-id serial-number serial-
     number
     ```

     where *slot-id* becomes the FPC slot ID of the satellite device and *serial-number* is the satellite device's serial number. The FPC slot ID must be 65 or larger, and it functions as the FPC slot identifier.

For instance, to map FPC slot ID 101 to the satellite device using the serial number ABCDEFGHIJKL:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 serial-number
ABCDEFGHIJKL
```

NOTE: To find out the serial number of the satellite device, use the `show chassis hardware` command on the satellite device.

- To configure the FPC slot ID for a standalone satellite device—a satellite device not part of a satellite device cluster—to a cascade port, enter:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc slot-id cascade-ports
interface-name
```

where *slot-id* becomes the FPC slot ID of the satellite device, and *interface-name* is the name of the interface.

For example, to configure the FPC slot ID of the satellite device that is connected to xe-0/0/1 to 101:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
```

If a prospective satellite device is connected to a Junos Fusion Enterprise without having a configured FPC slot ID, the prospective satellite device does not participate in the Junos Fusion Enterprise until an FPC ID is associated with it. The **show chassis satellite unprovision** output includes a list of satellite devices that are not participating in a Junos Fusion Enterprise because of an FPC ID association issue.

The FPC slot ID configuration must match on both aggregation devices in dual-homed dual aggregation device topologies.

Configuring the FPC Slot ID, Cascade Ports, and Satellite Device Clusters for Satellite Devices in a Satellite Device Cluster

Use this procedure to configure the FPC slot IDs, cascade ports, and satellite device clusters for satellite devices in a satellite device cluster:

1. Configure the cascade ports, and commit the configuration.

   A cascade port is a port on an aggregation device that connects to a satellite device in a satellite device cluster. An aggregation device can have multiple cascade ports connecting to multiple satellite device member switches in the same satellite device cluster. Data and control traffic is passed between the aggregation device and the satellite devices over a cascade port link.

   > **BEST PRACTICE**: Use the `show interfaces` command to confirm your interface is up before configuring it into a cascade port.

   To configure a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces interface-name cascade-port
   ```

   For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces xe-0/0/1 cascade-port
   ```

   Commit the configuration on both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   or onto a single Routing Engine:

   ```
   [edit]
   user@aggregation-device# commit
   ```

2. Create the satellite device clusters, and assign a name and a cluster ID to each satellite device cluster:

   ```
   [edit]
   user@aggregation-device# set chassis satellite-management cluster cluster-name cluster-id
   cluster-id-number
   ```

For instance, to create a satellite device cluster named `building-1` and assign it cluster ID `1`:

```
[edit]
user@aggregation-device# set chassis satellite-management cluster building-1 cluster-id 1
```

The *cluster-name* and *cluster-id-number* specified in this step must match on both aggregation devices in dual aggregation device topologies.

3. Define the cascade ports associated with the satellite device cluster.

   An aggregation device can have multiple cascade port connections to the satellite devices in the satellite device cluster, and it must have at least one cascade port connection to one of the satellite devices in the satellite device cluster.

   For example, to configure interfaces xe-0/0/1 and xe-0/0/2 on the aggregation device into cascade ports connecting to the satellite device cluster named `building-1`:

   ```
   [edit]
   user@aggregation-device# set chassis satellite-management cluster building-1 cascade-ports
   xe-0/0/1
   user@aggregation-device# set chassis satellite-management cluster building-1 cascade-ports
   xe-0/0/2
   ```

   NOTE: This step defines which aggregation device ports will be used as cascade ports with the satellite device cluster only.

   The aggregation device interfaces still must be configured into cascade ports, which is accomplished in step 1 of this procedure.

4. Configure the FPC slot ID number of each satellite device.

   In a Junos Fusion Enterprise, each satellite device, including each satellite device in a satellite device cluster, must be mapped to an FPC identifier (FPC ID). The FPC ID is in the range of 65 through 255, and it is used for Junos Fusion Enterprise configuration, monitoring, and maintenance. Interface names—which are identified using the *type-fpc* / *pic* / *port* format—use the FPC ID as the *fpc* variable when the satellite device is participating in a Junos Fusion Enterprise.

   - To map the FPC slot ID to the MAC address of a satellite device in a satellite device cluster:

NOTE: You must map the FPC slot ID to the satellite device's MAC address when the satellite device is a member of a satellite device cluster.

```
[edit]
user@aggregation-device# set chassis satellite-management cluster cluster-name fpc slot-ID
system-id mac-address
```

where *cluster-name* is the name of the satellite device cluster, *slot-id* becomes the FPC slot ID of the satellite device, and *mac-address* is the satellite device's MAC address. The FPC slot ID must be 65 or larger, and it functions as the FPC slot identifier.

For instance, to map FPC slot ID 101 to the satellite device using MAC address 00:00:5E:00:53:00, FPC slot ID 102 to the satellite device using MAC address 00:00:5E:00:53:01, and FPC slot 103 to the satellite device using MAC address 00:00:5E:00:53:02 in the satellite device cluster named `building-1`:

```
[edit]
user@aggregation-device# set chassis satellite-management cluster building-1 fpc 101
system-id 00:00:5E:00:53:00
user@aggregation-device# set chassis satellite-management cluster building-1 fpc 102
system-id 00:00:5E:00:53:01user@aggregation-device# set chassis satellite-management
cluster building-1 fpc 103 system-id 00:00:5E:00:53:02
```

NOTE: To find out the system MAC of the satellite device, use the `show chassis mac-addresses` command on the satellite device.

5. Assign a member ID to each satellite device in the satellite device cluster:

```
[edit]
user@aggregation-device# set chassis satellite-management cluster cluster-name fpc fpc-slot-
ID member-id member-ID-number
```

For instance, to assign member ID numbers 1,2, and 3 to FPC ID numbers 101, 102, and 103 in the satellite device cluster named `building-1`:

```
[edit]
user@aggregation-device# set chassis satellite-management cluster building-1 fpc 101 member-
```

```
id 1
user@aggregation-device# set chassis satellite-management cluster building-1 fpc 102 member-
id 2
user@aggregation-device# set chassis satellite-management cluster building-1 fpc 103 member-
id 3
```

The member ID assignments for a satellite device cluster must match on both Routing Engines in a dual aggregation device topology.

6. (Dual-homed dual aggregation device topologies only) Repeat this procedure to configure the FPC slot IDs, cascade ports, and satellite device clusters on the other aggregation device.

> **NOTE**: The cluster name, ID and FPC information for each satellite device in the cluster must be the same on both aggregation devices.

Managing Software Upgrade Groups on the Aggregation Device

A satellite software upgrade group is a group of satellite devices that are designated to run the same satellite software version using the same satellite software package. One Junos Fusion Enterprise can contain multiple software upgrade groups, and multiple software upgrade groups should be configured in most Junos Fusion Enterprises to avoid network downtimes during satellite software installations.

When a satellite device is added to a Junos Fusion Enterprise, the aggregation device checks if the satellite device is using an FPC ID that is included in a satellite software upgrade group. If the satellite device is using an FPC ID that is part of a satellite software upgrade group, the device upgrades its satellite software to the version of software associated with the satellite software upgrade group - unless it is already running the defined version.

When the satellite software package associated with an existing satellite software group is changed, the satellite software for all member satellite devices is upgraded using a throttled upgrade. The throttled upgrade ensures that the aggregation device is not overwhelmed with providing satellite software simultaneously to many satellite devices.

The two most common methods for installing satellite software onto a Junos OS device—autoconverting a device into a satellite device when it is cabled into an aggregation device and manually converting a device that is cabled into an aggregation device into a satellite device—require that a satellite software upgrade group is configured.

Software upgrade groups are managed from the aggregation device. All satellite devices in a satellite device cluster are part of the same software upgrade group, and a software upgrade group with the name of the satellite device cluster is automatically created when the satellite device cluster is created.

To manage a software upgrade group:

1. Log into the aggregation device.

2. Download the satellite software onto both aggregation devices (recommended) or onto a remote server.

   The satellite software can be downloaded from the main Junos Fusion software download page:

   Junos Fusion - Download Software

3. (Standalone satellite device only) Create a satellite software upgrade group, and associate the standalone satellite device with the satellite software upgrade group:

   ```
   [edit]
   user@aggregation-device# set chassis satellite-management upgrade-groups upgrade-group-name
   satellite slot-id-number-or-range
   ```

   where *upgrade-group-name* is the name of the upgrade group, and the *slot-id-number-or-range* is the FPC slot ID number or range of numbers, of the satellite devices that are being added to the upgrade group.

   NOTE: If you enter the name of an existing satellite software upgrade group as the *upgrade-group-name*, the specified satellite devices are added to the existing software upgrade group.

   For example, to create a software upgrade group named **group1** that includes all satellite devices numbered 101 through 120:

   ```
   [edit]
   user@aggregation-device# set chassis satellite-management upgrade-groups group1 satellite
   101-120
   ```

   The satellite software upgrade group name and associated FPC slot ID configurations must match on both Routing Engines in a dual-homed dual aggregation device topology.

4. Commit the configuration to both Routing Engines on the aggregation device:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

If you are using an aggregation device with a single Routing Engine or want to commit the configuration to a single Routing Engine only:

```
[edit]
user@aggregation-device# commit
```

The configuration must be committed before associating a satellite software image with the satellite software upgrade group, which is done in Step 5.

5. Associate the satellite software upgrade group with a satellite software image.

   - Satellite device clusters:

     - Associate all satellite devices in the cluster with the automatically-created satellite software upgrade group:

       ```
       user@aggregation-device> request system software add package-name upgrade-group
       upgrade-group-name
       ```

       where *package-name* is the URL to the satellite software package, and *upgrade-group-name* is the name of the satellite device cluster.

       For example, to associate a satellite software image named **satellite-3.0R1.2-signed.tgz** that is currently stored in the **/var/tmp** directory on the aggregation device to the upgrade group named **building1**:

       ```
       user@aggregation-device> request system software add /var/tmp/satellite-3.0R1.2-
       signed.tgz upgrade-group building1
       ```

   - Standalone satellite devices:

     - Associate the satellite device with the previously-configured satellite software upgrade group:

       ```
       user@aggregation-device> request system software add package-name upgrade-group
       upgrade-group-name
       ```

       where *package-name* is the URL to the satellite software package, and *upgrade-group-name* is the name of the upgrade group that was assigned by the user earlier in this procedure.

For example, to associate a satellite software image named **satellite-3.0R1.2-signed.tgz** that is currently stored in the **/var/tmp** directory on the aggregation device to the upgrade group named **group1**:

```
user@aggregation-device> request system software add /var/tmp/satellite-3.0R1.2-
signed.tgz upgrade-group group1
```

Associating a satellite software image to a new satellite software package can trigger a satellite software upgrade. A throttled satellite software upgrade might begin after entering the **request system software add** command to associate a satellite software package with a satellite software upgrade group. A satellite software upgrade might also be triggered when a configuration that uses the satellite software upgrade group is committed.

6. (Dual-homed dual aggregation device topology only) Repeat Steps 1 through 4 using the exact same configuration—including the same *package-name* and *upgrade-group-name*—to configure software upgrade groups on the second aggregation device.

   The software upgrade group configurations must match in dual aggregation topologies for the satellite software upgrade to proceed. If you do not associate the software upgrade group on the second aggregation device with a satellite software version, then the satellite device software upgrade will be managed only by the other aggregation device. If you associate the software upgrade group on the second aggregation with a satellite software version, then the satellite software version must be the same on both aggregation devices.

Configuring the Dual Aggregation Device Topology (Dual Aggregation Device Topologies Only)

Use this procedure to connect and configure a second aggregation device into a Junos Fusion Enterprise topology.

Before you begin:

- Ensure that a Junos Fusion topology has already been configured, and that the topology includes a satellite software upgrade group.

- Ensure that the aggregation devices are already cabled together and that all cabling to all satellite devices has been completed for both aggregation devices. For information on cabling requirements, see "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28.

1. (Required only if aggregation device was previously configured into single home mode) Delete single home configuration mode:

On aggregation device 1 and 2:

```
[edit]
user@aggregation-device# delete chassis satellite-management single-home
```

> **NOTE**: Single home mode is not supported in a dual-aggregated device Junos Fusion Enterprise topology.

2. Create and configure a redundancy group on the first aggregation device.

   A dual aggregation device topology in a Junos Fusion is a multichassis link aggregation group (MC-LAG) that uses the Inter-Chassis Communications Protocol (ICCP) to communicate between the aggregation devices. ICCP is typically used in an MC-LAG to exchange information between MC-LAG peers. The MC-LAG peers in a Junos Fusion dual aggregation topology are the aggregation devices.

   A redundancy group is required to enable ICCP in a Junos Fusion. A Junos Fusion topology supports one redundancy group that includes two member devices—the aggregation devices—while also including a configuration parameter that allows users to specify that the satellite devices or satellite clusters also belong to the redundancy group.

   > **NOTE**: All satellite devices, whether standalone satellites or satellite clusters, must be associated to a redundancy group on both aggregated devices; otherwise, they act as single-homed devices, which are not supported in a dual-aggregation device Junos Fusion Enterprise topology.

   To create and configure the redundancy group on the first aggregation device:

   a. Specify the redundancy group ID number on both aggregation devices. The redundancy group name is created and named as part of this process.

      The redundancy group ID number and name must match on both aggregation devices.

      On aggregation device 1 and 2:

      ```
      [edit chassis satellite-management redundancy-groups]
      user@aggregation-device# set redundancy-group-name  redundancy-group-id  redundancy-group-
      id-number
      ```

For instance, to create a redundancy group named junos-fusion-campus-network that uses redundancy group ID 1 on aggregation device 1:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network redundancy-group-id 1
```

Repeat this procedure on aggregation device 2:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network redundancy-group-id 1
```

b. Define the chassis ID number of the each aggregation device:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set chassis-id chassis-id-number
```

For instance, to assign the aggregation device 1 the chassis ID of 1 for the junos-fusion-campus-network redundancy group:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set chassis-id 1
```

To assign aggregation device 2 the chassis ID of 2 for the junos-fusion-campus-network redundancy group:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set chassis-id 2
```

The chassis ID numbers cannot match and are used to create the ICL that interconnects the aggregation device in the Junos Fusion topology.

c. Define the peer chassis ID number—the chassis ID number of the other aggregation device—and interface to use for the ICL:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set redundancy-group-name  peer-chassis-id peer-chassis-id-number
inter-chassis-link interface-name
```

For instance, to use the xe-0/0/1 interface on aggregation device 1 to create an ICL that connects to aggregation device 2:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network peer-chassis-id 2 inter-chassis-
link xe-0/0/1
```

To complete the configuration by defining the peer chassis ID and interface on aggregation device 2:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network peer-chassis-id 1 inter-chassis-
link xe-0/0/1
```

The ICL is used to pass traffic between the aggregation devices.

d. Define the satellite devices that are part of the redundancy group.

   You can add a standalone satellite device or a satellite device cluster to the redundancy group in this step.

   The satellite devices added to the redundancy group in this step must match on both redundancy groups.

   All satellite devices in the Junos Fusion should be added to the redundancy group in this step.

   - To add standalone satellite devices to the redundancy group:

     ```
     [edit chassis satellite-management redundancy-groups]
     user@aggregation-device# set redundancy-group-name  satellite satellite-device-fpc-IDs
     ```

     For instance, to include satellite devices using FPC IDs 100-140 in the redundancy group:

     ```
     [edit chassis satellite-management redundancy-groups]
     user@aggregation-device# set junos-fusion-campus-network satellite 100-140
     ```

   - To add a satellite device cluster to the redundancy group:

     ```
     [edit chassis satellite-management redundancy-groups]
     user@aggregation-device# set redundancy-group-name  cluster cluster-name
     ```

For instance, to include satellite device cluster **building-1** to the redundancy group:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network cluster building-1
```

Repeat the same configuration steps on the other aggregation device.

For instance:

```
[edit chassis satellite-management redundancy-groups]
user@aggregation-device# set junos-fusion-campus-network satellite 100-140
user@aggregation-device# set junos-fusion-campus-network cluster building-1
```

3. (Recommended) Ensure at least one link besides the ICL is connecting the aggregation devices. This link automatically becomes the ICCP link.

   An ICCP link can be one link or an aggregated ethernet interface. In most Junos Fusion Enterprise deployments, we recommend using a 40-Gbps link or an aggregated ethernet interface as the ICCP link.

   An ICCP link is recommended but is optional because ICCP traffic is transmitted across the ICL when a dedicated ICCP link is not configured.

   ICCP configuration is not required. ICCP is automatically provisioned in a Junos Fusion using dual aggregation devices, by default. User configuration of ICCP is not required and is only recommended for expert users.

   If you configure an ICCP parameter in a Junos Fusion, the user-configured parameter overrides the automatically provisioned parameter for the configured parameter only.

   You can disable automatic ICCP provisioning using the *no-auto-iccp-provisioning* statement.

   If you decide to configure ICCP, you must configure matching configurations on both aggregation devices.

   NOTE: ICCP configuration is beyond the scope of this document. See Getting Started with MC-LAG.

4. Configure ICCP.

   ICCP can be configured in one of the following ways:

   - Automatic ICCP provisioning

Automatic ICCP provisioning automatically configures ICCP in a dual aggregation device setup without any user action. Automatic ICCP provisioning is enabled by default and is often the preferred method of enabling ICCP for a Junos Fusion in greenfield deployments that are not being integrated into an existing network.

No user action is required to configure ICCP if automatic ICCP provisioning is used.

- Manual ICCP configuration.

  Manual ICCP configuration is typically used to integrate a Junos Fusion Enterprise into an existing network or by expert users that want to finely tune ICCP settings.

  Many Junos Fusion Enterprise installations occur in brownfield deployments and the Junos Fusion Enterprise has to be integrated into an existing Enterprise network. Brownfield deployments often have a need to maintain existing ICCP settings, in particular in scenarios where a Junos Fusion Enterprise is replacing an MC-LAG topology or is supporting a network that includes other MC-LAG topologies. ICCP must be configured manually in these scenarios.

  See Getting Started with MC-LAG for the steps and options available to configure ICCP.

  If you configure an ICCP parameter in a Junos Fusion, the user-configured parameter overrides the automatically provisioned parameter for the configured parameter only. You can disable all automatic ICCP provisioning using the *no-auto-iccp-provisioning* statement.

  If you decide to manually configure ICCP, you must configure matching configurations on both aggregation devices.

Installing Satellite Software and Adding Satellite Devices to the Junos Fusion

Use this procedure to install satellite software onto a satellite device. A satellite device is not active in a Junos Fusion until satellite software is installed.

Before you begin:

- Ensure you have prepared your satellite device, as described in the “Preparing a Switch Running Junos OS to Become a Satellite Device” section.

- Ensure that the satellite software package is compatible with the aggregation device software. See *Junos Fusion Hardware and Software Compatibility Matrices* at https://www.juniper.net/support/downloads/solutions/fusion/.

- Ensure the minimum satellite device version requirements are met. For information on requirements, see "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28.

- Complete the other steps in this document—created cascade ports, associated FPC slot IDs with satellite devices, and created the satellite software upgrade groups—to ensure the satellite software can be successfully installed.

To install satellite software onto a satellite device and add it to the Junos Fusion Enterprise.

1. Decide how satellite software will be installed onto the satellite devices:

    - Autoconversion(Recommended)—Satellite software is installed onto satellite device automatically when it is cabled to the aggregation device.

    - Manual conversion—Satellite software is installed when user enters a CLI command from aggregation device to install satellite software.

    - Pre-installation—Satellite software is installed on satellite device before the satellite device is cabled into the Junos Fusion Enterprise.

2. Install the satellite software, or configure how it will be installed:

    - To enable autoconversion for a standalone satellite device or a satellite device in a satellite device cluster, enter the following commands from an aggregation device:

      ```
      [edit]
      user@aggregation-device# set chassis satellite-management auto-satellite-conversion
      satellite slot-id
      user@aggregation-device# commit
      ```

      For example, to automatically convert FPC **101** into a satellite device:

      ```
      [edit]
      user@aggregation-device# set chassis satellite-management auto-satellite-conversion
      satellite 101
      user@aggregation-device# commit
      ```

      In this example, autoconversion installs the satellite software associated with FPC slot 101, which was defined in the satellite software upgrade group configuration.

      The process to install the satellite software onto the satellite device with the specified FPC slot ID does not begin until the configuration is committed.

    - To manually install satellite software onto a satellite device, enter the following command from an aggregation device:

      ```
      user@aggregation-device> request chassis satellite interface interface-name device-mode
      satellite
      ```

      where *interface-name* is one of the following values:

  - standalone satellite device: the *interface-name* is the cascade port interface on the aggregation device.

  - satellite device in satellite device cluster that is directly cabled to the aggregation device: the *interface-name* is the cascade port interface on the aggregation device.

  - satellite device in satellite device cluster that is not directly cabled to an aggregation device: the *interface-name* is a clustering port—a port on a satellite device in a satellite device cluster that interconnects satellite devices—on a satellite device.

  For example, to manually configure the switch that is connecting the satellite device to interface xe-0/0/1 on the aggregation device into a satellite device:

  ```
  user@aggregation-device> request chassis satellite interface xe-0/0/1 device-mode satellite
  ```

  To manually configure a switch connecting to interface xe-101/2/0 on a satellite device in a satellite device cluster into a satellite device:

  ```
  user@aggregation-device> request chassis satellite interface xe-101/2/0 device-mode
  satellite
  ```

- To pre-install software onto a satellite device before connecting it into the Junos Fusion Enterprise:

  a. Copy a version of satellite software onto the satellite device running Junos OS.

     For EX2300, EX3400, and EX4300 switches, you must install a platform specific satellite software image in order to pre-install satellite software. See *Understanding the Platform Specific Satellite Software Image* in "Understanding Software in a Junos Fusion Enterprise" on page 24.

     Satellite software images can be downloaded from the Junos Fusion software download page.

  b. Enter the following command from the satellite device:

     ```
     user@satellite-device> request chassis device-mode satellite URL-to-satellite-software
     ```

For instance, to install the satellite software package **satellite-ppc-3.0R1.2-signed.tgz** stored in the **/var/tmp/** folder on an EX4300 switch:

```
user@satellite-device> request chassis device-mode satellite /var/tmp/satellite-
ppc-3.0R1.2-signed.tgz
```

c. Cable the satellite device directly to the aggregation device or into a satellite device cluster.

> **NOTE**: The satellite device version is compared against the satellite device version associated with the software upgrade group upon insertion into the Junos Fusion. If the satellite device is running a version of satellite software that is different than it's associated satellite software upgrade group, the satellite software upgrade group installs the satellite software associated with the satellite software upgrade group onto the satellite device.

The procedure for adding a satellite device running satellite software into a Junos Fusion is also covered in "Adding a Switch Running Satellite Software to a Junos Fusion Enterprise" on page 85.

RELATED DOCUMENTATION

Junos Fusion Hardware and Software Compatibility Matrices

Understanding Junos Fusion Enterprise Software and Hardware Requirements

Verifying Connectivity, Device States, Satellite Software Versions, and Operations in a Junos Fusion | **107**

Understanding Junos Fusion Enterprise Components | **5**

Understanding Software in a Junos Fusion Enterprise | **24**

Junos Fusion Enterprise Installation Checklist

The checklist in Table 11 on page 72 summarizes the tasks you need to perform when installing a Junos Fusion Enterprise. This checklist should be used with the "Configuring or Expanding a Junos Fusion Enterprise" on page 49 document, which provides detailed step-by-step instructions for configuring a Junos Fusion Enterprise.

NOTE: If your aggregation device is part of an existing Junos Fusion Enterprise installation with satellite device clusters that is running Junos OS Release 16.1 and you want to upgrade to Junos OS Release 17.1 or later, please refer to the upgrade instructions in the Junos OS 17.1R1 Release Notes.

Table 11: Junos Fusion Enterprise Installation Checklist

Task	Additional Information	For More Information	Performed by and Date
Prepare Aggregation Device (Aggregation Devices)			
Install a supported version of Junos OS onto each aggregation device.	EX9200 switches can act as aggregation devices in a Junos Fusion Enterprise when running Junos OS Release 16.1R1 or later.	Junos Fusion main software download page and software support matrix: Junos Fusion - Download Software Junos Fusion Enterprise software requirements: Junos Fusion Hardware and Software Compatibility Matrices EX9200 switch software installation: Software Installation and Upgrade Guide Junos Fusion Enterprise software overview: "Understanding Software in a Junos Fusion Enterprise" on page 24	
Prepare Satellite Devices (Satellite Devices)			

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Ensure each satellite device is running a version of Junos OS that allows it to be converted into a satellite device.	EX2300 and EX3400 switches must be running Junos OS Release 15.1X53-D55 or later to be converted into a satellite device. EX4300 switches must be running Junos OS Release 14.1X53-D43 or later to be converted into a satellite device. QFX5100 switches must be running Junos OS Release 14.1X53-D43 or later to be converted into a satellite device.	Satellite device software requirements: Junos Fusion Hardware and Software Compatibility Matrices Upgrading Junos OS on an EX2300, EX3400, or EX4300 switch: Software Installation and Upgrade Guide Upgrading Junos OS on a QFX5100 switch: Installing Software Packages on QFX Series Devices	
Zeroize each satellite device.	**BEST PRACTICE**: Perform this procedure from the console port. To zeroize a satellite device: `request system zeroize`	Zeroizing a switch: • request system zeroize • *Reverting to the Default Factory Configuration for the EX Series Switch*	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date

(EX3400 and EX4300 switches only) Convert the built-in 40-Gbps interfaces from Virtual Chassis ports (VCPs) to network ports.	The number of built-in 40-Gbps interfaces with QSFP+ transceivers varies by EX4300 switch model.
	To convert four built-in 40-Gbps interfaces with QSFP+ transceivers on an EX4300 switch:
	`request virtual-chassis vc-port delete pic-slot 1 port 0`
	`request virtual-chassis vc-port delete pic-slot 1 port 1`
	`request virtual-chassis vc-port delete pic-slot 1 port 2`
	`request virtual-chassis vc-port delete pic-slot 1 port 3`
		Deleting a VCP:
		request virtual-chassis vc-port	

Configure Cascade Ports and FPC slot IDs (Aggregation Devices)			
Configure cascade ports on the aggregation devices.	A cascade port is a port on the aggregation device that connects to a satellite device. To configure a cascade port: `set interfaces xe-0/0/1 cascade-port`	Cascade port overview: "Understanding Junos Fusion Enterprise Components" on page 5 Cascade port configuration: • "Configuring or Expanding a Junos Fusion Enterprise" on page 49 • *cascade-port*	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
(Satellite device clusters only) Create and number the satellite device clusters. **NOTE**: You can skip this step if you are not using satellite device clusters.	Satellite device clustering allows you to connect up to ten satellite devices into a single cluster, then connect the satellite device cluster to the aggregation device as a single group instead of as individual satellite devices. This configuration must match on both aggregation devices. To create and number a satellite device cluster: `set chassis satellite-management cluster sd-cluster-building1 cluster-id 1`	Satellite device clustering overview: "Understanding Satellite Device Clustering in a Junos Fusion" on page 14 Satellite device clustering configuration: • "Configuring or Expanding a Junos Fusion Enterprise" on page 49 • *cluster-id*	
(Satellite device clusters only) Associate the satellite device clusters with a cascade port.	To associate a cascade port with a satellite device cluster: `set chassis satellite-management cluster sd-cluster-building1 cascade-ports xe-0/0/1`	Satellite device clustering configuration: "Configuring or Expanding a Junos Fusion Enterprise" on page 49	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Configure the FPC slot Identifiers (IDs) using one of the following methods on both aggregation devices: • map FPC slot ID to a satellite device’s MAC address (unique ID-based FPC identification) • map FPC slot ID to a satellite device’s serial number (unique ID-based FPC identification) • map FPC slot ID with a cascade port (connectivity-based FPC identification)	Each satellite device in a Junos Fusion is identified by it’s FPC slot ID. To map an FPC slot ID to a satellite device’s MAC address: • Satellite device in a cluster: **`set chassis satellite-management cluster sd-cluster-building1 fpc 101 system-id 00:00:5E:00:53:01`** **NOTE**: You must map the FPC slot ID to the satellite device’s MAC address when the satellite device is a member of a satellite device cluster. • Standalone satellite device: `[edit]` `user@aggregation-device#` **`set chassis satellite-management fpc 101 system-id 00:00:5E:00:53:01`** To map an FPC slot ID to a satellite device’s serial number:	FPC slot ID overview: "Understanding Junos Fusion Enterprise Components" on page 5 Configuring FPC slot IDs: • "Configuring or Expanding a Junos Fusion Enterprise" on page 49 • *system-id* • *serial-number* • *cascade-ports*	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date

	`set chassis satellite-management fpc 101 serial-number TA0123456789`
	To map an FPC slot ID to a cascade port:
	`set chassis satellite-management fpc 101 cascade-ports xe-0/0/1`		

(Satellite device clusters only) Assign a member ID to each satellite device in a satellite device cluster.	To assign a member ID to a satellite device in a satellite device cluster: `set chassis satellite-management cluster sd-cluster-building1 fpc 101 member-id 1` Satellite device cluster member ID configuration must match on both aggregation devices.	Satellite device clustering overview: "Understanding Satellite Device Clustering in a Junos Fusion" on page 14 Satellite device cluster member ID configuration: • "Configuring or Expanding a Junos Fusion Enterprise" on page 49 • *member-id*	
Satellite Software Upgrade Group (Aggregation Devices)			
Acquire the satellite software image and place it on the aggregation devices (recommended) or on a remote server.	The satellite software image is used to install satellite software onto satellite devices.	Junos Fusion main software download page: Junos Fusion - Download Software	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Manage the satellite software upgrade groups. - (satellite devices that are part of a satellite device cluster) associate the satellite devices in a cluster with a satellite software image. - (standalone satellite devices) create the satellite software upgrade group and include the satellite device in it.	A satellite software upgrade group is used to upgrade the satellite software of all satellite devices in the upgrade group. A satellite device must be part of a satellite software upgrade group to install satellite software on satellite devices in most installation scenarios. All satellite devices in a satellite device cluster are automatically part of the same satellite software upgrade group. The satellite software upgrade group for the satellite devices in the cluster is automatically created and has the same name as the satellite device cluster. Satellite software upgrade group associations must match on both aggregation devices. - (satellite device cluster) To associate all satellite devices in the satellite device cluster with a satellite software image. For example: **request system software add /var/tmp/**	Satellite software upgrade group overview: "Understanding Software in a Junos Fusion Enterprise" on page 24 Satellite software upgrade group management: - "Managing Satellite Software Upgrade Groups in a Junos Fusion" on page 100 - *satellite* - "Configuring or Expanding a Junos Fusion Enterprise" on page 49 - *request system software add (Junos OS)*	

Table 11: Junos Fusion Enterprise Installation Checklist ***(Continued)***

Task	Additional Information	For More Information	Performed by and Date
	satellite-3.0R1.2-signed.tgz upgrade-group sd-cluster-building1 • (standalone satellite device) Create a satellite software upgrade group, and associate the satellite device with a satellite software image. For example: **set chassis satellite-management upgrade-groups standalone-satdevs-building1 satellite 130-139** **request system software add /var/tmp/satellite-3.0R1.2-signed.tgz upgrade-group standalone-satdevs-building1**		
Configuring the Second Aggregation Device (Dual Aggregation Device Topologies Only) (Aggregation Devices)			

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Delete single home configuration mode on both aggregation devices.	To delete single home configuration mode on aggregation device 1: `delete chassis satellite-management single-home` Enter the same command on aggregation device 2: `delete chassis satellite-management single-home`	Dual aggregation device overview: "Understanding Junos Fusion Enterprise Components" on page 5 Deleting single home configuration: • "Configuring or Expanding a Junos Fusion Enterprise" on page 49 *single-home*	
Create and number the redundancy group on both aggregation devices.	To create and number the redundancy group on aggregation device 1: **set chassis satellite-management redundancy-groups junos-fusion-campus-network redundancy-group-id 1** Enter the same command on aggregation device 2:**set chassis satellite-management redundancy-groups junos-fusion-campus-network redundancy-group-id 1**	Dual aggregation device overview: "Understanding Junos Fusion Enterprise Components" on page 5 Dual aggregation device configuration: "Configuring or Expanding a Junos Fusion Enterprise" on page 49	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Define the chassis ID number on each aggregation device.	To define the chassis ID on aggregation device 1:**set chassis satellite-management redundancy-groups chassis-id 1** To define the chassis ID on aggregation device 2:**set chassis satellite-management redundancy-groups chassis-id 2**	Dual aggregation device overview: "Understanding Junos Fusion Enterprise Components" on page 5 Dual aggregation device configuration: "Configuring or Expanding a Junos Fusion Enterprise" on page 49	
Define the peer chassis ID number and ICL interface on each aggregation device.	To define the peer chassis ID and ICL interface on aggregation device 1: **set chassis satellite-management redundancy-groups junos-fusion-campus-network peer-chassis-id 2 inter-chassis-link xe-0/0/1** To define the peer chassis ID and ICL interface on aggregation device 2: **set chassis satellite-management redundancy-groups junos-fusion-campus-network peer-chassis-id 1 inter-chassis-link xe-0/0/1**	Dual aggregation device overview: "Understanding Junos Fusion Enterprise Components" on page 5 Dual aggregation device configuration: "Configuring or Expanding a Junos Fusion Enterprise" on page 49	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Add all satellite devices to the redundancy group on each aggregation device.	On aggregation device 1: **set chassis satellite-management redundancy-groups junos-fusion-campus-network satellite 130-131** **set chassis satellite-management redundancy-groups junos-fusion-campus-network cluster building-1** **set chassis satellite-management redundancy-groups junos-fusion-campus-network cluster building-2** Enter the same commands on aggregation device 2: **set chassis satellite-management redundancy-groups junos-fusion-campus-network satellite 130-131** **set chassis satellite-management redundancy-groups junos-fusion-campus-network cluster building-1** **set chassis satellite-management redundancy-groups junos-fusion-campus-network cluster building-2**	Dual aggregation device overview: "Understanding Junos Fusion Enterprise Components" on page 5 Dual aggregation device configuration: "Configuring or Expanding a Junos Fusion Enterprise" on page 49	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
Ensure ICCP is configured: - Automatic ICCP provisioning. If you are not integrating your Junos Fusion Enterprise into an existing Enterprise or campus network, ICCP is automatically provisioned. No user action is required. - Manual ICCP configuration. If you are integrating your Junos Fusion Enterprise into an existing Enterprise or campus network, you may have to modify some ICCP setting to ensure the Junos Fusion Enterprise functions properly in your environment.	- Automatic ICCP provisioning: No user action required. - Manual ICCP configuration. See Configuring Multichassis Link Aggregation on EX Series Switches.	ICCP overview: "Understanding ICCP in a Junos Fusion using Dual Aggregation Devices" on page 39 Manual ICCP configuration: - Configuring Multichassis Link Aggregation on EX Series Switches	
Adding Satellite Devices (Aggregation Devices)			

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date

Install satellite software onto a satellite device that is currently running Junos OS using one of the following methods:
• (Recommended) Autoconversion—Satellite software installed when satellite device cabled to aggregation device.
• Manual conversion—Satellite software is installed when user enters CLI command to install satellite software.
• Pre-installation—Satellite software is installed on satellite device before cabling it into the Junos Fusion.
A switch may have satellite software pre-installed because it was ordered
	• To enable autoconversion:
	`set chassis satellite-management auto-satellite-conversion satellite 101`
	• To manually convert a satellite device:
	NOTE: This command is entered from an aggregation device.
	`request chassis satellite interface xe-0/0/1 device-mode satellite`
	• To manually install satellite software onto a satellite device:
	NOTE: This command is entered on the satellite device before it is configured into the Junos Fusion Enterprise. Please use the platform specific satellite software package appropriate for the platform as documented in *Understanding*
		Satellite software installation methods overview: "Understanding Software in a Junos Fusion Enterprise" on page 24
		Installing satellite software:
		• "Configuring or Expanding a Junos Fusion Enterprise" on page 49
		• *satellite (Junos Fusion Automatic Satellite Conversion)*
		• *request chassis satellite interface*
		• *request chassis device-mode satellite*	

Table 11: Junos Fusion Enterprise Installation Checklist *(Continued)*

Task	Additional Information	For More Information	Performed by and Date
from the factory running satellite software, it was previously part of a different Junos Fusion, or a user manually installed satellite software onto the switch.	*Platform-specific Satellite Software* in "Understanding Software in a Junos Fusion Enterprise" on page 24.		

RELATED DOCUMENTATION

- Junos Fusion Hardware and Software Compatibility Matrices
- Understanding Junos Fusion Enterprise Software and Hardware Requirements | 28
- Configuring or Expanding a Junos Fusion Enterprise | 49
- Understanding Junos Fusion Enterprise Components | 5

Adding a Switch Running Satellite Software to a Junos Fusion Enterprise

Use this procedure to add a switch that is already running satellite software to an operational Junos Fusion Enterprise as a satellite device.

NOTE: To add a switch running satellite software version 2.0 to a satellite device cluster of a Junos Fusion Enterprise system:

1. Convert the switch to Junos OS. See "Installing Junos OS Software on a Standalone Device Running Satellite Software" on page 128.

2. Switch to the Junos Fusion Enterprise system. See the section *Installing Satellite Software and Adding Satellite Devices to the Junos Fusion* in "Configuring or Expanding a Junos Fusion Enterprise" on page 49.

A switch could already be running satellite software because it was previously part of another Junos Fusion, or because a user manually installed the satellite software.

To add a switch running satellite software to a Junos Fusion Enterprise as a satellite device:

Before you begin:

- Ensure the version of satellite software on your switch is supported by the Junos Fusion Enterprise. See "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28.

- Ensure that a Junos Fusion Enterprise is configured and operational. For detailed information on setting up a Junos Fusion Enterprise, see "Configuring or Expanding a Junos Fusion Enterprise" on page 49.

1. Log into the aggregation device.
2. Configure the link on the aggregation device into a cascade port, if you have not done so already.

   For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces xe-0/0/1 cascade-port
   ```
3. Associate an FPC slot ID with the satellite device.

   There are multiple methods of associating FPC slot IDs. See "Configuring or Expanding a Junos Fusion Enterprise" on page 49 for detailed information regarding FPC slot ID associations with satellite devices.

   Examples:

   - To associate FPC slot ID 101 with the satellite device that is connected to xe-0/0/1:

     ```
     [edit]
     user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
     ```

- To associate FPC slot ID 101 with the satellite device using the serial number ABCDEFGHIJKL:

  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 serial-number
  ABCDEFGHIJKL
  ```

- To associate FPC slot ID 101 with the satellite device using MAC address 12:34:56:AB:CD:EF:

  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 system-id
  12:34:56:AB:CD:EF
  ```

4. (Recommended) Configure the satellite switch into a satellite software upgrade group that uses the same version of satellite software that was manually installed onto the switch.

   This step is advisable, but not always required. Completing this step ensures that the satellite software on your device is not upgraded to the version of satellite software associated with the satellite software upgrade group upon installation.

5. Commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   If you want to commit the configuration to a single Routing Engine:

   ```
   [edit]
   user@aggregation-device# commit
   ```

6. Cable the aggregation device to the satellite device using the assigned cascade port interface on the aggregation device that was assigned in Step 2.

   Cascade port interface support is discussed in "Understanding Junos Fusion Enterprise Software and Hardware Requirements" on page 28.

7. Power on the satellite device, if you have not already done so.

   > **NOTE**: The satellite device can be powered on at any point in this procedure.

RELATED DOCUMENTATION

Configuring or Expanding a Junos Fusion Enterprise | 49

Understanding Junos Fusion Enterprise Software and Hardware Requirements | 28

Enabling Configuration Synchronization Between Aggregation Devices in a Junos Fusion

A Junos Fusion using multiple aggregation devices often requires that the configuration of a feature—for example, an extended port, and entities such as routing instances and VLANs that include the extended port—must match on all aggregation devices. If a configuration statement for the feature—in this case, the extended port—is specified differently on one aggregation device, the statement on that aggregation device might be implemented in an unpredictable manner or might not be implemented at all.

Configuration synchronization can be used to ensure that configuration done in a configuration group is applied on all aggregation devices when committed. Configuration synchronization simplifies administration of a Junos Fusion by allowing users to enter configuration statements in a configuration group and apply the configuration group to all aggregation devices rather than repeating a configuration procedure manually on each aggregation device. Configuration synchronization also ensures configuration consistency in that the same configuration is applied to all aggregation devices.

We strongly recommend using configuration synchronization for software features that must be configured exactly the same on all aggregation devices.

The available group configuration options are beyond the scope of this document; see Understanding MC-LAG Configuration Synchronization and Synchronizing and Committing MC-LAG Configurations for additional information on using group configurations in an MC-LAG topology.

To enable configuration synchronization between aggregation devices in a Junos Fusion.

NOTE: For the sake of brevity, the examples in this procedure show the configuration on only two aggregation devices. Unless specifically called out, the examples for two aggregation devices also apply to topologies with four aggregation devices.

1. Ensure the aggregation devices are reachable from one another:

   Aggregation device 1:

   ```
   user@ad1> ping ad2 rapid
   PING ad2.host.example.net (192.168.255.41): 56 data bytes
   !!!!!
   mostly o--- ad2.example.net ping statistics ---
   ```

```
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.317/0.331/0.378/0.024 ms
```

Aggregation device 2:

```
user@ad2> ping ad1 rapid
PING ad1.host.example.net (192.168.255.40): 56 data bytes
!!!!!
--- ad1.example.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.317/0.331/0.378/0.024 ms
```

If the devices cannot ping one another, try statically mapping the hostnames of each device's management IP address and retry the ping.

Aggregation device 1:

```
user@ad1# set system static-host-mapping inet 192.168.255.41
user@ad1# commit
user@ad1# run ping ad2 rapid
```

Aggregation device 2:

```
user@ad2# set system static-host-mapping ad1 inet 192.168.255.40
user@ad2# commit
user@ad2# run ping ad1 rapid
```

If the devices cannot ping one another after the hostnames are statically mapped, see Connecting and Configuring an EX9200 Switch (CLI Procedure) or the Installation and Upgrade Guide for EX9200 Switches.

2. Enable configuration synchronization:

   Aggregation device 1:

   ```
   user@ad1# set system commit peers-synchronize
   ```

   Aggregation device 2:

   ```
   user@ad2# set system commit peers-synchronize
   ```

3. Configure each aggregation device so that the other aggregation devices are identified as configuration peers. Enter the authentication credentials of each peer aggregation device to ensure group configurations on one aggregation device are committed to the other aggregation devices.

   BEST PRACTICE: Configure a system master password to provide stronger encryption for configuration secrets using the `master-password` CLI statement. For more information on hardening shared secrets, see Master Password for Configuration Encryption.

   WARNING: The password *password* is used in this configuration step for illustrative purposes only. Use a more secure password in your device configuration.

   NOTE: This step assumes a user with an authentication password has already been created on each Juniper Networks switch acting as an aggregation device. For instructions on configuring username and password combinations, see Connecting and Configuring an EX9200 Switch (CLI Procedure).

   Aggregation device 1:

   ```
   user@ad1# set system commit peers ad2 user root authentication password
   ```

   Aggregation device 2:

   ```
   user@ad2# set system commit peers ad1 user root authentication password
   ```

4. Enable the Network Configuration (NETCONF) protocol over SSH:

   Aggregation device 1:

   ```
   user@ad1# set system services netconf ssh
   ```

   Aggregation device 2:

   ```
   user@ad2# set system services netconf ssh
   ```

5. Commit the configuration:

Aggregation device 1:

```
user@ad1# commit
```

Aggregation device 2:

```
user@ad2# commit
```

6. (Optional) Create a configuration group for testing to ensure configuration synchronization is working.

   Example for Junos Fusion Enterprise with aggregation devices that have one Routing Engine:

   Aggregation Device 1:

   ```
   user@ad1# set groups TEST when peers [ad1 ad2]
   user@ad1# set apply-groups TEST
   ```

   Aggregation Device 2:

   ```
   user@ad2# set apply-groups TEST
   ```

7. (Optional) Configure and commit a group on aggregation device 1, and confirm it is implemented on aggregation device 2:

   > **NOTE**: This step shows how to change one interface configuration using groups. Interface ranges cannot be specified within groups and synchronized between configuration peers in a Junos Fusion to configure multiple interfaces simultaneously.

   Aggregation device 1:

   ```
   user@ad1# set groups TEST interfaces ge-0/0/1 description testing123
   user@ad1# commit
   ```

   Aggregation device 2:

   ```
   user@ad2# show groups TEST
   when {
       peers [ ad1 ad2 ];
   ```

```
}
interfaces {
    ge-0/0/1 {
        description testing123;
    }
}
user@ad2# run show interfaces ge-0/0/1
Physical interface: ge-0/0/1, Enabled, Physical link is Down
  Interface index: 235, SNMP ifIndex: 743
  Description: testing123
  (additional output removed for brevity)
```

Perform the same procedure to verify configuration synchronization from aggregation device 2 to aggregation device 1, if desired.

Delete the test configuration group on each aggregation device.

Aggregation device 1:

```
user@ad1# delete groups test
```

Aggregation device 2:

```
user@ad2# delete groups test
```

See Enabling Junos Fusion Enterprise on an Enterprise Campus Network for a sample Junos Fusion Enterprise topology configured largely using configuration synchronization.

RELATED DOCUMENTATION

- Network Configuration Example: Configuring MC-LAG on EX9200 Switches in the Core for Campus Networks
- Synchronizing and Committing MC-LAG Configurations
- Understanding MC-LAG Configuration Synchronization
- Understanding Configuration Synchronization in a Junos Fusion | 27
- Configuring or Expanding a Junos Fusion Enterprise | 49

Configuring Uplink Port Policies on a Junos Fusion

IN THIS SECTION

Ports on a satellite device that can be used as uplink ports are called candidate uplink ports. Each satellite device model has a set of default candidate uplink ports that the device can use to connect to the aggregation device and, in the case of a satellite device cluster, to other satellite devices. You can override the default set of candidate uplink and clustering ports by defining a candidate uplink port policy for the device.

To configure a candidate uplink port policy, you must first configure an uplink port group. The uplink port group defines a set of candidate uplink ports on a satellite device. Uplink port groups are assigned to candidate uplink port policies, which are assigned to satellite devices.

NOTE: The candidate uplink port policy must include at least one port from the default candidate uplink port. Otherwise, the aggregation device will not be able to communicate with the satellite device in order to provision the satellite device with the uplink port policy.

Configuring an Uplink Port Policy for a Standalone Satellite Device

To configure an uplink port policy:

1. Create an uplink port group:

```
[edit policy-options satellite-policies]
user@switch# set port-group-alias port-group-alias-name
```

2. Configure the PICs that contain ports to be identified as candidate uplink ports:

```
[edit policy-options satellite-policies port-group-alias port-group-alias-name]
user@switch# set pic pic-number
```

3. Configure the ports on the PICs to be identified as candidate uplink ports:

```
[edit policy-options satellite-policies port-group-alias port-group-alias-name pic pic-number]
user@switch# set port [port-number | port-number-range | all]
```

4. Create a candidate uplink port policy:

```
[edit policy-options satellite-policies]
user@switch# set candidate-uplink-port-policy policy-name
```

5. Assign the uplink port group to the candidate uplink port policy:

```
[edit policy-options satellite-policies candidate-uplink-port-policy policy-name]
user@switch# set uplink-port-group group-name
```

Configuring an Uplink Port Policy for a Satellite Device Cluster

Candidate uplink port policies for a satellite device cluster can be applied at the cluster level, FPC level, or globally. Policies configured at the FPC-level take precedence over cluster and global policies. Policies configured at the cluster level take precedence over global policies.

1. Follow steps 1-3 in the procedure above to create an uplink port group.
2. Configure a candidate uplink port policy for a satellite cluster at the cluster level, FPC level, or global level:

    - To configure a policy at the cluster level:

    ```
    [edit]
    user@switch# set chassis satellite-management cluster cluster-name cluster-policy
    satellite-port-policy-name
    ```

    - To configure a policy at the FPC level:

    ```
    [edit]
    user@switch# set chassis satellite-management cluster cluster-name fpc fpc-number cluster-
    policy satellite-port-policy-name
    ```

- To configure a policy at the global level:

  ```
  [edit]
  user@switch# set chassis satellite-management cluster-policy satellite-port-policy-name
  ```

3. Assign the uplink port group to the candidate uplink port policy:

   ```
   [edit policy-options satellite-policies candidate-uplink-port-policy policy-name]
   user@switch# set uplink-port-group group-name
   ```

RELATED DOCUMENTATION

Understanding Satellite Policies in a Junos Fusion | 45

Configuring Satellite Device Alarm Handling Using an Environment Monitoring Satellite Policy in a Junos Fusion

This topic shows how to configure the alarm levels for link-down events on a satellite device in a Junos Fusion.

To configure system alarm handling in a Junos Fusion using an environment monitoring satellite policy:

1. Log in to the aggregation device.
2. Create and name the environment monitoring satellite policy:

   ```
   [edit]
   user@aggregation-device# set policy-options satellite-policies environment-monitoring-policy
   policy-name
   ```

   For example, to create an environment monitoring satellite policy named **linkdown-alarm-monitoring-1**:

   ```
   [edit]
   user@aggregation-device# set policy-options satellite-policies environment-monitoring-policy
   linkdown-alarm-monitoring-1
   ```

3. Configure the link-down alarm behavior for the Junos Fusion using one or both of the following methods:

   - Set the default link-down alarm to one setting whenever it is experienced in a Junos Fusion:

     ```
     [edit policy-options satellite-policies environment-monitoring-policy policy-name]
     user@aggregation-device# set alarm linkdown  [ignore | red | yellow]
     ```

     For example, to set the default link-down alarm to ignore for **linkdown-alarm-monitoring-1**:

     ```
     [edit policy-options satellite-policies environment-monitoring-policy linkdown-alarm-
     monitoring-1]
     user@aggregation-device# set alarm linkdown ignore
     ```

   - Set the link-down alarm behavior for a specific satellite device hardware model using terms:

     ```
     [edit policy-options satellite-policies environment-monitoring-policy policy-name]
     user@aggregation-device# set term term-name from product-model model-name alarm linkdown
     [ignore | red | yellow]
     ```

     where *term-name* is the user-defined name of the term, and *model-name* defines the product model of the satellite device that uses the satellite policy.

     You can apply environment monitoring satellite policies individually or globally. You can, therefore, create multiple policies using the instructions in this step and apply them to different satellite devices in your Junos Fusion, when needed.

     You can use multiple terms in the same environment monitoring satellite policy.

     For example, if you wanted to configure EX4300 switches acting as satellite devices to send yellow alarms when link-down errors occur while QFX5100 switches acting as satellite devices send red alarms for the same condition:

     ```
     [edit policy-options satellite-policies environment-monitoring-policy linkdown-alarm-
     monitoring-1]
     user@aggregation-device# set term ex4300-yellow from product-model EX4300* alarm linkdown
     yellow
     user@aggregation-device# set term qfx5100-red from product-model QFX5100* alarm linkdown
     red
     ```

4. Associate the environment monitoring satellite policy with a Junos Fusion configuration.

- To associate an environment monitoring satellite policy for all satellite devices in a Junos Fusion:

  ```
  [edit chassis satellite-management]
  user@aggregation-device# set environment-monitoring-policy policy-name
  ```

  For example, to associate an environment monitoring satellite policy named **linkdown-alarm-monitoring-1** for all satellite devices in a Junos Fusion:

  ```
  [edit chassis satellite-management]
  user@aggregation-device# set environment-monitoring-policy linkdown-alarm-monitoring-1
  ```

- To associate an environment monitoring satellite policy for select FPC IDs in a Junos Fusion:

  ```
  [edit chassis satellite-management fpc slot-id]
  user@aggregation-device# set environment-monitoring-policy policy-name
  ```

  For example, to associate an environment monitoring satellite policy named **linkdown-alarm-monitoring-1** for the satellite device associated with FPC ID 101 in a Junos Fusion:

  ```
  [edit chassis satellite-management fpc 101]
  user@aggregation-device# set environment-monitoring-policy linkdown-alarm-monitoring-1
  ```

You can configure a different environment monitoring policy for a single satellite device using the **fpc *slot-id*** when an environment monitoring policy for all satellite devices is configured. The environment monitoring policy for the FPC is enabled in cases when both an individual and global environment monitoring policy are configured.

5. Commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   If you want to commit the configuration to the active Routing Engine only:

   ```
   [edit]
   user@aggregation-device# commit
   ```

RELATED DOCUMENTATION

Configuring Junos Fusion Provider Edge

Configuring or Expanding a Junos Fusion Enterprise

CHAPTER 3

Junos Fusion Enterprise Configuration Statements

CHAPTER 4

Junos Fusion Enterprise Administration

IN THIS CHAPTER

Managing Satellite Software Upgrade Groups in a Junos Fusion

IN THIS SECTION

This topic discusses maintaining satellite software upgrade groups in a Junos Fusion. For more information on the process for creating a satellite software upgrade group, see *Configuring Junos Fusion Provider Edge* or Configuring or Expanding a Junos Fusion Enterprise.

A satellite software upgrade group is a group of satellite devices that are designated to upgrade to the same satellite software version using the same satellite software package. One Junos Fusion can contain multiple software upgrade groups, and multiple software upgrade groups should be configured in most Junos Fusions to avoid network downtimes during satellite software installations.

When a satellite device is added to a Junos Fusion, the aggregation device checks if the satellite device is using an FPC ID that is included in a satellite software upgrade group. If the satellite device is using an FPC ID that is part of a satellite software upgrade group, the device upgrades its satellite software to the version of software associated with the satellite software upgrade group - unless it is already running the defined version.

When the satellite software package associated with an existing satellite software group is changed, the satellite software for all member satellite devices is upgraded using a throttled upgrade. The throttled upgrade ensures that the aggregation device is not overwhelmed with providing satellite software simultaneously to many satellite devices.

The two most common methods of installing satellite software—autoconverting a device into a satellite device when it is cabled into an aggregation device and manually converting a device that is cabled into an aggregation device into a satellite device—require a configured satellite software upgrade group.

Software upgrade groups are configured and managed from the aggregation device. All satellite devices in a satellite device cluster are part of the same software upgrade group, and a software upgrade group with the name of the satellite device cluster is automatically created when the satellite device cluster is created.

Creating a Satellite Software Upgrade Group

If your satellite device is a member of a satellite device cluster, a satellite software upgrade group with the name of the satellite device cluster is automatically created when the satellite device cluster is created. This satellite software upgrade group must be used to manage the satellite software for all member satellite devices in the satellite device cluster.

For information on creating a satellite software upgrade group for a satellite device that is not part of a satellite device cluster, see *Configuring Junos Fusion Provider Edge* or Configuring or Expanding a Junos Fusion Enterprise.

Adding Satellite Devices to a Satellite Software Upgrade Group

To add a satellite device to an existing satellite software upgrade group, enter the `set chassis satellite-management upgrade-groups` *upgrade-group-name* `satellite` *slot-id-or-range* command:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-groups upgrade-group-name
satellite slot-id-or-range
```

where *upgrade-group-name* is the name of the existing satellite software upgrade group, and the *slot-id-or-range* is the FPC slot ID or range of FPC slot IDs of the satellite devices that are being added to the upgrade group.

For example, to add FPC slot IDs 121, 122, and 123 to a satellite software upgrade group named **group1**:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-groups group1 satellite 121-123
```

Additionally, you can use the **all** statement as your *slot-id-or-range* to include all satellite devices in the Junos Fusion in the satellite software upgrade group.

For example, to add all satellite devices in the Junos Fusion to a satellite software upgrade group named **group1**:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-groups group1 satellite all
```

Removing a Satellite Device from a Satellite Software Upgrade Group

To remove a satellite device from an existing satellite software upgrade group, enter the `delete chassis satellite-management upgrade-groups` *`upgrade-group-name`* `satellite` *`slot-id-or-range`* statement to delete the statements that initially added the member satellite devices to the satellite software upgrade group.

```
[edit]
user@aggregation-device# delete chassis satellite-management upgrade-groups upgrade-group-name
satellite slot-id-or-range
```

where *upgrade-group-name* is the name of the existing satellite software upgrade group, and the *slot-id-or-range* is the FPC slot ID or range of FPC slot IDs of the satellite devices that are being added to the upgrade group.

In cases where you want to remove some FPC slot IDs that were configured within a range of FPC slot IDs, you might consider re-creating the satellite software group by first deleting it, then re-creating it. To delete the satellite software upgrade group:

```
[edit]
user@aggregation-device# delete chassis satellite-management upgrade-groups upgrade-group-name
```

You can then re-create the satellite software upgrade group and add satellite devices using the `set chassis satellite-management upgrade-groups` *`upgrade-group-name`* `satellite` *`slot-id-or-range`* statement:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-groups upgrade-group-name
satellite slot-id-or-range
```

For more information on the satellite software upgrade group creation process, see *Configuring Junos Fusion Provider Edge* or Configuring or Expanding a Junos Fusion Enterprise.

Modifying the Satellite Software Used by a Satellite Software Upgrade Group

Before you begin:

- Ensure that a satellite software package is downloaded to the location where you will use it to install the satellite software.

```
user@aggregation-device> request system software add package-name upgrade-group upgrade-group-
name
```

NOTE: A satellite software *upgrade-group-name* can be a user-configured upgrade group or the name of a satellite device cluster.

To associate a satellite software image named **satellite-2.0R1.2-signed.tgz** that is currently stored in the **/var/tmp/** directory from the aggregation device to the upgrade group named **group1**:

```
user@aggregation-device> request system software add /var/tmp/satellite-2.0R1.2-signed.tgz
upgrade-group group1
```

To associate a satellite software package that was previously installed on the aggregation device with a software upgrade group:

```
user@aggregation-device> request system software add version version upgrade-group group1
```

For instance:

```
user@aggregation-device> request system software add version 2.0R1.2 upgrade-group group1
```

The satellite software upgrade group is associated with the software package after either of these commands are entered.

NOTE: A satellite software upgrade group can be a user-configured upgrade group or the name of a satellite device cluster.

If the group was already associated with a satellite software upgrade group, the previous satellite software package associated with the software group remains the second option for updating satellite software for the satellite software upgrade group. You can disassociate any satellite software package from a satellite software upgrade group using the instructions in the next section.

To associate a new satellite software image with the software upgrade group:

Deleting Associated Satellite Software from a Satellite Software Upgrade Group

This section describes how to delete a satellite software package association from a satellite software upgrade group.

This procedure is always optional. You can always update the satellite software associated with a satellite software upgrade group using the procedure in the previous section, without deleting the satellite software from the satellite software upgrade group.

When a new satellite software package is associated with a satellite software upgrade, the previous satellite software package remains associated with the upgrade group as a backup option. The satellite software upgrade group can be associated with up to two satellite software packages, so no other satellite software packages can be associated with the satellite software upgrade group.

This process disassociates the specified satellite software package from the list of potential packages used by a satellite software upgrade group. It is useful for maintenance purposes only, like if you wanted to ensure a satellite software upgrade group was never associated with a specific satellite software package.

To disassociate a satellite software image from a satellite software upgrade group:

```
user@aggregation-device> request system software delete upgrade-group upgrade-group-name
```

where the *upgrade-group-name* is the name of the upgrade group that was assigned by the user.

For example, to delete the current satellite software image association to the upgrade group named **group1**:

```
user@aggregation-device> request system software delete upgrade-group group1
```

Deleting Satellite Software on the Aggregation Device

This section describes how to remove a satellite software package from a Junos Fusion system. This will remove the software from the aggregation device as well as any association with any satellite software upgrade groups. This should be done when another satellite software version is available and will free up the space occupied by the software being removed.

> **NOTE**: We recommend deleting satellite software that is not in use to free up space on a QFX10000 acting as an aggregation device.

```
user@aggregation-device> request system software delete version version
```

For example:

```
user@aggregation-device> request system software delete version 2.0R1.2
```

RELATED DOCUMENTATION

Configuring Junos Fusion Provider Edge

Configuring or Expanding a Junos Fusion Enterprise

Upgrading Junos OS and Satellite Software in an Operational Junos Fusion Enterprise with Dual Aggregation Devices

You may have to upgrade Junos OS on the aggregation devices in your Junos Fusion Enterprise after initial setup.

To ensure consistent behavior and feature support in your Junos Fusion Enterprise, we strongly recommend that both aggregation devices—and both Routing Engines in the aggregation devices—run the same version of Junos OS.

Satellite software should also be upgraded after the Junos OS upgrade to ensure it is compatible with the upgraded Junos OS.

We recommend following this procedure to upgrade Junos OS in a Junos Fusion Enterprise using a dual aggregation device topology:

1. Upgrade the Junos OS software on the backup Routing Engine of one of the aggregation devices. Do not reboot the backup Routing Engine to complete the upgrade at this point of the procedure.

   See Junos Fusion Hardware and Software Compatibility Matrices for software compatibility information and to retrieve Junos OS images for EX9200 switches that can act as aggregation devices in a Junos Fusion Enterprise.

   This step is performed in this example by showing an upgrade to 17.2R1 with a Junos OS image that is installed in the local /var/tmp folder. See Understanding Software Installation on EX Series Switches for information on other procedures that can be used to upgrade Junos OS running on a Routing Engine on an EX9200 switch.

   ```
   user@ad2-ex9208> request system software add /var/tmp/junos-install-ex92xx-
   x86-64-17.1R2.7.tgz re1
   ```

2. Upgrade the Junos OS software on the primary Routing Engine of the same aggregation device. Do not reboot the primary Routing Engine to complete the upgrade at this point of the procedure.

   ```
   user@ad2-ex9208> request system software add /var/tmp/junos-install-ex92xx-
   x86-64-17.1R2.7.tgz re0
   ```

3. After steps 1 and 2 are completed successfully, reboot both Routing Engines simultaneously:

   ```
   user@ad2-ex9208> request system reboot both-routing-engines
   ```

4. Repeat the same procedure on the other aggregation device:

   ```
   user@ad1-ex9208> request system software add /var/tmp/junos-install-ex92xx-
   x86-64-17.1R2.7.tgz re1
   user@ad1-ex9208> request system software add /var/tmp/junos-install-ex92xx-
   x86-64-17.1R2.7.tgz re0
   user@ad1-ex9208> request system reboot both-routing-engines
   ```

5. After all Routing Engines on both aggregation devices have rebooted to complete the Junos OS upgrade, upgrade the satellite software on all satellite devices to the satellite software version that is compatible with the Junos OS running on the aggregation devices.

   To identify the version of satellite software that works with the new version of Junos OS, see Junos Fusion Hardware and Software Compatibility Matrices.

   To install the new version of satellite software, see Installing Satellite Software and Adding Satellite Devices to the Junos Fusion and Modifying the Satellite Software Used by a Satellite Software Upgrade Group.

RELATED DOCUMENTATION

Junos Fusion Hardware and Software Compatibility Matrices

Installing Satellite Software and Adding Satellite Devices to the Junos Fusion

Verifying Connectivity, Device States, Satellite Software Versions, and Operations in a Junos Fusion

IN THIS SECTION

This topic provides information on common procedures to verify connectivity, device states, satellite software versions, and other operations in a Junos Fusion. It covers:

Verifying a Junos Fusion Configuration

IN THIS SECTION

Purpose

Verify that a device is recognized as a satellite device by the aggregation device.

Action

Enter the **show chassis satellite** command and review the output.

```
user@aggregation-device> show chassis satellite
                        Device          Cascade      Port       Extended Ports
Alias            Slot   State           Ports        State      Total/Up
qfx5100-24q-01   100    Online          xe-0/0/1     online     9/2
                                        xe-1/3/0     online
qfx5100-24q-02   101    Online          xe-0/0/2     online     20/10
                                        xe-1/3/1     online
qfx5100-24q-03   102    Online          xe-0/0/3     online     16/4
                                        xe-1/3/2     online
qfx5100-24q-04   103    Online          xe-0/0/4     absent     13/3
                                        xe-1/3/3     online
ex4300-01        109    Online          xe-1/0/1     online     49/2
ex4300-02        110    Online          xe-1/0/2     online     49/2
```

Meaning

Use the output of **show chassis satellite** to confirm the following connections in a Junos Fusion:

- Whether a satellite device is recognized at all by the aggregation device. If the satellite device does not appear in the **show chassis satellite** output, then it is not recognized by the aggregation device as a satellite device.
- The state of a particular satellite device, via the **Device State** output.
- The state of the cascade port connection, via the **Cascade State** output.

Verifying Basic Junos Fusion Connectivity

IN THIS SECTION

Purpose

Verify that all satellite devices are recognized by the aggregation device, and that all cascade and extended ports are recognized.

Action

Enter the `show chassis satellite` command on the aggregation device.

```
user@aggregation-device> show chassis satellite
                        Device          Cascade      Port       Extended Ports
Alias            Slot   State           Ports        State      Total/Up
qfx5100-24q-01   100    Online          xe-0/0/1     online     9/2
                                        xe-1/3/0     online
qfx5100-24q-02   101    Online          xe-0/0/2     online     20/12
                                        xe-1/3/1     online
qfx5100-24q-03   102    Online          xe-0/0/3     online     16/6
                                        xe-1/3/2     online
qfx5100-24q-04   103    Online          xe-0/0/4     online     16/4
                                        xe-1/3/3     online
qfx5100-24q-05   104    Online          xe-0/0/5     online     13/3
                                        xe-1/3/4     online
qfx5100-24q-06   105    Online          xe-0/0/6     online     24/15
                                        xe-1/3/5     online
qfx5100-24q-07   106    Online          xe-0/0/7     online     24/15
                                        xe-1/3/6     online
qfx5100-24q-08   107    Online          xe-0/0/8     online     21/12
                                        xe-1/3/7     online
ex4300-01        109    Online          xe-1/0/1     online     49/2
ex4300-02        110    Online          xe-1/0/2     online     49/2
ex4300-03        111    Online          xe-1/0/3     online     49/2
ex4300-04        112    Online          xe-1/0/4     online     49/11
ex4300-05        113    Online          xe-1/0/5     online     49/11
ex4300-06        114    Online          xe-1/0/6     online     49/11
ex4300-07        115    Online          xe-1/0/7     online     49/11
ex4300-08        116    Online          xe-1/1/0     online     49/11
ex4300-09        117    Online          xe-1/1/1     online     49/11
```

```
ex4300-10          118    Online           xe-1/1/2     online     49/11
ex4300-11          119    Online           xe-1/1/3     online     49/11
ex4300-12          120    Online           xe-1/1/4     online     49/11
ex4300-13          121    Online           xe-1/1/5     online     49/11
ex4300-14          122    Online           xe-1/1/6     online     49/11
ex4300-15          123    Online           xe-1/1/7     online     49/11
ex4300-16          124    Online           xe-1/2/1     online     49/11
ex4300-17          125    Online           xe-1/2/2     online     49/11
ex4300-18          126    Online           xe-1/2/3     online     49/2
ex4300-19          127    Online           xe-1/2/4     online     49/1
ex4300-20          128    Online           xe-1/2/5     online     49/1
ex4300-21          129    Online           xe-1/2/6     online     49/1
ex4300-22          130    Online           xe-1/2/7     online     49/1
```

Meaning

The output confirms:

- Each listed satellite device—the satellite devices are listed by alias-name in the `Alias` column or by FPC slot ID in the `Slot` column—is recognized by the aggregation device, because the `Device State` output is `Online` for every listed satellite device.

- Each cascade port is operational, because `Port State` is `online` for every cascade port. The cascade port is the port on the aggregation device that connects to the satellite device.

- The number of available and active extended ports for each satellite device, using the `Extended Ports total` and `Extended Ports up` outputs. The number of extended ports varies by satellite devices, and in this output the total number of extended ports includes both network-facing extended ports as well as uplink ports.

Verifying the Satellite Device Hardware Model

IN THIS SECTION

Purpose

Verify the hardware model of each satellite device in the Junos Fusion.

Action

Enter the `show chassis satellite terse` command on the aggregation device.

```
user@aggregation-device> show chassis satellite terse
       Device                            Extended Ports
Slot   State            Model            Total/Up    Version
101    Online           QFX5100-48S-6Q   7/6         3.0R1.0
102    Online           QFX5100-48S-6Q   7/6         3.0R1.0
103    Online           QFX5100-48S-6Q   6/4         3.0R1.0
104    Online           QFX5100-48S-6Q   14/14       3.0R1.0
105    Online           QFX5100-48S-6Q   18/18       3.0R1.0
106    Online           QFX5100-48S-6Q   17/16       3.0R1.0
107    Online           EX4300-48T       52/6        3.0R1.0
108    Online           EX4300-48T       52/13       3.0R1.0
109    Online           EX4300-48T       51/13       3.0R1.0
110    Online           EX4300-48T       51/14       3.0R1.0
111    Online           EX4300-48T       51/13       3.0R1.0
112    Online           EX4300-48T       51/12       3.0R1.0
113    Online           EX4300-48T       51/13       3.0R1.0
114    Online           QFX5100-24Q-2P   17/13       3.0R1.0
```

Meaning

The output shows the device model of each satellite device in the `Device Model` output, which are listed by FPC slot identification number using the `Slot` output.

This command is also useful for verifying the version satellite software running on each satellite device, as the version is listed in the `Version` output.

Verifying Cascade Port and Uplink Port State

IN THIS SECTION

Purpose

Verify that the cascade port and uplink port interfaces are up.

Action

Enter the `show chassis satellite interface` command:

```
user@aggregation-device> show chassis satellite interface


Interface         State        Type
lo0               Up           Loopback

sd-101/0/0        Up           Satellite

sd-102/0/0        Up           Satellite

sd-103/0/0        Up           Satellite

sd-104/0/0        Up           Satellite

sd-105/0/0        Up           Satellite

sd-106/0/0        Up           Satellite

sd-107/0/0        Up           Satellite

sd-108/0/0        Up           Satellite

sd-109/0/0        Up           Satellite

sd-110/0/0        Up           Satellite

sd-111/0/0        Up           Satellite

sd-112/0/0        Up           Satellite
```

```
sd-113/0/0        Up           Satellite
sd-114/0/0        Up           Satellite
xe-0/0/1          Up           Cascade
xe-0/0/2          Up           Cascade
xe-0/0/3          Up           Cascade
xe-0/0/4          Up           Cascade
xe-0/0/5          Up           Cascade
xe-0/0/6          Up           Cascade
xe-0/0/7          Up           Cascade
xe-0/0/8          Up           Cascade
xe-0/0/9          Up           Cascade
xe-0/2/0          Up           Cascade
xe-0/2/1          Up           Cascade
xe-0/2/2          Up           Cascade
xe-0/2/3          Up           Cascade
xe-0/2/4          Up           Cascade
xe-0/2/5          Up           Cascade
xe-0/2/6          Up           Cascade
xe-0/2/7          Up           Cascade
xe-1/0/1          Up           Cascade
xe-1/0/2          Up           Cascade
```

```
xe-1/0/3          Up           Cascade

xe-1/2/1          Up           Cascade

xe-1/2/2          Up           Cascade

xe-1/2/3          Up           Cascade

xe-2/0/0          Up           Cascade

xe-2/0/1          Up           Cascade

xe-2/0/2          Up           Cascade

xe-2/0/3          Up           Cascade

xe-2/0/4          Up           Cascade

xe-2/0/5          Up           Cascade

xe-2/0/6          Up           Cascade

xe-2/0/7          Up           Cascade

xe-2/1/0          Up           Cascade

xe-2/1/1          Up           Cascade

xe-2/1/2          Up           Cascade

xe-2/1/3          Up           Cascade

xe-2/1/4          Up           Cascade

xe-2/1/5          Up           Cascade

xe-2/1/6          Up           Cascade

xe-2/1/7          Up           Cascade

xe-2/2/0          Up           Cascade

xe-2/2/1          Up           Cascade
```

```
xe-2/2/2          Up           Cascade
xe-2/2/3          Up           Cascade
xe-2/2/4          Up           Cascade
xe-2/2/5          Up           Cascade
xe-2/2/6          Up           Cascade
xe-2/2/7          Up           Cascade
xe-2/3/0          Up           Cascade
xe-2/3/3          Dn           Cascade
xe-2/3/4          Up           Cascade
xe-2/3/5          Up           Cascade
xe-2/3/6          Up           Cascade
xe-2/3/7          Up           Cascade
```

Meaning

The output shows:

- Whether the recognized port is up or down, using the `State` column output. The `State` column output is `Up` when the interface is up and `Dn` when the interface is down.

Verifying That a Cascade Port Recognizes a Satellite Device

IN THIS SECTION

Purpose

Verify that a cascade port on an aggregation device recognizes a satellite device in the Junos Fusion. This procedure also provides a method of verifying the hardware and software information for each satellite device in the Junos Fusion.

Action

Enter the `show chassis satellite neighbor` command:

```
user@aggregation-device> show chassis satellite neighbor
Interface   State      Port Info   System Name  Model           SW Version
xe-2/3/7    Init
xe-2/3/6    Init
xe-2/3/5    Init
xe-2/3/4    Init
xe-2/3/3    Dn
xe-2/3/0    Two-Way    xe-0/2/2        ex4300-29 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/2/7    Two-Way    xe-0/2/2        ex4300-28 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/2/6    Two-Way    xe-0/2/2        ex4300-27 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/2/5    Two-Way    xe-0/2/2        ex4300-26 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/2/4    Init
xe-2/2/3    Init
xe-2/2/2    Two-Way    xe-0/0/48:3 qfx5100-48s-06 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-2/2/1    Two-Way    xe-0/0/48:3 qfx5100-48s-05 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-2/2/0    Init
xe-2/1/7    Init
xe-2/1/6    Init
xe-2/1/5    Two-Way    xe-0/0/4:2  qfx5100-24q-09 QFX5100-24Q-2P 0.1I20150224_18
27_dc-builder
xe-2/1/4    Two-Way    xe-0/2/1        ex4300-31 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/1/3    Two-Way    xe-0/2/1        ex4300-30 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/1/2    Two-Way    xe-0/2/1        ex4300-29 EX4300-48T     0.1I20150224_182
7_dc-builder
```

```
xe-2/1/1    Two-Way    xe-0/2/1        ex4300-28 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/1/0    Init
xe-2/0/7    Two-Way    xe-0/2/1        ex4300-26 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-2/0/6    Init
xe-2/0/5    Init
xe-2/0/4    Init
xe-2/0/3    Init
xe-2/0/2    Two-Way    xe-0/0/48:2 qfx5100-48s-04 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-2/0/1    Two-Way    xe-0/0/48:2 qfx5100-48s-03 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-2/0/0    Init
xe-1/2/3    Two-Way    xe-0/0/0:0  qfx5100-24q-09 QFX5100-24Q-2P 0.1I20150224_18
27_dc-builder
xe-1/2/2    Two-Way    xe-0/2/0        ex4300-31 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-1/2/1    Two-Way    xe-0/2/0        ex4300-30 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-1/0/3    Two-Way    xe-0/2/0        ex4300-29 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-1/0/2    Two-Way    xe-0/2/0        ex4300-28 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-1/0/1    Two-Way    xe-0/2/0        ex4300-27 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-0/2/7    Two-Way    xe-0/0/0:1  qfx5100-24q-09 QFX5100-24Q-2P 0.1I20150224_18
27_dc-builder
xe-0/2/6    Init
xe-0/2/5    Init
xe-0/2/4    Two-Way    xe-0/0/48:1 qfx5100-48s-05 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/2/3    Two-Way    xe-0/0/48:1 qfx5100-48s-04 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/2/2    Two-Way    xe-0/0/48:1 qfx5100-48s-03 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/2/1    Init
xe-0/2/0    Init
xe-0/0/9    Two-Way    xe-0/2/0        ex4300-26 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-0/0/8    Two-Way    xe-0/2/0        ex4300-25 EX4300-48T     0.1I20150224_182
7_dc-builder
xe-0/0/7    Two-Way    xe-0/0/48:0 qfx5100-48s-07 QFX5100-48S-6Q 0.1I20150224_18
```

```
27_dc-builder
xe-0/0/6    Two-Way    xe-0/0/48:0 qfx5100-48s-06 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/0/5    Two-Way    xe-0/0/48:0 qfx5100-48s-05 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/0/4    Two-Way    xe-0/0/48:0 qfx5100-48s-04 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/0/3    Two-Way    xe-0/0/48:0 qfx5100-48s-03 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/0/2    Two-Way    xe-0/0/48:0 qfx5100-48s-02 QFX5100-48S-6Q 0.1I20150224_18
27_dc-builder
xe-0/0/1    Init
```

Meaning

The output confirms:

- The cascade ports on the aggregation device that are recognized by the Junos Fusion. All recognized cascade port interfaces are listed in the `Interface` output.
- The uplink ports on the satellite devices that are connected to the cascade ports. The cascade port on each satellite device is identified in the `Port Info` column, and the satellite device itself is identified in the `System Name` output.
- Whether the cascade port to uplink port connection has initialized, using the `State` output. The `State` output is `Two-Way` when the satellite device is properly initialized, and traffic can be passed between the aggregation device and the satellite device over the link.
- The hardware model of each satellite device in the `Model` column, and the satellite software running on each satellite device in the `SW Version` output.

Verifying Extended Port Operation

IN THIS SECTION

Purpose

Verify that a specific extended port is recognized by the aggregation device, and is operational.

Action

Enter the `show chassis satellite extended-port` command on the aggregation device:

```
user@aggregation-device> show chassis satellite extended-port
Legend for interface types:
   * -- Uplink interface
                              Rx            Tx            Admin/Op IFD
Name           State          Request State Request State State    Idx   PCID
et-100/0/2     AddComplete    None          Ready         Up/Dn    838   110
et-104/0/2     AddComplete    None          Ready         Up/Dn    813   110
et-107/0/23    AddComplete    None          Ready         Up/Up    544   194
ge-109/0/0     AddComplete    None          Ready         Up/Up    402   115
ge-109/0/1     AddComplete    None          Ready         Up/Dn    403   114
ge-109/0/10    AddComplete    None          Ready         Up/Dn    412   113
ge-109/0/11    AddComplete    None          Ready         Up/Dn    413   112
ge-109/0/12    AddComplete    None          Ready         Up/Dn    414   123
ge-109/0/13    AddComplete    None          Ready         Up/Dn    415   122
ge-109/0/14    AddComplete    None          Ready         Up/Dn    416   125
ge-109/0/15    AddComplete    None          Ready         Up/Dn    417   124
ge-109/0/16    AddComplete    None          Ready         Up/Dn    418   131
ge-109/0/17    AddComplete    None          Ready         Up/Dn    419   130
ge-109/0/18    AddComplete    None          Ready         Up/Dn    420   133
ge-109/0/19    AddComplete    None          Ready         Up/Dn    421   132
ge-109/0/2     AddComplete    None          Ready         Up/Dn    404   117
ge-109/0/20    AddComplete    None          Ready         Up/Dn    422   127
ge-109/0/21    AddComplete    None          Ready         Up/Dn    423   126
ge-109/0/22    AddComplete    None          Ready         Up/Dn    424   129
ge-109/0/23    AddComplete    None          Ready         Up/Dn    425   128
ge-109/0/24    AddComplete    None          Ready         Up/Dn    426   103
ge-109/0/25    AddComplete    None          Ready         Up/Dn    427   102
ge-109/0/26    AddComplete    None          Ready         Up/Dn    428   105
ge-109/0/27    AddComplete    None          Ready         Up/Dn    429   104
ge-109/0/28    AddComplete    None          Ready         Up/Dn    430   107
ge-109/0/29    AddComplete    None          Ready         Up/Dn    431   106
ge-109/0/3     AddComplete    None          Ready         Up/Dn    405   116
ge-109/0/30    AddComplete    None          Ready         Up/Dn    432   109
ge-109/0/31    AddComplete    None          Ready         Up/Dn    433   108
```

```
ge-109/0/32    AddComplete    None          Ready         Up/Dn    434   135
ge-109/0/33    AddComplete    None          Ready         Up/Dn    435   134
ge-109/0/34    AddComplete    None          Ready         Up/Dn    436   137
ge-109/0/35    AddComplete    None          Ready         Up/Dn    437   136
ge-109/0/36    AddComplete    None          Ready         Up/Dn    438   144
ge-109/0/37    AddComplete    None          Ready         Up/Dn    439   143
ge-109/0/38    AddComplete    None          Ready         Up/Dn    440   146
ge-109/0/39    AddComplete    None          Ready         Up/Dn    441   145
ge-109/0/4     AddComplete    None          Ready         Up/Dn    406   119
ge-109/0/40    AddComplete    None          Ready         Up/Dn    442   140
ge-109/0/41    AddComplete    None          Ready         Up/Dn    443   139
ge-109/0/42    AddComplete    None          Ready         Up/Dn    444   142
ge-109/0/43    AddComplete    None          Ready         Up/Dn    445   141
ge-109/0/44    AddComplete    None          Ready         Up/Dn    446   148
ge-109/0/45    AddComplete    None          Ready         Up/Dn    447   147
ge-109/0/46    AddComplete    None          Ready         Up/Dn    448   150
ge-109/0/47    AddComplete    None          Ready         Up/Dn    449   149
ge-109/0/5     AddComplete    None          Ready         Up/Dn    407   118
ge-109/0/6     AddComplete    None          Ready         Up/Dn    408   121
ge-109/0/7     AddComplete    None          Ready         Up/Dn    409   120
ge-109/0/8     AddComplete    None          Ready         Up/Dn    410   111
ge-109/0/9     AddComplete    None          Ready         Up/Dn    411   110
ge-110/0/0     AddComplete    None          Ready         Up/Up    728   115
ge-110/0/1     AddComplete    None          Ready         Up/Dn    729   114
```

Meaning

The output confirms:

- That an extended port is recognized by the aggregation device. All extended ports are listed in the `Name` column of the output.
- That the listed extended ports have been added to the Junos Fusion, as shown by the `AddComplete` output in the `State` column.
- The administrative and operational state of each extended port. An extended port is operating correctly when the `Admin State` and `Op State` outputs are both in the `Up` state.

Verifying the Satellite Software Version

IN THIS SECTION

Purpose

Verify the satellite software versions available on the aggregation device in a Junos Fusion.

Action

Enter the `show chassis satellite software` command on the aggregation device.

```
user@aggregation-device> show chassis satellite software
Version                         Platforms           Group
3.0R1.1                          i386 ppc            group1
                                                    group2
                                                    group3
                                                    group4
                                                    group5
3.0R1.0                          i386 ppc
```

For more detailed output, you can also enter the `show chassis satellite software detail` on the aggregation device.

```

Software package version: 3.0R1.6
Platforms supported by package: i386 ppc arm arm563xx
  Platform      Host Version  Models Supported
  i386          3.0.3         QFX5100-24Q-2P
                              QFX5100-48C-6Q
                              QFX5100-48S-6Q
                              QFX5100-48T-6Q
                              QFX5100-96S-8Q
                              QFX5100-48SH-6Q
                              QFX5100-48TH-6Q
  ppc           1.1.2         EX4300-24P
                              EX4300-24T
                              EX4300-48P
                              EX4300-48T
                              EX4300-48T-BF
                              EX4300-48T-DC
                              EX4300-48T-DC-BF
  arm           1.0.0         EX2300-24P
                              EX2300-24T-DC
                              EX2300-C-12T
                              EX4300-C-12P
  arm563xx      1.0.0         EX3400-24P
                              EX3400-24T
                              EX3400-48T
                              EX3400-48P
Current Groups: group1
                group2
                group3
                group4
                group5
```

Meaning

The version of satellite software installed is displayed in the `Version` or `Software package version` column, and the satellite software upgrade group associated with each version of satellite software is listed in the `Group` or `Current Groups` output.

Verifying the Devices and Software Used in a Satellite Software Upgrade Group

IN THIS SECTION

Purpose

Verify the satellite software upgrade groups in the Junos Fusion, and which satellite devices are part of which satellite software upgrade groups.

A satellite software upgrade group can be a user configured group or the name of a satellite device cluster.

Action

Enter the `show chassis satellite upgrade-group` command on the aggregation device.

show chassis satellite upgrade-group

```
user@aggregation-device> show chassis satellite upgrade-group
                                              Group              Device
Group         Sw-Version                      State      Slot    State
__ungrouped__
group1        3.0R1.1                         in-sync    107     version-in-sync
                                                         108     version-in-sync
                                                         109     version-in-sync
                                                         110     version-in-sync
                                                         111     version-in-sync
                                                         112     version-in-sync
                                                         113     version-in-sync
group2        3.0R1.1                         in-sync    102     version-in-sync
                                                         103     version-in-sync
                                                         104     version-in-sync
                                                         105     version-in-sync
                                                         106     version-in-sync
                                                         114     version-in-sync
```

Meaning

The output shows that two satellite software upgrade groups—`ex4300` and `qfx`—have been created, and that both are using satellite software version 1.0R1.1. The `Group Slot` output shows which satellite devices—listed by FPC slot ID number—are in which software group, and the `Device State` output showing `version-in-sync` confirms that the satellite devices are running the satellite software that is associated with the satellite software upgrade group.

RELATED DOCUMENTATION

Configuring Junos Fusion Provider Edge

Configuring or Expanding a Junos Fusion Enterprise

Converting a Satellite Device in a Junos Fusion to a Standalone Device

IN THIS SECTION

In the event that you need to convert a satellite device to a standalone device, you will need to download and install a new Junos OS software package on the satellite device. The satellite device stops participating in the Junos Fusion topology once the software installation starts.

The following steps explain how to convert a satellite device that is participating in a Junos Fusion to a standalone device running Junos OS. If you have a standalone switch that is not part of a Junos Fusion but is running satellite software, and you want the switch to run Junos OS software, see "Installing Junos OS Software on a Standalone Device Running Satellite Software" on page 128.

NOTE: The QFX5100-48SH and QFX5100-48TH switch models are shipped from the factory with satellite device software. You cannot convert these switches to become standalone devices.

Conversion of EX2300 and EX3400 switches from satellite devices to standalone devices cannot be initiated from the aggregation device. To install Junos OS software on an EX2300 or EX3400 switch acting as a satellite device, see "Installing Junos OS Software on a Standalone Device Running Satellite Software" on page 128.

Download Junos OS Software

Before you install a new Junos OS software package on a satellite device, make sure you download the correct software package for that device:

- If the satellite device is a QFX5110, QFX5200 or EX4300 switch, you install a standard, signed **jinstall** version of Junos OS.

- If the satellite device is a QFX5100 switch that can be converted to a standalone device, you must install a Preboot eXecution Environment (PXE) version of Junos OS. The PXE version of Junos OS software supports the same feature set as the other Junos OS software packages for a release, but is specially engineered to install Junos OS onto a device running satellite software. The PXE Junos OS package name uses the format **install-media-pxe-qfx-5-*version*-domestic.tgz**.

- For Junos Fusion systems running Junos OS Release 17.2R1 and later, if the satellite device is a QFX5100 switch that can be converted to a standalone device, you must install a signed PXE version of Junos OS to convert the satellite device running satellite software to a standalone device running Junos OS software. The signed PXE Junos OS package name uses the format **install-media-pxe-qfx-5-*version*-domestic-signed.tgz**.

To download the version of Junos OS that you want to run on the satellite device after removing it from the Junos Fusion:

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology** > **Junos Platform** > **Junos Fusion** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the version of Junos OS that you want to run on the satellite device after removing it from the Junos Fusion.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the routing platform or to your internal software distribution site.

Disable the Automatic Conversion Configuration

Before removing a satellite device from an operational Junos Fusion, you must disable the configuration for automatic satellite conversion. If automatic satellite conversion is enabled for the FPC slot ID, the Junos OS installation cannot proceed.

For example, the following installation on an EX4300 satellite device is blocked:

```
[edit]
user@aggregation-device> request chassis satellite install fpc-slot 103 /var/tmp/jinstall-
```

```
ex-4300-14.1X53-D43.7-domestic-signed.tgz
Convert satellite device to Junos standalone device? [yes,no] (no) yes
```

```
Verified jinstall-ex-4300-14.1X53-D43.7-domestic.tgz signed by PackageProductionEc_2017 method
ECDSA256+SHA256
Satellite 103 is configured in the auto-satellite-conversion list
Please remove it from the list before converting to standalone
```

You can check the automatic satellite conversion configuration by entering the `show` statement at the `[edit chassis satellite-management auto-satellite-conversion]` hierarchy level.

1. If automatic satellite conversion is enabled for the satellite device's FPC slot ID, remove the FPC slot ID from the automatic satellite conversion configuration.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite slot-id
   ```

   For example, to remove FPC slot ID 103 from the Junos Fusion.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite 103
   ```

2. Commit the configuration.

   - To commit the configuration to a single Routing Engine only:

     ```
     [edit]
     user@aggregation-device# commit
     ```

   - To commit the configuration to all Routing Engines in multiple-aggregation device topology:

     ```
     [edit]
     user@aggregation-device# commit synchronize
     ```

Install Junos OS Software on the Satellite Device

1. To install the Junos OS software on the satellite device to convert the device to a standalone device, use the following CLI command:

   ```
   [edit]
   user@aggregation-device> request chassis satellite install fpc-slot slot-id URL-to-software-
   package
   ```

   For example, to install a software package stored in the `var/tmp` folder on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 103:

   ```
   [edit]
   user@aggregation-device> request chassis satellite install fpc-slot 103 /var/tmp/jinstall-
   ex-4300-14.1X53-D43.7-domestic-signed.tgz
   Convert satellite device to Junos standalone device? [yes,no] (no) yes
   ```

   ```
   Verified jinstall-ex-4300-14.1X53-D43.7-domestic.tgz signed by PackageProductionEc_2017
   method ECDSA256+SHA256
   Initiating Junos standalone conversion on device 103...
   Response from device:   Conversion started
   ```

   NOTE: If you are converting a QFX5100 switch and the Junos Fusion is running a Junos OS release earlier than 17.2R1, you must install the unsigned PXE software package on the QFX5100 switch:

   ```
   [edit]
   user@aggregation-device> request chassis satellite install fpc-slot 103 /var/tmp/
   install-media-pxe-qfx-5-14.1X53-D43.7-domestic.tgz
   ```

   The satellite device stops participating in the Junos Fusion topology once the software installation starts. The software upgrade starts after this command is entered.

2. To check the progress of the conversion, issue the `show chassis satellite fpc-slot` command:

   ```
   [edit]
   user@aggregation-device> show chassis satellite fpc-slot 103 extensive
                               Device          Cascade      Port        Extended
   Alias               Slot    State           Ports        State       Ports
   ex4300-24t-16       103     Online          xe-1/0/3     online      52/29
   ```

```
    xe-2/0/3     online

When                 Event                        Action
Nov 30 15:48:22.914  Rx SW-Update JSON-RPC response Conversion started
Nov 30 15:47:54.375  Start-SW-Update              Junos conversion
```

3. Wait for the reboot that accompanies the software installation to complete.
4. When you are prompted to log back into your device, uncable the device from the Junos Fusion topology. See *Remove a Transceiver*. Your device has been removed from Junos Fusion.

> **NOTE**: The device uses a factory-default configuration after the Junos OS installation is complete.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.2R1	For Junos Fusion systems running Junos OS Release 17.2R1 and later, if the satellite device is a QFX5100 switch that can be converted to a standalone device, you must install a signed PXE version of Junos OS to convert the satellite device running satellite software to a standalone device running Junos OS software.

RELATED DOCUMENTATION

Understanding Software in a Junos Fusion Provider Edge

Understanding Software in a Junos Fusion Enterprise

Installing Junos OS Software on a Standalone Device Running Satellite Software

This process should be used when you have a standalone switch running satellite software and you want the switch to run Junos OS software. A standalone device is running satellite software for one of the following reasons:

- It was removed from a Junos Fusion without following the instructions in "Converting a Satellite Device in a Junos Fusion to a Standalone Device" on page 124, which include a Junos OS installation.

- Satellite software was installed on the device but the device was never provisioned into a Junos Fusion.

> **NOTE**: If you are removing a satellite device from a Junos Fusion, you must first make sure that automatic satellite conversion is disabled for the satellite device’s FPC slot ID. See "Converting a Satellite Device in a Junos Fusion to a Standalone Device" on page 124.

To install Junos OS onto a QFX5100, QFX5100 or QFX5200 switch running satellite software:

- Select a Junos OS image that meets the satellite software to Junos OS conversion requirements. See Junos Fusion Hardware and Software Compatibility Matrices for satellite software to Junos OS conversion requirements.

- Copy the Junos OS image onto a USB flash drive and use the USB flash drive to install the Junos OS. See Performing a Recovery Installation Using an Emergency Boot Device.

To install Junos OS onto an EX4300 switch running satellite software:

1. Log in to the console port of your switch.

2. Power off the switch, and power it back on.

3. While the switch is powering back on, enter the UBoot prompt (=>) by pressing Ctrl+C on your keyboard.

4. From the Uboot prompt, set the operating system environment mode on the switch to Junos. Save the configuration and reset the kernel:

```
=> setenv osmode junos
=> setenv snos_previous_boot 0
=> save
=> reset
```

   After the reset operation completes, the loader prompt (`loader>`) appears.

5. Install Junos OS using a USB flash drive from the loader prompt. See Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive.

To install Junos OS onto an EX2300 or EX3400 switch running satellite software:

- Log in to the satellite software (SNOS) on the switch to be converted back to Junos OS and use the following sequence of commands to install the Junos package:

```
#######################################
dd bs=512 count=1 if=/dev/zero of=/dev/sda
echo -e "o\nn\np\n1\n\n\nw" | fdisk /dev/sda
mkfs.vfat /dev/sda1
fw_setenv target_os
reboot
##################################
>>Get to the loader prompt
##################################
loader> install --format tftp://<tftp server>/<Junos package name>
```

RELATED DOCUMENTATION

Understanding Junos Fusion Enterprise Software and Hardware Requirements

Junos Fusion Hardware and Software Compatibility Matrices

Converting a Satellite Device in a Junos Fusion to a Standalone Device | 124

CHAPTER 5

Junos Fusion Enterprise Operational Commands

CHAPTER 6

Enabling Layer 3 Support in a Junos Fusion Enterprise

IN THIS CHAPTER

Understanding Integrated Routing and Bridging (IRB) Interfaces in a Junos Fusion Enterprise

In most campus networking environments, endpoint devices must have a path to send and receive Layer 3 traffic.

In a typical Junos Fusion Enterprise deployment, the EX9200 switch assumes the responsibilities of an aggregation layer switch and is typically the gateway to layer 3. Integrated routing and bridging (IRB) interfaces are, therefore, configured on the EX9200 switches acting as aggregation devices to move traffic between Layer 2 and Layer 3.

See Understanding Integrated Routing and Bridging for information on configuring IRB interfaces.

See the Adding Layer 3 Support to a Junos Fusion Enterprise section of the Enabling Junos Fusion Enterprise on an Enterprise Campus Network for a sample IRB interface configuration in a Junos Fusion Enterprise.

RELATED DOCUMENTATION

Understanding Integrated Routing and Bridging

CHAPTER 7

802.1X in a Junos Fusion Enterprise

IN THIS CHAPTER

Understanding 802.1X on a Junos Fusion Enterprise

This topic describes 802.1X in a Junos Fusion Enterprise.

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN. The 802.1X authentication feature is based upon the IEEE 802.1X standard Port-Based Network Access Control.

The range of 802.1X configuration options are beyond the scope of this document. For additional information on 802.1X, see 802.1X for Switches Overview and the Access Control User Guide for EX9200 Switches.

The following requirements should be understood when configuring 802.1X for a Junos Fusion Enterprise:

- The authentication server cannot connect to the Junos Fusion Enterprise through an extended port.

- 802.1X configuration must match on both aggregation devices in a Junos Fusion Enterprise. 802.1X , therefore, should typically be configured using configuration groups that are applied to both aggregation devices using commit synchronization. See "Understanding Configuration Synchronization in a Junos Fusion" on page 27 and "Enabling Configuration Synchronization Between Aggregation Devices in a Junos Fusion" on page 88.

- 802.1X control is handled by either aggregation device on a per-session basis. Either aggregation device can act as the primary device for 802.1X control for any 802.1X session. If traffic flow through one aggregation device is disrupted during an 802.1X session, the 802.1X session may be interrupted and control could be transferred to the other aggregation device.

- A captive portal cannot be configured on an extended port.

See Enabling 802.1X in the Enabling Junos Fusion Enterprise on an Enterprise Campus Network document for an example of 802.1X configuration on a Junos Fusion Enterprise.

CHAPTER 8

Junos Fusion Enterprise Half-Duplex Links on Satellite Devices

IN THIS CHAPTER

Understanding Half-Duplex Links on Satellite Devices in a Junos Fusion Enterprise

IN THIS SECTION

This topic describes half-duplex links on satellite devices in a Junos Fusion Enterprise.

This topic covers:

Half-Duplex Links on Satellite Devices Overview

Half-duplex communication is supported on all built-in network copper ports on EX2300, EX3400, and EX4300 satellite devices in a Junos Fusion Enterprise (JFE). *Half-duplex* is bidirectional communication, but signals can flow in only one direction at a time. *Full-duplex* communication means that both ends of the communication can send and receive signals at the same time.

The built-in network copper ports are configured by default as full-duplex 1-gigabit links with autonegotiation. If the link partner is set to autonegotiate the link, then the link is autonegotiated to full duplex or half-duplex. If the link is not set to autonegotiation, then the satellite-device link defaults to half-duplex unless the interface is explicitly configured for full duplex.

On EX2300, EX3400, and EX4300 satellite devices, the link mode is handled as follows:

- If the link partner is operating in half-duplex, the satellite device interface goes to half-duplex.
- If the link partner is not capable of autonegotiation, the satellite device interface goes to half duplex.
- If the link partner is capable of autonegotiation and is operating in full duplex, the satellite device interface also works in full duplex.

Understanding Configuration of Full-Duplex Link Mode on a Satellite Device and Verification of Half-Duplex Mode

Like all features in a Junos Fusion Enterprise, link modes are configured and verified from the aggregation devices.

To explicitly configure full duplex:

```
[edit]
user@aggregation-device# set interfaces interface-name link-mode full-duplex
```

To verify a half-duplex setting:

```
user@aggregation-device> show interfaces interface-name  extensive
```

RELATED DOCUMENTATION

Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support

CHAPTER 9

Junos Fusion Enterprise Network Monitoring and Analyzers

IN THIS CHAPTER

Understanding sFlow Technology on a Junos Fusion Enterprise

IN THIS SECTION

This topic describes sFlow technology in a Junos Fusion Enterprise.

This topic covers:

sFlow Technology on a Junos Fusion Enterprise Overview

sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow technology randomly samples network packets and sends the samples to a monitoring system. In a Junos Fusion Enterprise, you can configure sFlow technology on the aggregation device to continuously monitor traffic on all extended interfaces simultaneously.

Many sFlow technology concepts for standalone switches also apply to sFlow technology on a Junos Fusion Enterprise. See Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch for a detailed overview of sFlow on standalone EX Series switches.

Understanding the sFlow Sampling Mechanism on a Junos Fusion Enterprise

sFlow technology uses the following two sampling mechanisms:

- Packet-based sampling: Samples one packet out of a specified number of packets from an interface enabled for sFlow technology.
- Time-based sampling: Samples interface statistics at a specified interval from an interface enabled for sFlow technology.

The sampling information is used to create a network traffic visibility picture. The Juniper Networks Junos operating system (Junos OS) fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

NOTE: sFlow technology on the switches samples only raw packet headers. A raw Ethernet packet is the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent (embedded in the switch), and a centralized collector. The sFlow agent’s two main activities are random sampling and statistics gathering. The sFlow agent combines interface counters and flow samples and sends them across the network to the sFlow collector in UDP datagrams, directing those datagrams to the IP address and UDP destination port of the collector. Each datagram contains the following information:

- The IP address of the sFlow agent
- The number of samples
- The interface through which the packets entered the agent
- The interface through which the packets exited the agent
- The source and destination interface for the packets
- The source and destination VLAN for the packets

Like all features in a Junos Fusion Enterprise, sFlow technology is configured from the aggregation devices.

BEST PRACTICE: We recommend the following consideration guidelines for sFlow technology in a Junos Fusion Enterprise:

- Configure sFlow technology on both aggregation devices.
- Configure the same sampling rates on all the extended ports. If you configure different sampling rates, then the lowest value is used for all ports. Note that counter samples are sent from both aggregation devices for an extended port.
- Use the configuration sync feature to synchronize the configuration across the aggregation devices.
- After synchronization is finished, make sure that the collector is reachable from both aggregation devices.

Limitations for sFlow on a Junos Fusion Enterprise

Consider the following limitations when you configure sFlow technology on a Junos Fusion Enterprise:

- You cannot configure sFlow technology on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.
- You cannot configure sFlow technology on a cascade port.
- When using the configuration sync feature, sFlow collector statistics are not synced between the aggregation devices.
- Adaptive sampling is not supported for extended ports. Given this limitation, make sure that you configure the appropriate sampling rate for your configuration so that there is no congestion for CPU traffic.

Understanding Port Mirroring Analyzers on a Junos Fusion Enterprise

IN THIS SECTION

This topic describes port mirroring analyzers in a Junos Fusion Enterprise.

This topic covers:

Port Mirroring Analyzers on a Junos Fusion Enterprise Overview

Port mirroring can be used for traffic analysis on routers and switches that, unlike hubs, do not broadcast packets to every port on the destination device. Port mirroring sends copies of all packets or policy-based sample packets to local or remote analyzers where you can monitor and analyze the data.

In a Junos Fusion Enterprise, analyzers are used to mirror traffic from an extended port on a satellite device to an output interface or VLAN. The output interface or VLAN can be connected to the aggregation device or to an extended port on a satellite device.

You can configure an analyzer to mirror:

- Bridged packets (Layer 2 packets)
- Routed packets (Layer 3 packets)

Many port mirroring analyzer concepts for standalone switches also apply to port mirroring analyzers on Junos Fusion Enterprise. See Understanding Port Mirroring Analyzers for a detailed overview of port mirroring analyzers on standalone switches.

Understanding the Configuration of Analyzers in a Junos Fusion Enterprise

Like all features in a Junos Fusion Enterprise, port mirroring analyzers are configured from the aggregation devices.

The mirroring options in a Junos Fusion Enterprise are:

- Mirror traffic from a native interface to an extended port.
- Mirror traffic from an extended port on one satellite device to an extended port on another satellite device.
- Mirror traffic from an extended port to a native interface. Configure remote mirroring for this scenario—that is, configure an analyzer output VLAN with an ICL and a native interface as remote-mirroring VLAN members in one aggregation device and an ICL as a remote-mirroring VLAN member in the peer aggregation device, so that both aggregation devices can mirror to the native interface.

> **NOTE**: Even if the mirroring source and destination are on the same satellite device, the mirrored traffic always goes back to the aggregation device.

BEST PRACTICE: We recommend the following configuration guidelines for analyzers in a Junos Fusion Enterprise:

- Configure remote mirroring.
- Configure an analyzer output VLAN with both an ICL (interchassis link) and the mirror destination as VLAN members, so that mirrored traffic can travel through the ICL to the peer aggregation device if the mirror destination is not directly reachable on the local aggregation device. This is applicable in scenarios where the mirror destination is single-homed or a dual-homed satellite device and the cascade port is down on the local aggregation device.
- Use the configuration sync feature to synchronize the configuration across aggregation devices.

Limitations for Port Mirroring Analyzers on a Junos Fusion Enterprise

Consider the following limitations when you configure port mirroring analyzers on a Junos Fusion Enterprise:

- You cannot mirror a cascade port or an ICL. (See the configuration guidelines in Understanding Port Mirroring Analyzers for other port types that cannot be mirrored.)
- An analyzer input VLAN mirrors all interfaces in the VLAN *except* the ICL in the VLAN. This limitation keeps mirrored traffic from causing congestion in the ICL.

RELATED DOCUMENTATION

Understanding Port Mirroring Analyzers

CHAPTER 10

Junos Fusion Enterprise Private VLANs

IN THIS CHAPTER

Understanding Private VLANs on a Junos Fusion Enterprise

IN THIS SECTION

This topic describes private VLANs (PVLANs) in a Junos Fusion Enterprise.

This topic covers:

PVLANs on a Junos Fusion Enterprise Overview

Junos Fusion Enterprise (JFE) supports private VLANs (PVLANs). PVLANs on a Junos Fusion Enterprise are an extension of PVLANs on standalone switches that enables PVLANs on extended ports on satellite devices.

PVLANs are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the known communication between known hosts. PVLAN is a standard introduced by RFC 5517 to achieve port or device isolation in a Layer 2 VLAN by partitioning a VLAN broadcast domain (also called a *primary VLAN*) into smaller subdomains (also called *secondary VLANs*).

PVLANs can be used for such purposes as:

- To help ensure the security of service providers sharing a server farm
- To provide security to subscribers of various service providers sharing a common metropolitan area network
- To achieve isolation within the same subnet in a very large enterprise network

In a Junos Fusion Enterprise, PVLANs can be configured on ports belonging to the aggregation device or to an extended port on a satellite device.

PVLAN concepts for standalone switches apply to PVLANs on a Junos Fusion Enterprise. See Understanding Private VLANs.

NOTE: Some “Guidelines and Restrictions for PVLANs” in Understanding Private VLANs, however, do not apply to PVLANs on a Junos Fusion Enterprise for the following reasons:

- Restrictions on use of MSTP and VSTP—Spanning-tree protocols are not supported on Junos Fusion Enterprise.
- Restrictions on use of mac-table-size, *no-mac-learning*, *mac-statistics*, and interface-mac-limit—These statements are not supported on Junos Fusion Enterprise.

Understanding the Configuration of PVLANs in a Junos Fusion Enterprise

Like all features in a Junos Fusion Enterprise, PVLANs are configured from the aggregation devices.

Junos Fusion Enterprise PVLAN topologies support the following:

- Multiple satellite devices can be clustered into a group and cabled into the JFE as a group instead of as individual satellite devices.
- Aggregation device *native ports* (that is, ports on the aggregation device that are not acting as cascade ports) or satellite device extended ports can act as promiscuous ports, isolated ports, or community VLAN ports. See Understanding Private VLANs for definitions of PVLAN port types. These port types are also described in RFC 5517.
- The promiscuous port can be attached to a core switch or router through physical interfaces or aggregated links.
- PVLANs are supported in dual aggregation device JFEs.

BEST PRACTICE: We recommend the following configuration guidelines for PVLANs in a Junos Fusion Enterprise:

- In a dual-aggregation device JFE, we recommend that you use the interchassis link (ICL) as the inter-switch link for PVLAN inter-switching. Although any port link in the JFE *could* serve as the inter-switch link, the high-bandwidth requirements on the inter-switch link make the ICL the best choice.

- PVLAN ports can span across the switches in the JFE. We recommend that you interconnect 10-gigabit or 40-gigabit ports as they provide the high bandwidth needed for PVLAN trunk traffic.

Limitations for PVLANs on a Junos Fusion Enterprise

Consider the following limitations when you configure PVLANs on a Junos Fusion Enterprise:

- PVLANs on a JFE do not work if local switching is enabled on satellite devices.

- You cannot change the role of a PVLAN bridge domain from primary VLAN to secondary VLAN or the reverse in a single commit cycle.

- Protocols configured per VLAN cannot be configured on secondary VLANs. Secondary VLANs inherit protocol configurations from the primary VLAN.

RELATED DOCUMENTATION

Understanding Private VLANs

CHAPTER 11

Power over Ethernet, LLDP, and LLDP-MED on Junos Fusion Enterprise

IN THIS CHAPTER

Understanding Power over Ethernet in a Junos Fusion

IN THIS SECTION

This topic describes Power over Ethernet (PoE) in a Junos Fusion.

This topic covers:

Power over Ethernet in a Junos Fusion Overview

Power over Ethernet (PoE) enables electric power, along with data, to be passed over a copper Ethernet LAN cable. Powered devices—such as *VoIP* telephones, wireless access points, video cameras, and point-of-sale devices—that support PoE can receive power safely from the same access ports that are used to connect personal computers to the network. This reduces the amount of wiring in a network, and it also eliminates the need to position a powered device near an AC power outlet, making network design more flexible and efficient.

In a Junos Fusion, PoE is used to carry electric power from an extended port on a satellite device to a connected device. An extended port is any network-facing port on a satellite device in a Junos Fusion.

Many PoE concepts for standalone switches also apply to PoE on Junos Fusion. See Understanding PoE on EX Series Switches for a detailed overview of PoE on standalone EX Series switches.

Understanding the Role of the Aggregation Devices for PoE Support in a Junos Fusion

An aggregation device is responsible for configuring, monitoring, and maintaining all configurations for all extended ports in a Junos Fusion, including PoE. Therefore, all commands used to configure, monitor, and maintain PoE in a Junos Fusion are entered from the aggregation device.

An extended port on the satellite device must support PoE to enable PoE in a Junos Fusion. No hardware limitations for PoE support are introduced by the aggregation device in a Junos Fusion.

NOTE: PoE is supported in a Junos Fusion Provide Edge and a Junos Fusion Enterprise despite not being supported in MX series routers or standalone EX9200 switches. All MX series routers and EX9200 switch models, when configured into the aggregation device role in a Junos Fusion , can enable PoE Junos Fusion because the PoE hardware support is supported on the satellite devices.

Understanding the Role of the Satellite Devices for PoE Support in a Junos Fusion

A satellite device in a Junos Fusion provides PoE hardware support in a Junos Fusion. Each satellite device in a Junos Fusion that supports PoE has its own PoE controller. The PoE controller keeps track of the PoE power consumption on the satellite device and allocates power to PoE extended ports. The maximum PoE power consumption for a satellite device—the total amount of power available for the satellite device's PoE controller to allocate to all of the satellite device's PoE interfaces—is determined individually by the switch model of the satellite devices and by the power supply or supplies installed in that satellite device.

In allocating power, the satellite device's PoE controller cannot exceed the satellite device's maximum PoE power availability.

The maximum PoE power consumption varies by satellite device in a Junos Fusion , because the hardware specifications of the satellite devices determine the maximum PoE power availability.

See Understanding PoE on EX Series Switches for a listing of the PoE power consumption limit for each EX Series switch model and power supply configuration.

Understanding PoE Configuration in a Junos Fusion

Like all features in a Junos Fusion, PoE is configured from the aggregation devices.

In dual aggregation device topologies, the PoE configurations should match identically on both aggregation devices.

PoE in a Junos Fusion works by periodically checking the PoE configuration on each aggregation device, and updating the configuration when a PoE change is identified. If the aggregation devices have different PoE configurations, the PoE configurations for the Junos Fusion will continually change because the Junos Fusion always uses the PoE configuration of the last aggregation device that was checked.

Understanding PoE Support Standards for Extended Ports in a Junos Fusion

The extended port hardware—specifically, the extended port hardware interface on the satellite device in the Junos Fusion —must support PoE to enable PoE in a Junos Fusion.

All extended ports that support PoE on satellite devices in a Junos Fusion support the IEEE 802.3at PoE + standard. The IEEE 802.3at PoE+ standard allows an extended port that supports PoE to provide up to 30 W of power to a connected device.

Understanding Maximum PoE Power Budgets in a Junos Fusion

The maximum PoE power budgets are determined for each individual satellite device in a Junos Fusion.

Maximum PoE power budgets for a satellite device vary by the switch model and power supply configuration of the satellite device.

To learn the maximum PoE power supply budget for a satellite device:

- See Understanding PoE on EX Series Switches for a table of maximum power supply budgets by switch device model.
- Enter the **show poe controller** command from your aggregation device and view the Maximum Power output.

Understanding PoE Controller Software in a Junos Fusion

All switches that support PoE have a PoE controller that runs PoE controller software, including switches acting as satellite devices in a Junos Fusion.

PoE controller software is bundled with Junos OS. PoE controller software should be updated before installing a switch as a satellite device in a Junos Fusion.

For information on PoE controller software requirements in a Junos Fusion Enterprise, see Understanding Junos Fusion Enterprise Software and Hardware Requirements.

For information on PoE controller software requirements in a Junos Fusion Provider Edge, see *Understanding Junos Fusion Provider Edge Software and Hardware Requirements*

For information on checking or upgrading the PoE controller software version, see Upgrading the PoE Controller Software.

Understanding PoE Power Allocation Configuration Options in a Junos Fusion

Junos Fusion supports several optional features that help manage PoE power allocation on the satellite devices.

The PoE power allocation options are discussed in greater detail in Understanding PoE on EX Series Switches.

RELATED DOCUMENTATION

Configuring Power over Ethernet in a Junos Fusion | 150

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure) | 155

Understanding LLDP and LLDP-MED on a Junos Fusion

IN THIS SECTION

This topic describes Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) in a Junos Fusion.

This topic covers:

LLDP and LLDP-MED in a Junos Fusion Overview

LLDP and LLDP-MED are used to learn and distribute device information on network links. The information enables the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Junos operating system (Junos OS).

Many LLDP and LLDP-MED concepts for standalone EX Series switches that support the features also apply to LLDP and LLDP-MED on Junos Fusion. See Understanding LLDP and LLDP-MED on EX Series Switches for a detailed overview of LLDP and LLDP-MED on standalone EX Series switches.

NOTE: LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone. LLDP-MED is an important access layer switch feature that is supported in a Junos Fusion despite not being supported on a standalone EX9200 switch.

Understanding LLDP and LLDP-MED Configuration and Traffic Handling in a Junos Fusion

LLDP and LLDP-MED traffic is generally handled the same in a Junos Fusion or a standalone series switch. LLDP and LLDP-MED configuration on an extended port in a Junos Fusion is identical for a standalone EX Series switch. See Configuring LLDP (CLI Procedure) or Configuring LLDP-MED (CLI Procedure).

The following specifications apply to the device information transmitted by LLDP and LLDP-MED in a Junos Fusion topology with two or more aggregation devices:

- Management address TLVs are merged into a single packet in such a way that the packet contains two or more management address TLVs.

- The SNMP index used as the port ID TLV is derived so that all aggregation devices receive the same index value for port IDs of extended ports.

- The system name for extended ports is the configured redundancy group name. A redundancy group has to be configured in order to enable a topology with two or more aggregation devices.

- The chassis ID is the same for all aggregation devices. If a system MAC address is defined for the redundancy group, is it used as the chassis ID. The system MAC address is configured using the `set chassis satellite-management redundancy-groups` *`redundancy-group-name`* `system-mac-address` *`system-mac-address`* command. If the system MAC is not configured, the chassis ID is the default MAC address, which is 00:00:00:00:00:01.

  BEST PRACTICE: We recommend specifying a system MAC address if you are running LLDP or LLCP-MED traffic in your Junos Fusion topology.

RELATED DOCUMENTATION

Configuring LLDP (CLI Procedure)

Configuring LLDP-MED (CLI Procedure)

Configuring Power over Ethernet in a Junos Fusion

IN THIS SECTION

PoE Configurable Options

Table 12 on page 151 shows the configurable PoE options and their default settings in a Junos Fusion.

Some PoE options can be configured globally and per interface. In cases where a PoE interface setting is different from a global PoE setting, the PoE interface setting is configured on the interface.

Table 12: Configurable PoE Options and Default Settings

Option	Default	Description
disable (Power over Ethernet)	Not included in default configuration. **NOTE**: PoE ports are disabled by default in a Junos Fusion.	Disables PoE on the interface if PoE was enabled. The interface maintains network connectivity but no longer supplies power to a connected powered device. Power is not allocated to the interface.
guard-band	**0** W	Reserves a specified amount of power from the PoE power budget for possible spikes in PoE power consumption. In a Junos Fusion, the guard band can be 0 to 19 W.
management	**class**	Sets the PoE power management mode for the extended port. The power management mode determines how power to a PoE extended port is allocated: • **class**—In this mode, the power allocated to a PoE extended port is determined by the class of the connected powered device. If there is no powered device connected, standard 15.4W power is allocated on the interface. • **static**—The maximum power delivered by an interface is statically configured and is independent of the class of the connected powered device. The maximum power is allocated to the interface even if a powered device is not connected.
maximum-power (Interface)	**30.0** W (PoE+, IEEE 802.3at)	Sets the maximum power that can be delivered by a PoE interface when the power management mode is **static**. In a Junos Fusion, all extended ports support PoE+ so the maximum power is up to 30 W. This setting is ignored if the power management mode is **class**.

Table 12: Configurable PoE Options and Default Settings *(Continued)*

Option	Default	Description
priority (Power over Ethernet)	**low**	Sets an interface’s power priority to either **low** or **high**. If power is insufficient for all PoE interfaces, the PoE power to low-priority interfaces is shut down before power to high-priority interfaces is shut down. Among interfaces that have the same assigned priority, the power priority is determined by port number, with lower-numbered ports having higher priority.

Enabling PoE

PoE is disabled by default for all extended ports in a Junos Fusion.

To enable PoE on all PoE-supported interfaces:

```
[edit]
user@aggregation-device# set poe interface all-extended
```

To enable PoE on a specific PoE-supported interface:

```
[edit]
user@aggregation-device# set poe interface interface-name
```

For instance, to enable PoE on extended port interface ge-100/0/24:

```
[edit]
user@aggregation-device# set poe interface ge-100/0/24
```

Disabling PoE

PoE is disabled by default in a Junos Fusion. Use this procedure to disable PoE in a Junos Fusion that has PoE previously enabled.

If PoE is enabled globally but disabled on a specific interface, PoE is disabled on the specified interface. This procedure can, therefore, be used to individually disable ports in cases where PoE is globally enabled.

If you want to disable PoE on all extended port interfaces in a Junos Fusion:

```
[edit]
user@aggregation-device# set poe interface all-extended disable
```

If you want to disable PoE on one extended port interface:

```
[edit]
user@aggregation-device# set poe interface interface-name disable
```

For instance, to disable PoE on extended port 101/0/1 in a Junos Fusion:

```
[edit]
user@aggregation-device# set poe interface 101/0/1 disable
```

If you want to enable PoE on all PoE-supported extended ports in a Junos Fusion except 101/0/10, enter the following commands:

```
[edit]
user@aggregation-device# set poe interface all-extendeduser@aggregation-device# set poe
interface 101/0/10 disable
```

Setting the Power Management Mode

The power management mode in a Junos Fusion is set for all extended ports in a Junos Fusion .

The default power management mode is class.

To set the power management mode to static for all PoE extended ports:

```
[edit]
user@aggregation-device# set poe management static
```

To set the power management mode back to class for all PoE extended ports:

```
[edit]
user@aggregation-device# set poe management class
```

Setting the Maximum Power That Can Be Delivered from a PoE Interface

To set the maximum power that can be delivered to a connected device using PoE when the power management mode is set to static:

```
[edit]
user@aggregation-device# set poe interface interface-name maximum-power watts
```

To configure all extended port interfaces to the same maximum power, enter **all-extended** as the *interface-name*.

For instance, to change the maximum power for all PoE extended ports configured in static power management mode to 25 watts:

```
[edit]
user@aggregation-device# set poe interface all-extended maximum-power 25
```

To change the maximum power for interface 101/0/1 to 25 watts:

```
[edit]
user@aggregation-device# set poe interface 101/0/1 maximum-power 25
```

Setting the Guard Band

One guard band is configured for all extended ports in a Junos Fusion.

To set the guard band for all extended ports in a Junos Fusion:

```
[edit]
user@aggregation-device# set poe guard-band watts
```

For instance, to set the guard-band to 19 watts for all PoE extended ports:

```
[edit]
user@aggregation-device# set poe guard-band 19
```

Setting the PoE Interface Priority

To set a PoE interface priority to high:

```
[edit]
user@aggregation-device# set poe interface interface-name priority high
```

For instance, to assign a high priority to interface 101/0/1:

```
[edit]
user@aggregation-device# set poe interface 101/0/1 priority high
```

To set a PoE interface priority to low:

```
[edit]
user@aggregation-device# set poe interface interface-name priority low
```

For instance, to assign a low priority to interface 102/0/1:

```
[edit]
user@aggregation-device# set poe interface 102/0/1 priority low
```

RELATED DOCUMENTATION

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure) | 155

Understanding Power over Ethernet in a Junos Fusion | 145

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure)

IN THIS SECTION

You can verify the Power over Ethernet (PoE) configuration and status on Junos Fusion.

This topic describes how to verify:

PoE Power Budgets, Consumption, and Mode on Satellite Devices

IN THIS SECTION

Purpose

Verify the PoE configuration and status, such as the PoE power budget, total PoE power consumption, power management mode, and the supported PoE standard.

Action

Enter the following command:

```
user@aggregation-device> show poe controller
```

```
Controller  Maximum   Power         Guard    Management   Status        Lldp
index       power     consumption   band                                Priority
 100        925.00W   0.00W          19W     Class        AT_MODE       Disabled
 120        125.00W   6.08W          19W     Class        AT_MODE       Disabled
```

Meaning

- Satellite device 100 has a PoE power budget of 925 W, of which 0 W were being used by the PoE extended ports at the time the command was executed. The Guard band field shows that 19 W of power is reserved out of the PoE power budget to protect against spikes in power demand. The power management mode is class. The PoE ports on the switch support PoE+ (IEEE 802.3at).
- Satellite device 120 has a PoE power budget of 125 W, of which 6.08 W were being used by the PoE extended ports at the time the command was executed. The Guard band field shows that 19 W of

power is reserved out of the PoE power budget to protect against spikes in power demand. The power management mode is class. The PoE ports on the switch support PoE+ (IEEE 802.3at).

PoE Interface Configuration and Status

IN THIS SECTION

Purpose

Verify that PoE interfaces are enabled and set to the correct maximum power and priority settings. Also verify current operational status and power consumption.

Action

To view configuration and status for all PoE interfaces, enter:

```
user@switch> show poe interface
Interface    Admin       Oper    Max        Priority       Power          Class
             status      status  power                     consumption
ge-100/0/0   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/1   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/2   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/3   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/4   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/5   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/6   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/7   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/8   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/9   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/10  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/11  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/12  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/13  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/14  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/15  Enabled     OFF     16.0W      Low            0.0W           not-applicable
```

```
ge-100/0/16  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/17  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/18  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/19  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/20  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/21  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/22  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/23  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/24  Enabled      ON     16.0W      Low            3.7W            2
ge-100/0/25  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/26  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/27  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/28  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/29  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/30  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/31  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/32  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/33  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/34  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/35  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/36  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/37  Enabled      ON     16.0W      Low            2.0W            0
ge-100/0/38  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/39  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/40  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/41  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/42  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/43  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/44  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/45  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/46  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-100/0/47  Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-120/0/0   Enabled      ON     16.0W      Low            3.9W            2
ge-120/0/1   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-120/0/2   Enabled     OFF     16.0W      Low            2.0W           not-applicable
ge-120/0/3   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-120/0/4   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-120/0/5   Enabled     OFF     16.0W      Low            0.0W           not-applicable
ge-120/0/6   Enabled      ON     16.0W      Low            0.0W            4
ge-120/0/7   Enabled     OFF     0.0W       Low            0.0W           not-applicable
ge-120/0/8   Enabled     OFF     0.0W       Low            0.0W           not-applicable
ge-120/0/9   Enabled     OFF     0.0W       Low            0.0W           not-applicable
ge-120/0/10  Enabled     OFF     0.0W       Low            0.0W           not-applicable
```

```
ge-120/0/11  Enabled     OFF     0.0W       Low             0.0W            not-applicable
<additional output removed for brevity>
```

To view configuration and status for a single PoE interface, enter:

```
user@switch> show poe interface ge-120/0/0
PoE interface status:
PoE interface                : ge-120/0/0
Administrative status        : Enabled
Operational status           :   ON
Power limit on the interface : 7.0W
Priority                     : Low
Power consumed               : 3.9W
Class of power device        :        2
PoE Mode                     :   802.3at
```

Meaning

The command output shows the status and configuration of interfaces. For example, the interface 120/0/0 is administratively enabled. Its operational status is **ON**; that is, the interface is currently delivering power to a connected powered device. The maximum power allocated to the interface is 7.0 W. The interface has a low PoE power priority. At the time the command was executed, the powered device was consuming 3.9 W. The class of the powered device is class 2. If the PoE power management mode is class, the class of the powered device determines the maximum power allocated to the interface, which is 7 W in the case of class 2 devices.

The PoE Mode field indicates that the interface supports IEEE 802.3at (PoE+).

RELATED DOCUMENTATION

Configuring Power over Ethernet in a Junos Fusion | **150**

Understanding Power over Ethernet in a Junos Fusion | **145**

CHAPTER 12

Configuration Statements and Operational Commands

IN THIS CHAPTER

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands

CHAPTER 13

Link Aggregation and LACP on Junos Fusion Enterprise

IN THIS CHAPTER

Configuring Link Aggregation on Satellite Devices in a Junos Fusion Enterprise

Link aggregation, as defined by IEEE 802.3ad, allows users to bundle multiple Ethernet interfaces into a single logical interface. An aggregated Ethernet interface, also known as a link aggregation group (LAG), balances traffic across its member links within the aggregated Ethernet bundle and effectively increases the uplink bandwidth. Aggregated Ethernet interfaces also increase high availability, because an aggregated Ethernet interface is composed of multiple member links that can continue to carry traffic when one member link fails.

In a Junos Fusion Enterprise, you can configure aggregated Ethernet interfaces using extended port member links to increase uplink bandwidth and high availability for endpoint devices connected to a satellite device. These aggregated Ethernet interfaces can be configured to use Link Aggregation Control Protocol (LACP).

LACP is a subcomponent of the IEEE 802.3ad standard that simplifies management of LAGs. LACP automates the addition and deletion of individual links to the LAG without user intervention, and can also prevent communication failures by detecting misconfigurations within a LAG. LACP-enabled devices exchange LACP protocol data units (PDUs) to monitor links between LAG peers. You can configure Ethernet links to actively transmit LACP PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when they receive them from another link.

LAG and LACP configuration on extended ports in a Junos Fusion Enterprise is identical for a standalone EX Series switch. The following guidelines apply to link aggregation in a Junos Fusion Enterprise:

- The member links must be located on the same satellite device.
- Up to 1000 LAGs are supported, with up to 16 members per LAG.
- LAGs are numbered from ae0 through ae4091.
- The LAG must be configured on both sides of the link.
- The interfaces on either side of the link must be set to the same speed and be in full-duplex mode.

To configure link aggregation in a Junos Fusion Enterprise:

1. Configure the maximum number of aggregated Ethernet interfaces:

```
[edit]
user@aggregation-device#  set chassis aggregated-devices ethernet device-count number
```

2. Create and name the aggregated Ethernet interface:

```
[edit]
user@aggregation-device#  set interfaces aex
```

> **NOTE**: Specify the aggregated Ethernet interface name as ae*x*, where *x* is the interface instance number. The instance number can be from 0 through 4091.

3. Assign interfaces to the aggregated Ethernet interface:

```
[edit]
user@aggregation-device# set interfaces interface-name ether-options 802.3ad aex
```

For example:

```
[edit]
user@aggregation-device# set interfaces xe-100/0/12 ether-options 802.3ad ae0
user@aggregation-device# set interfaces xe-100/0/13 ether-options 802.3ad ae0
user@aggregation-device# set interfaces xe-100/0/46 ether-options 802.3ad ae1
```

4. Enable LACP for the aggregated Ethernet interface:

```
[edit]
user@aggregation-device#  set interfaces aex aggregated-ether-options lacp
```

For information on configuring LACP parameters, see "Configuring Aggregated Ethernet LACP" on page 164.

RELATED DOCUMENTATION

Configuring an Aggregated Ethernet Interface | **163**

Configuring Aggregated Ethernet LACP | **164**

Configuring an Aggregated Ethernet Interface

You can associate a physical interface with an aggregated Ethernet interface.

To configure an aggregated Ethernet interface:

1. Specify that you want to configure the link aggregation group interface.

```
user@host# edit interfaces interface-name
```

2. Configure the aggregated Ethernet interface.

```
[edit interfaces interface-name]
user@host# set ether-options 802.3ad aex
```

You specify the interface instance number *x* to complete the link association; You must also include a statement defining `aex` at the `[edit interfaces]` hierarchy level. You can optionally specify other physical properties that apply specifically to the aggregated Ethernet interfaces; for details, see Ethernet Interfaces Overview.

NOTE: In general, aggregated Ethernet bundles support the features available on all supported interfaces that can become a member link within the bundle. As an exception, Gigabit Ethernet IQ features and some newer Gigabit Ethernet features are not supported in aggregated Ethernet bundles.

Gigabit Ethernet IQ and SFP interfaces can be member links, but IQ- and SFP-specific features are not supported on the aggregated Ethernet bundle even if all the member links individually support those features.

You need to configure the correct link speed for the aggregated Ethernet interface to eliminate any warning message.

NOTE: Before you commit an aggregated Ethernet configuration, ensure that link mode is not configured on any member interface of the aggregated Ethernet bundle; otherwise, the configuration commit check fails.

RELATED DOCUMENTATION

Aggregated Ethernet Interfaces Overview

Configuring Aggregated Ethernet LACP

IN THIS SECTION

For aggregated Ethernet interfaces, you can configure the Link Aggregation Control Protocol (LACP). LACP is one method of bundling several physical interfaces to form one logical interface. You can configure both VLAN-tagged and untagged aggregated Ethernet with or without LACP enabled.

For Multichassis Link Aggregation (MC-LAG), you must specify the `system-id` and `admin key`. MC-LAG peers use the same `system-id` while sending the LACP messages. The `system-id` can be configured on the MC-LAG network device and synchronized between peers for validation.

LACP exchanges are made between actors and partners. An actor is the local interface in an LACP exchange. A partner is the remote interface in an LACP exchange.

LACP is defined in IEEE 802.3ad, *Aggregation of Multiple Link Segments*.

LACP was designed to achieve the following:

- Automatic addition and deletion of individual links to the aggregate bundle without user intervention
- Link monitoring to check whether both ends of the bundle are connected to the correct group

The Junos OS implementation of LACP provides link monitoring but not automatic addition and deletion of links.

The LACP mode can be active or passive. If the actor and partner are both in passive mode, they do not exchange LACP packets, which results in the aggregated Ethernet links not coming up. If either the actor or partner is active, they do exchange LACP packets. By default, LACP is turned off on aggregated Ethernet interfaces. If LACP is configured, it is in passive mode by default. To initiate transmission of LACP packets and response to LACP packets, you must configure LACP in active mode.

To enable LACP active mode, include the `lacp` statement at the `[edit interfaces interface-name aggregated-ether-options]` hierarchy level, and specify the `active` option:

```
[edit interfaces interface-name aggregated-ether-options]
lacp {
    active;
}
```

NOTE: The LACP process exists in the system only if you configure the system in either active or passive LACP mode.

To restore the default behavior, include the lacp statement at the [edit interfaces *interface-name* aggregated-ether-options] hierarchy level, and specify the passive option:

```
[edit interfaces interface-name aggregated-ether-options]
lacp {
    passive;
}
```

Starting with Junos OS release 12.2, you can also configure LACP to override the IEEE 802.3ad standard and to allow the standby link always to receive traffic. Overriding the default behavior facilitates subsecond failover.

To override the IEEE 802.3ad standard and facilitate subsecond failover, include the fast-failover statement at the [edit interfaces *interface-name* aggregated-ether-options lacp] hierarchy level.

For more information, see the following sections:

Configuring the LACP Interval

By default, the actor and partner send LACP packets every second. You can configure the interval at which the interfaces send LACP packets by including the periodic statement at the [edit interfaces *interface-name* aggregated-ether-options lacp] hierarchy level:

```
[edit interfaces interface-name aggregated-ether-options lacp]
periodic interval;
```

The interval can be fast (every second) or slow (every 30 seconds). You can configure different periodic rates on active and passive interfaces. When you configure the active and passive interfaces at different rates, the transmitter honors the receiver’s rate.

NOTE: Source address filtering does not work when LACP is enabled.

Percentage policers are not supported on aggregated Ethernet interfaces with the CCC protocol family configured. For more information about percentage policers, see the Routing Policies, Firewall Filters, and Traffic Policers User Guide.

Generally, LACP is supported on all untagged aggregated Ethernet interfaces. For more information, see Configuring Untagged Aggregated Ethernet Interfaces.

Configuring LACP Link Protection

NOTE: When using LACP link protection, you can configure only two member links to an aggregated Ethernet interface: one active and one standby.

To force active and standby links within an aggregated Ethernet, you can configure LACP link protection and system priority at the aggregated Ethernet interface level using the `link-protection` and `system-priority` statements. Configuring values at this level results in only the configured interfaces using the defined configuration. LACP interface configuration also enables you to override global (chassis) LACP settings.

LACP link protection also uses port priority. You can configure port priority at the Ethernet interface `[ether-options]` hierarchy level using the `port-priority` statement. If you choose not to configure port priority, LACP link protection uses the default value for port priority (127).

NOTE: LACP link protection supports per-unit scheduling configuration on aggregated Ethernet interfaces.

To enable LACP link protection for an aggregated Ethernet interfaces, use the `link-protection` statement at the `[edit interfaces aeX aggregated-ether-options lacp]` hierarchy level:

```
[edit interfaces aeX aggregated-ether-options lacp]
link-protection;
    disable;
    revertive;
    non-revertive;
}
```

By default, LACP link protection reverts to a higher-priority (lower-numbered) link when that higher-priority link becomes operational or a link is added to the aggregator that is determined to be higher in priority. However, you can suppress link calculation by adding the `non-revertive` statement to the LACP link protection configuration. In nonrevertive mode, once a link is active and collecting and distributing packets, the subsequent addition of a higher-priority (better) link does not result in a switch and the current link remains active.

If LACP link protection is configured to be nonrevertive at the global (`[edit chassis]` hierarchy) level, you can add the `revertive` statement to the LACP link protection configuration to override the nonrevertive setting for the interface. In revertive mode, the addition of a higher-priority link to the aggregator results in LACP performing a priority recalculation and switching from the current active link to the new active link.

⚠ **CAUTION**: If both ends of an aggregator have LACP link protection enabled, make sure to configure both ends of the aggregator to use the same mode. Mismatching LACP link protection modes can result in lost traffic.

We strongly recommend you to use LACP on both ends of the aggregator, when you connect an aggregated Ethernet interface with two member interfaces to any other vendor device. Otherwise, the vendor device (say a Layer 2 switch, or a router), will not be able to manage the traffic coming from the two link aggregated Ethernet bundle. As a result, you might observe the vendor device sending back the traffic to the backup member link of the aggregated Ethernet interface.

Currently, MX-MPC2-3D, MX-MPC2-3D-Q, MX-MPC2-3D-EQ, MX-MPC1-3D, MX-MPC1-3D-Q, and MPC-3D-16XGE-SFPP do not drop traffic coming back to the backup link, whereas DPCE-R-Q-20GE-2XGE, DPCE-R-Q-20GE-SFP, DPCE-R-Q-40GE-SFP, DPCE-R-Q-4XGE-XFP, DPCE-X-Q-40GE-SFP, and DPCE-X-Q-4XGE-XFP drop traffic coming to the backup link.

Configuring LACP System Priority

To configure LACP system priority for aggregated Ethernet interfaces on the interface, use the `system-priority` statement at the `[edit interfaces ae`*`X`*` aggregated-ether-options lacp]` hierarchy level:

```
[edit interfaces aeX aggregated-ether-options lacp]
system-priority;
```

The system priority is a 2-octet binary value that is part of the LACP system ID. The LACP system ID consists of the system priority as the two most-significant octets and the interface MAC address as the six least-significant octets. The system with the numerically lower value for system priority has the higher priority. By default, system priority is 127, with a range of 0 to 65,535.

Configuring LACP System Identifier

To configure the LACP system identifier for aggregated Ethernet interfaces, use the `system-id` statement at the `[edit interfaces ae`*`X`*` aggregated-ether-options lacp]` hierarchy level:

```
[edit interfaces aeX aggregated-ether-options lacp]
system-id system-id;
```

The user-defined system identifier in LACP enables two ports from two separate devices to act as though they were part of the same aggregate group.

The system identifier is a 48-bit (6-byte) globally unique field. It is used in combination with a 16-bit system-priority value, which results in a unique LACP system identifier.

Configuring LACP administrative Key

To configure an administrative key for LACP, include the `admin-key` *`number`* statement at the `edit interfaces ae`*`x`* `aggregated-ether-options lacp]` hierarchy level:

```
[edit interfaces ae x aggregated-ether-options-lacp]
admin-key number;
```

NOTE: You must configure MC-LAG to configure the `admin-key` statement. For more information about MC-LAG, see Configuring Multichassis Link Aggregation on MX Series Routers .

Configuring LACP Port Priority

To configure LACP port priority for aggregated Ethernet interfaces, use the `port-priority` statement at the `[edit interfaces` *`interface-name`* `ether-options 802.3ad ae`*`X`* `lacp]` or `[edit interfaces` *`interface-name`* `ether-options 802.3ad ae`*`X`* `lacp]` hierarchy levels:

```
[edit interfaces interface-name ether-options 802.3ad aeX lacp]
port-priority priority;
```

The port priority is a 2-octet field that is part of the LACP port ID. The LACP port ID consists of the port priority as the two most-significant octets and the port number as the two least-significant octets. The system with the numerically lower value for port priority has the higher priority. By default, port priority is 127, with a range of 0 to 65,535.

Port aggregation selection is made by each system based on the highest port priority and are assigned by the system with the highest priority. Ports are selected and assigned starting with the highest priority port of the highest priority system and working down in priority from there.

NOTE: Port aggregation selection (discussed above) is performed for the active link when LACP link protection is enabled. Without LACP link protection, port priority is not used in port aggregation selection.

Tracing LACP Operations

To trace the operations of the LACP process, include the `traceoptions` statement at the `[edit protocols lacp]` hierarchy level:

```
[edit protocols lacp]
traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

You can specify the following flags in the `protocols lacp traceoptions` statement:

- `all`—All LACP tracing operations
- `configuration`—Configuration code
- `packet`—Packets sent and received
- `process`—LACP process events
- `protocol`—LACP protocol state machine
- `routing-socket`—Routing socket events
- `startup`—Process startup events

LACP Limitations

LACP can link together multiple different physical interfaces, but only features that are supported across all of the linked devices will be supported in the resulting link aggregation group (LAG) bundle. For example, different PICs can support a different number of forwarding classes. If you use link aggregation to link together the ports of a PIC that supports up to 16 forwarding classes with a PIC that supports up to 8 forwarding classes, the resulting LAG bundle will only support up to 8 forwarding classes. Similarly, linking together a PIC that supports WRED with a PIC that does not support it will result in a LAG bundle that does not support WRED.

Example: Configuring Aggregated Ethernet LACP

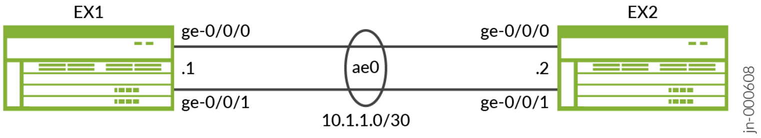
IN THIS SECTION

This example shows how to configure an aggregated ethernet interface with active LACP between two EX switches.

Topology

IN THIS SECTION

Two EX switches are connected together using two interfaces in an aggregated ethernet configuration.



Configure aggregated Ethernet LACP over an untagged interface:

NOTE: We are only showing the configuration for EX1 in this example. EX2 has the same configuration except for the IP address.

LACP with Untagged Aggregated Ethernet

The chassis configuration allows for 1 aggregated ethernet interface. The `802.3ad` configuration associates both interfaces `ge-0/0/0` and `ge-0/0/1` with interface `ae0`. The `ae0 aggregated-ether-options` configuration enables active mode LACP.

```
user@EX1# show
...
chassis {
    aggregated-devices {
        ethernet {
            device-count 1;
        }
    }
}
interfaces {
    ge-0/0/0 {
        ether-options {
            802.3ad ae0;
        }
    }
    ge-0/0/1 {
        ether-options {
            802.3ad ae0;
        }
    }
    ae0 {
        aggregated-ether-options {
            lacp {
                active;
            }
        }
        unit 0 {
            family inet {
                address 10.1.1.1/30;
            }
        }
    }
}
```

Verification

IN THIS SECTION

Verifying the Aggregated Ethernet Interface

Purpose

Verify the aggregated ethernet interface has been created and is up.

Action

Use the command `show interfaces terse | match ae` from operational mode.

```
user@EX1> show interfaces terse | match ae
ge-0/0/0.0              up    up   aenet    --> ae0.0
ge-0/0/1.0              up    up   aenet    --> ae0.0
ae0                     up    up
ae0.0                   up    up   inet     10.1.1.1/30
```

Meaning

The output shows that ge-0/0/0 and ge-0/0/1 are bundled together to create the aggregated ethernet interface `ae0` and the interface is up.

Verifying LACP is Active

Purpose

Verify which interfaces are participating in LACP and the current state.

Action

Use the command `show lacp interfaces` from operational mode.

```
user@EX1> show lacp interfaces
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/0                  Current   Fast periodic Collecting distributing
      ge-0/0/1                  Current   Fast periodic Collecting distributing
```

Meaning

The output shows that the active mode LACP is enabled.

Verify Reachability

Purpose

Verify that ping works between the two EX switches.

Action

Use the `ping 10.1.1.2 count 2` operational mode command on EX1.

```
user@EX1> ping 10.1.1.2 count 2
PING 10.1.1.2 (10.1.1.2): 56 data bytes
64 bytes from 10.1.1.2: icmp_seq=0 ttl=64 time=2.249 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=64 time=2.315 ms

--- 10.1.1.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.249/2.282/2.315/0.033 ms
```

Meaning

EX1 is able to ping EX2 across the aggregated ethernet interface.

RELATED DOCUMENTATION

- lacp
- link-protection
- traceoptions

CHAPTER 14

SNMP MIB Support on Junos Fusion Enterprise

IN THIS CHAPTER

Chassis MIB Support (Junos Fusion)

The Chassis MIB has been enhanced to enable satellite devices to be represented in the chassis MIB. Satellite devices are represented as FPCs/slots (100, 101,102,..) in the aggregation device. The support is enabled using a separate range of container indices (CIDX), which allows the SNMP process to redirect relevant SNMP requests to the satellite device management process.

The CIDX for representing satellite device hardware components in Junos Fusion are offset by 100 from indices for hardware components on Junos devices; for example a regular CIDX 2 (Power Supply) is 102 for the power supply of the satellite device. Using these indices you can distinguish the satellite device hardware from the aggregate device. The L1 index for satellite device entries refers to their FPC slot identifiers. As per the chassis MIB convention, identifiers are 1-based. For example, satellite device 100 will have an L1 index of 101, satellite device 101 will have an L1 index of 102, and so on.

Table 13 on page 175shows the CIDXs used for satellite devices.

Table 13: CIDX's for Satellite Devices

CIDX	Component Type
102	Power Supply
104	Fan
107	FPC

Table 13: CIDX's for Satellite Devices *(Continued)*

CIDX	Component Type
108	PIC

The following tables have been enhanced to include object IDs for satellite devices:

- jnxContainersTable
- jnxContentsTable
- jnxFilledTable
- jnxOperatingTable
- jnxFRUTable

Examples of new object IDs in the jnxContainersTable:

```
jnxContainersType.102 = jnxSatelliteDeviceSlotPower.0
jnxContainersType.104 = jnxSatelliteDeviceSlotFan.0
jnxContainersType.107 = jnxSatelliteDeviceSlotFPC.0
jnxContainersType.108 = jnxSatelliteDeviceMediaCardSpacePIC.0
…
…
jnxContainersDescr.102 = SD PEM slot
jnxContainersDescr.104 = SD FAN slot
jnxContainersDescr.107 = SD FPC slot
jnxContainersDescr.108 = SD PIC slot
```

Examples of new object IDs in the jnxContentsTable:

```
jnxContentsType.102.102.1.0 = jnxSatelliteDeviceSlotPower
jnxContentsType.102.102.2.0 = jnxSatelliteDeviceSlotPower
jnxContentsType.104.102.1.0 = jnxSatelliteDeviceSlotFan
jnxContentsType.104.102.2.0 = jnxSatelliteDeviceSlotFan
jnxContentsType.104.102.3.0 = jnxSatelliteDeviceSlotFan
jnxContentsType.104.102.4.0 = jnxSatelliteDeviceSlotFan
jnxContentsType.104.102.5.0 = jnxSatelliteDeviceSlotFan
jnxContentsType.107.102.0.0 = jnxSatelliteDeviceSlotFPC
jnxContentsType.108.102.1.0 = jnxSatelliteDeviceMediaCardSpacePIC
```

```
…
jnxContentsDescr.102.102.1.0 = SD101 PEM 0
jnxContentsDescr.102.102.2.0 = SD101 PEM 1
jnxContentsDescr.104.102.1.0 = SD101 Fan Tray 0
jnxContentsDescr.104.102.2.0 = SD101 Fan Tray 1
jnxContentsDescr.104.102.3.0 = SD101 Fan Tray 2
jnxContentsDescr.104.102.4.0 = SD101 Fan Tray 3
jnxContentsDescr.104.102.5.0 = SD101 Fan Tray 4
jnxContentsDescr.107.102.0.0 = SD101 FPC: QFX5100-48S-6Q @ 101/*/*
jnxContentsDescr.108.102.1.0 = SD101 PIC: 48x10G-6x40G @ 101/0/*
```

The following SNMP traps are generated for Satellite Devices, which are also logged as syslog messages:

- Satellite Device (as FPC) add (online) or remove
- Satellite Device Fan add (online) or remove
- Satellite Device PSU add (online) or remove
- Satellite Device PIC add (online) or remove
- Satellite Device FAN failure or status
- Satellite Device PSU failure or status

Table 14 on page 177 shows the SNMP traps that can be generated for satellite devices.

Table 14: SNMP Traps Generated for Satellite Devices

Trap	Condition
jnxFruRemoval	Sent when the specified FRU (FAN/PSU) has been removed from the chassis, or the satellite device has been removed from the aggregation device's database
jnxFruInsertion	Sent when the specified FRU (FAN/PSU) has been inserted into the satellite device
jnxFruPowerOff	Sent when the specified FRU (FAN/PSU) has been powered off in the satellite device
jnxFruPowerOn	Sent when the specified FRU (FAN/PSU) has been powered on in the satellite device

Table 14: SNMP Traps Generated for Satellite Devices *(Continued)*

Trap	Condition
jnxFruFailed	Sent when the specified FRU (FAN/PSU) has failed in the satellite device. Typically, this is due to the FRU not powering up or being unable to load software. FRU replacement might be required
jnxFruOK	
jnxFruOffline	Sent when FPC's new reported state is not online or PSU/FAN/PIC is not present due to satellite device removal
jnxFruOnline	Sent when specified FRU (FPC,PIC,PSU,FAN) gets added in the aggregation device database
jnxFruCheck	Sent when the specified FRU (FAN/PSU) has encountered operational errors

Given below are examples of the system log messages generated:

```
messages:Apr 15 21:28:36  card spmd[6706]: SPMD_SNMP_TRAP10: SNMP trap generated: Fru Offline
(jnxFruContentsIndex 102, jnxFruL1Index 109, jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName SD108
PEM 0, jnxFruType 7, jnxFruSlot 0, jnxFruOfflineReason 1, jnxFruLastPowerOff 0,
jnxFruLastPowerOn 0)
```

```
messages:Apr 15 21:28:36  card spmd[6706]: SPMD_SNMP_TRAP10: SNMP trap generated: Fru Offline
(jnxFruContentsIndex 104, jnxFruL1Index 109, jnxFruL2Index 1, jnxFruL3Index 1, jnxFruName SD108
Fan Tray 0, jnxFruType 13, jnxFruSlot 0, jnxFruOfflineReason 1, jnxFruLastPowerOff 0,
jnxFruLastPowerOn 0)
```

```
messages:Apr 15 21:28:57  card spmd[8847]: SPMD_SNMP_TRAP7: SNMP trap generated: Fru Online
(jnxFruContentsIndex 107, jnxFruL1Index 103, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName SD102
FPC:  @ 102/*/*, jnxFruType 3, jnxFruSlot 102)
```

```
messages:Apr 15 21:28:36  card spmd[6706]: SPMD_SNMP_TRAP10: SNMP trap generated: Fru Offline
(jnxFruContentsIndex 108, jnxFruL1Index 109, jnxFruL2Index 1, jnxFruL3Index 0, jnxFruName SD108
PIC: 48x 10/100/1000 Base-T @ 108/0/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 1,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 0)
```

CHAPTER 15

Media Access Control Security (MACsec) on Junos Fusion Enterprise

IN THIS CHAPTER

Understanding Media Access Control Security on a Junos Fusion Enterprise

IN THIS SECTION

Media Access Control Security (MACsec) is widely used in campus deployments to secure network traffic between endpoints and access switches. You can enable MACsec on extended ports in a Junos Fusion Enterprise topology to provide secure communication between the satellite device and connected hosts.

MacSec Overview

MACsec is an 802.1AE IEEE industry-standard security technology that provides secure communication on Ethernet links between directly-connected nodes. MACsec is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec provides point-to-point integrity and can be used in combination with other security solutions, such as IP Security (IPsec) and Secure Sockets Layer (SSL), to provide end-to-end network security.

See Understanding Media Access Control Security (MACsec) for a detailed overview of MACsec.

Enabling MACsec in a Junos Fusion Enterprise

To enable MACsec on a link connecting an endpoint device—such as a server, phone, or personal computer—to an extended port in a Junos Fusion Enterprise, the endpoint device must support MACsec and must be running client software that allows it to enable a MACsec-secured connection. A secure association using dynamic secure association security mode (dynamic SAK) must be configured on the extended port that connects to the host. The secure association keys are retrieved from the RADIUS server as part of the 802.1X authentication process. The keys are exchanged between the MACsec peers to create a secure connection.

MacSec configuration in Junos Fusion is done on the aggregated device and is identical for a standalone EX Series switch. See Configuring MACsec on EX, QFX and SRX Devices.

NOTE: When MACsec is enabled in a Junos Fusion with dual aggregation devices, the exchange of EAPoL packets that takes place during the 802.1X authentication session is limited to one aggregation device (AD). The MKA protocol is triggered only on that (AD), and the keys generated by MKA are not synced across the ADs. If the AD on which the keys are generated fails, then the MACsec sessions must be re-authenticated using the other AD.

RELATED DOCUMENTATION

Configuring MACsec on EX, QFX and SRX Devices

CHAPTER 16

Class of Service on Junos Fusion Enterprise

IN THIS CHAPTER

Understanding CoS in Junos Fusion Enterprise

IN THIS SECTION

Junos Fusion provides a method of significantly expanding the number of available network interfaces on an *aggregation device* by allowing the aggregation device to add interfaces through interconnections with *satellite devices*. The entire system—the interconnected aggregation device and satellite devices—is called Junos Fusion. Junos Fusion simplifies network administration by appearing in the network topology as a single device, and the single device is managed from a single IP address.

See Figure 11 on page 183 and Figure 12 on page 183 for illustrations of the Junos Fusion Enterprise topology.

Figure 11: Basic Junos Fusion Topology

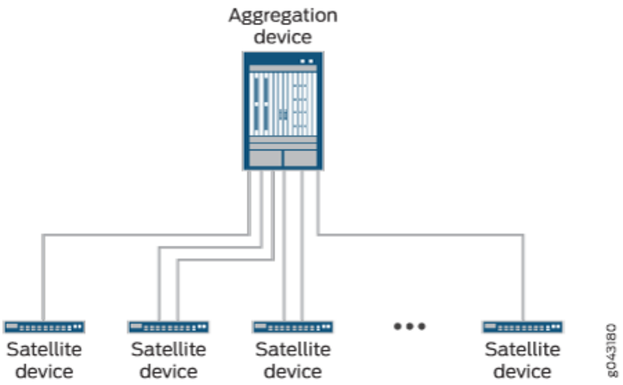
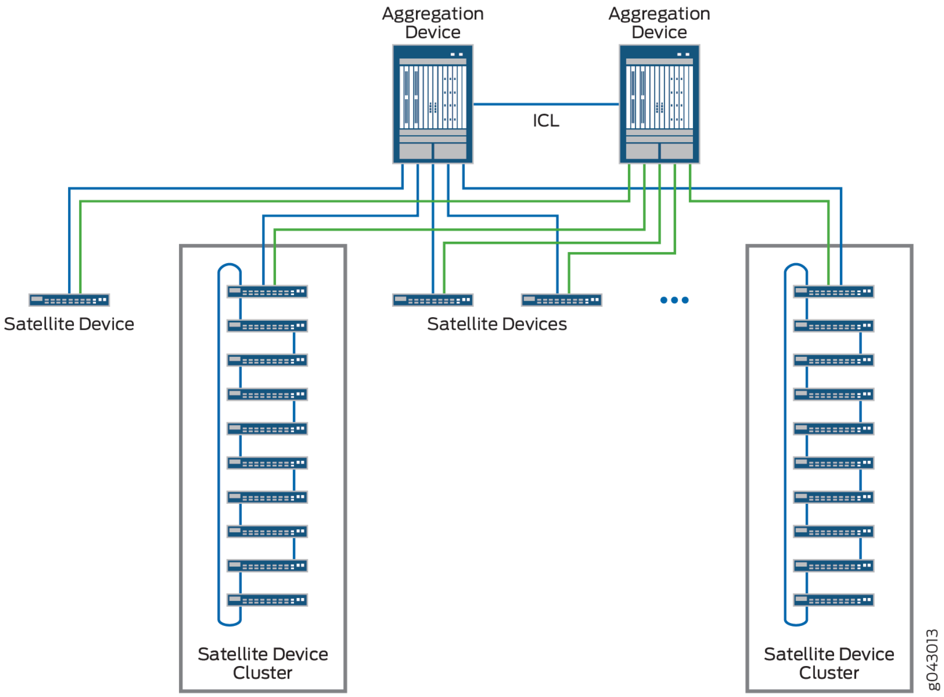


Figure 12: Junos Fusion Topology with Dual Aggregation Devices and Satellite Device Clusters



For Junos Fusion Enterprise, an aggregation device is an EX9200 switch that is running Junos OS Release 16.1R1 or later. Beginning with Junos OS Release 17.1R1, Junos Fusion Enterprise supports CoS. CoS configuration is the same on Junos Fusion Enterprise regardless of the selected architecture - single or dual aggregation devices, single or cluster satellite devices.

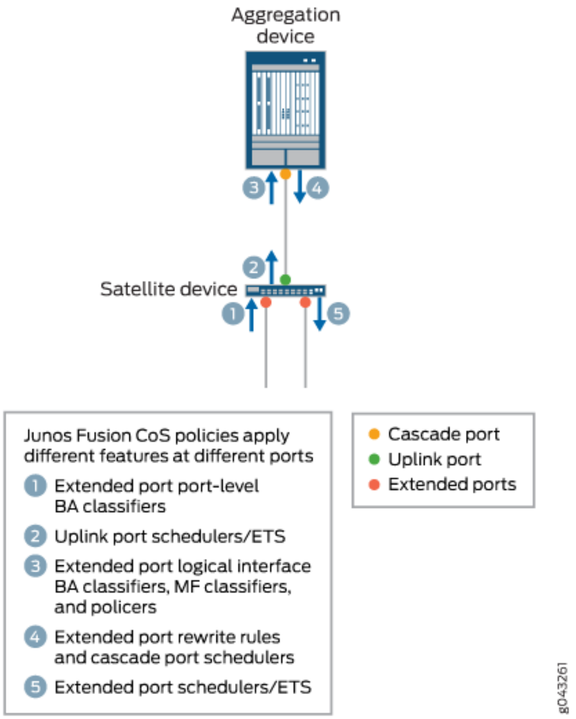
This topic describes class of service (CoS) on the different types of ports in Junos Fusion.

This topic covers:

Overview of CoS on Different Types of Ports in Junos Fusion

Figure 13 on page 184 provides an overview of packet flow through Junos Fusion and how CoS features are applied at the different ports.

Figure 13: Junos Fusion CoS Feature Application


Aggregation device
3
4
2
Satellite device
1
5
Junos Fusion CoS policies apply different features at different ports
1 Extended port port-level BA classifiers
2 Uplink port schedulers/ETS
3 Extended port logical interface BA classifiers, MF classifiers, and policers
4 Extended port rewrite rules and cascade port schedulers
5 Extended port schedulers/ETS
● Cascade port
● Uplink port
● Extended ports
g043261

All configuration for CoS policies for Junos Fusion is done on the aggregation device. For CoS policies that you define for extended ports, however, different portions of that policy are applied at different points in a packet's path through Junos Fusion. From Figure 13 on page 184:

1. As a packet enters an extended port, any port-level (physical interface-level) behavior aggregate (BA) classifier you define for that port is applied to derive a forwarding class and packet loss priority.

2. As that packet exits the uplink port, you can apply schedulers or enhanced transmission selection (ETS) based on the port-level BA classifier assigned at the ingress extended port.

3. As the packet enters the aggregation device at the cascade port, any multifield classifiers, policers, or logical interface-level BA classifiers you define for the ingress extended port are applied.

4. As the packet exits the aggregation device at the cascade port, any rewrite rules you define for the egress extended port, as well as any schedulers you define for the cascade port, are applied. Also, the forwarding class determined in the previous step is carried in the 801.2BR header to the satellite device and used to select the output queue at the egress extended port.

5. Finally, as the packet exits an extended port, any schedulers or ETS you define for that port are applied based on the forwarding class determined by the multifield classifiers, policers, or logical interface-level BA classifiers defined for the ingress extended port.

The following sections provide further information about implementing CoS on each port type in Junos Fusion.

CoS on Extended Ports and Uplink Ports in Junos Fusion

All class of service (CoS) scheduling policies for extended ports and uplink ports on the satellite devices are provisioned on the EX9200 aggregation device. Similarly, standard Junos OS CoS commands are issued on the EX9200 aggregation device for retrieving extended port and uplink port CoS states and queue statistics. The EX9200 aggregation device supports configuring the following CoS features for each extended port and uplink port on each satellite device:

- Behavior aggregate classifiers
- Multifield classifiers
- Input and output policers
- Forwarding classes
- Traffic control profiles
- Schedulers and scheduler maps
- Egress rewrite rules

NOTE: Configuring CoS policies on *satellite devices* (on both extended and uplink ports) has the following restrictions:

- IP precedence classifiers are not supported. DSCP classifiers are supported, however.
- Interpolated drop profiles are not supported.
- The `transmit-rate` option is supported for schedulers. However, the `remainder`, `rate-limit`, and `exact` options are not supported under `transmit-rate`.

While CoS features for satellite device ports are configured on the aggregation device, the actual classification, queueing, and scheduling is performed on the satellite devices. Information on actual traffic shaping is not passed back to the aggregation device. Logical interface statistics for the **show interfaces** command are collected on the aggregate device and do not include shaping rate data. For actual traffic statistics gathered on satellite device interfaces, use the statistics for the physical interface and not the logical interface.

> **NOTE**: CoS statistics are not supported on extended ports.

CoS on Cascade Ports in Junos Fusion

When a cascade port is created, two logical interfaces are automatically created:

- One in-band management logical interface (assigned unit 32769) for traffic that only flows between the aggregation device and the satellite devices, such as keepalives, for provisioning information, and for software updates.
- One for data logical interface (assigned unit 32770) for regular traffic that flows into and out of Junos Fusion.

Per-unit scheduling is automatically enabled on the cascade port to support multiple queues on each of the logical interfaces.

> **NOTE**: All cascade ports must be configured on Modular Port Concentrators (MPCs) that support per-unit scheduling.

50 Mbps of bandwidth is reserved for the management logical interface. The remaining bandwidth is available to the data logical interface. A shaping rate of 10 percent is also applied to the management logical interface, which means it can use up to 10 percent of the full interface bandwidth, if available.

The default scheduling policy is applied to the data logical interface. This reserves 95 percent of the available bandwidth and buffer space for the best effort forwarding class (mapped to queue 0) and 5 percent for the network control forwarding class (mapped to queue 3). You can create custom forwarding classes and schedulers by applying a custom scheduler map to this logical interface.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.1R1	Beginning with Junos OS Release 17.1R1, Junos Fusion Enterprise supports CoS.

RELATED DOCUMENTATION

Junos Fusion Enterprise Overview | 2
Understanding Junos Fusion Enterprise Components | 5
Configuring CoS in Junos Fusion Enterprise | 187

Configuring CoS in Junos Fusion Enterprise

IN THIS SECTION

Junos Fusion significantly expands the number of available network interfaces on an *aggregation device* by allowing the aggregation device to add interfaces through interconnections with *satellite devices*. The entire system—the interconnected aggregation device and satellite devices—is called Junos Fusion. Junos Fusion simplifies network administration by appearing in the network topology as a single device, and the single device is managed from a single IP address.

This topic describes how to configure CoS on the different types of ports in Junos Fusion.

This topic covers:

Configuring Behavior Aggregate Classifiers on Satellite Device Extended Ports

Normally, you apply a behavior aggregate (BA) classifier to a logical interface on an EX9200 device at the `[edit class-of-service interfaces` *`interface-name`* `unit` *`logical-unit-number`*`]` hierarchy level. When traffic from a satellite device extended port reaches the aggregation device, the BA classifier configured for the logical interface level of the satellite device extended port is applied the same as it is for traffic from other non-extended ports to help determine the forwarding class of the traffic; policers and multifield classifiers can also factor in determining the forwarding class of the traffic. When the aggregation devices sends the traffic out to the satellite device, the forwarding class is carried in the 801.2BR header. The satellite device then uses the forwarding class to select the output queue at the *egress extended port*.

You can also apply a BA classifier at the physical interface level of an extended port. This classifier is used to determine the output queue at the *uplink port* of the satellite device.

NOTE: IP precedence classifiers are not supported on extended ports at the physical interface level. DSCP classifiers are supported, however.

NOTE: You cannot apply a physical interface-level classifier on an EX9200 local port.

To add a behavior aggregate classifier to the physical interface level of a satellite device extended port in Junos Fusion:

1. Define the classifier.

```
[edit class-of-service]
user@ex9200-agg-device#set classifiers dscp dscp-1 forwarding-class best-effort-3 loss-priority low code-points 001010
```

2. Apply the classifier to the physical extended port.

```
[edit class-of-service]
user@ex9200-agg-device#set interfaces xe-100/0/33 classifiers dscp dscp-1
```

3. Commit the changes and then confirm the configuration.

```
[edit class-of-service]
user@ex9200-agg-device# show
classifiers {
    dscp dscp-1 {
        forwarding-class best-effort-3 {
            loss-priority low code-points 001010;
        }
    }
}
interfaces {
    xe-100/0/33 {
        classifiers {
            dscp dscp-1;
        }
    }
}
```

In the above configuration example, packets entering port xe-100/0/33 with a DSCP value of `001010` will be assigned a forwarding class of `best-effort-3` to select the output queue at the uplink port as the packet travels from the satellite device to the aggregation device.

SEE ALSO

- Understanding Junos Fusion Ports | 19
- Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic
- Overview of Assigning Service Levels to Packets Based on Multiple Packet Header Fields

Configuring Rewrite Rules on Satellite Device Extended Ports

You apply rewrite rules to logical interfaces on satellite device extended ports.

To add a rewrite rule to a satellite device extended port in a Junos Fusion:

1. Define the rewrite rule.

```
[edit class-of-service]
user@ex9200-agg-device#set rewrite-rules ieee-802.1 rewrite1p forwarding-class best-effort
loss-priority low code-point 010
```

2. Apply the rewrite rule to a logical interface.

```
[edit class-of-service]
user@ex9200-agg-device#set interfaces xe-108/0/47 unit 0 rewrite-rules ieee-802.1 rewrite1p
```

3. Commit the changes and then confirm the configuration.

```
[edit class-of-service]
user@ex9200-agg-device# show
rewrite-rules {
    ieee-802.1 rewrite1p {
        forwarding-class best-effort {
            loss-priority low code-point 010;
        }
    }
}
interfaces {
    xe-108/0/47 {
        unit 0 {
            rewrite-rules {
                ieee-802.1 rewrite-1p;
            }
        }
    }
}
```

In Junos OS, rewrite rules only look at the forwarding class and packet loss priority of the packet (as assigned by a behavior aggregate or multifield classifier at ingress), not at the incoming CoS value, to determine the CoS value to write to the packet header at egress. The above configuration means that, for any packet exiting the xe-108/0/47.0 interface that has a forwarding class of `best-effort` and a packet loss priority of `low`, the ieee-802.1 CoS value will be rewritten to `010`.

SEE ALSO

- Understanding Junos Fusion Ports | 19
- Rewriting Packet Headers to Ensure Forwarding Behavior

Changing the Default Scheduling Policy on an Aggregated Device Cascade Port

When a cascade port is created, two logical interfaces are automatically created:

- One in-band management logical interface (assigned unit 32769) for traffic that only flows between the aggregation device and the satellite devices, such as keepalives, for provisioning information, and for software updates.
- One for data logical interface (assigned unit 32770) for regular traffic that flows into and out of Junos Fusion.

Let's say, for example, that interface xe-0/0/1 is configured as a cascade port. The command `show interfaces xe-0/0/1 terse` produces output similar to the following:

```
user@ex9200-agg-device# run show interfaces xe-0/0/1 terse
Interface               Admin Link Proto    Local                 Remote
xe-0/0/1                up    up
xe-0/0/1.32769          up    up   inet     10.0.0.5/30
xe-0/0/1.32770          up    up   bridge
```

The control logical interface (unit 32769) is automatically assigned an internal traffic control profile (__cp_control_tc_prof) that guarantees 50 Mbps of bandwidth for the logical interface, a 10 percent shaping rate, and the default scheduling policy. The default scheduling policy is applied to the data logical interface. For example:

```
user@ex9200-agg-device# run show class-of-service interface xe-0/0/1
Physical interface: xe-0/0/1, Index: 144
Maximum usable queues: 8, Queues in use: 4
  Scheduler map: <default>, Index: 2
  Congestion-notification: Disabled

  Logical interface: xe-0/0/1.32769, Index: 344
Object                  Name                   Type                    Index
Traffic-control-profile __cp_control_tc_prof   Output                  17227
Classifier              ipprec-compatibility   ip                         13

  Logical interface: xe-0/0/1.32770, Index: 343
Object                  Name                   Type                    Index
Scheduler-map           <default>              Output                      2
```

and:

```
user@ex9200-agg-device# run show class-of-service scheduler-hierarchy interface xe-0/0/1
Interface/                    Shaping Guarnteed  Guaranteed/   Queue   Excess
Resource name                    rate      rate       Excess  weight   weight
                                kbits     kbits     priority          high/low
  xe-0/0/1.32770             10000000         0                          1    1
    BE                       10000000         0     Low  Low     118
    NC                       10000000         0     Low  Low       6
  xe-0/0/1.32769              1000000     50000                         62   62
    BE                        1000000     47500     Low  Low     118
    NC                        1000000      2500     Low  Low       6
```

You can create custom forwarding classes and schedulers for the data logical interface by applying a customer scheduler map to that logical interface. For example, to apply a customer scheduler policy to the data logical interface:

1. Create customer schedulers.

   ```
   [edit class-of-service]
   user@ex9200-agg-device#set schedulers AF_SCH_CORE transmit-rate percent 40
   user@ex9200-agg-device#set schedulers AF_SCH_CORE buffer-size percent 40
   user@ex9200-agg-device#set schedulers AF_SCH_CORE priority medium-high
   ```

```
user@ex9200-agg-device#set schedulers BE_SCH_CORE transmit-rate percent 10
user@ex9200-agg-device#set schedulers BE_SCH_CORE buffer-size percent 10
user@ex9200-agg-device#set schedulers BE_SCH_CORE priority low
user@ex9200-agg-device#set schedulers EF_SCH_CORE transmit-rate percent 40
user@ex9200-agg-device#set schedulers EF_SCH_CORE buffer-size percent 40
user@ex9200-agg-device#set schedulers EF_SCH_CORE priority medium-low
user@ex9200-agg-device#set schedulers NC_SCH_CORE transmit-rate percent 10
user@ex9200-agg-device#set schedulers NC_SCH_CORE buffer-size percent 10
user@ex9200-agg-device#set schedulers NC_SCH_CORE priority high
```

2. Create a scheduler map.

```
[edit class-of-service]
user@ex9200-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class BE scheduler
BE_SCH_CORE
user@ex9200-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class EF scheduler
EF_SCH_CORE
user@ex9200-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class AF scheduler
AF_SCH_CORE
user@ex9200-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class NC scheduler
NC_SCH_CORE
```

3. Apply the scheduler map to the data logical interface.

```
[edit class-of-service]
user@ex9200-agg-device#set interfaces xe-0/0/1 unit 32770 scheduler-map CORE_SCHED_MAP
```

4. Commit the changes and then confirm the configuration.

```
[edit class-of-service]
user@ex9200-agg-device# show
interfaces {
    xe-0/0/1 {
        unit 32770 {
            scheduler-map CORE_SCHED_MAP;
        }
    }
}
scheduler-maps {
    CORE_SCHED_MAP {
        forwarding-class BE scheduler BE_SCH_CORE;
        forwarding-class EF scheduler EF_SCH_CORE;
        forwarding-class AF scheduler AF_SCH_CORE;
        forwarding-class NC scheduler NC_SCH_CORE;
    }
}
schedulers {
    BE_SCH_CORE {
        transmit-rate percent 10;
        buffer-size percent 10;
        priority low;
    }
    EF_SCH_CORE {
        transmit-rate percent 40;
        buffer-size percent 40;
        priority medium-low;
    }
    AF_SCH_CORE {
        transmit-rate percent 40;
        buffer-size percent 40;
        priority medium-high;
    }
    NC_SCH_CORE {
        transmit-rate percent 10;
        buffer-size percent 10;
        priority high;
    }
}
```

5. Verify your changes.

```
user@ex9200-agg-device# run show class-of-service interface xe-0/0/1
Physical interface: xe-0/0/1, Index: 144
Maximum usable queues: 8, Queues in use: 4
  Scheduler map: <default>, Index: 2
  Congestion-notification: Disabled

  Logical interface: xe-0/0/1.32769, Index: 344
Object                  Name                   Type                    Index
Traffic-control-profile __cp_control_tc_prof   Output                  17227
Classifier              ipprec-compatibility   ip                         13

  Logical interface: xe-0/0/1.32770, Index: 343
```

```
Object                  Name                   Type                    Index
Scheduler-map           CORE_SCHED_MAP         Output                  23433
```

and:

```
user@ex9200-agg-device# run show class-of-service scheduler-hierarchy interface xe-0/0/1
Interface/                    Shaping Guarnteed  Guaranteed/   Queue   Excess
Resource name                    rate      rate       Excess  weight   weight
                                kbits     kbits     priority          high/low
  xe-0/0/1.32770             10000000        0                          1    1
    BE                       10000000        0     Low  Low      12
    EF                       10000000        0  Medium  Low      50
    AF                       10000000        0  Medium  Low      50
    NC                       10000000        0    High High      12
  xe-0/0/1.32769              1000000    50000                         62   62
    BE                        1000000    47500     Low  Low     118
    NC                        1000000     2500     Low  Low       6
```

SEE ALSO

How Schedulers Define Output Queue Properties

Default Schedulers Overview

RELATED DOCUMENTATION

Understanding CoS in Junos Fusion Enterprise | 182

CHAPTER 17

Extending a Junos Fusion Enterprise Using EVPN-MPLS

IN THIS CHAPTER

Understanding EVPN-MPLS Interworking with Junos Fusion Enterprise and MC-LAG

IN THIS SECTION

Starting with Junos OS Release 17.4R1, you can use Ethernet VPN (EVPN) to extend a Junos Fusion Enterprise or multichassis link aggregation group (MC-LAG) network over an MPLS network to a data center or campus network. With the introduction of this feature, you can now interconnect dispersed campus and data center sites to form a single Layer 2 virtual bridge.

Figure 14 on page 196 shows a Junos Fusion Enterprise topology with two EX9200 switches that serve as aggregation devices (PE2 and PE3) to which the satellite devices are multihomed. The two aggregation devices use an interchassis link (ICL) and the Inter-Chassis Control Protocol (ICCP) protocol from MC-LAG to connect and maintain the Junos Fusion Enterprise topology. PE1 in the EVPN-MPLS environment interworks with PE2 and PE3 in the Junos Fusion Enterprise with MC-LAG.

Figure 14: EVPN-MPLS Interworking with Junos Fusion Enterprise

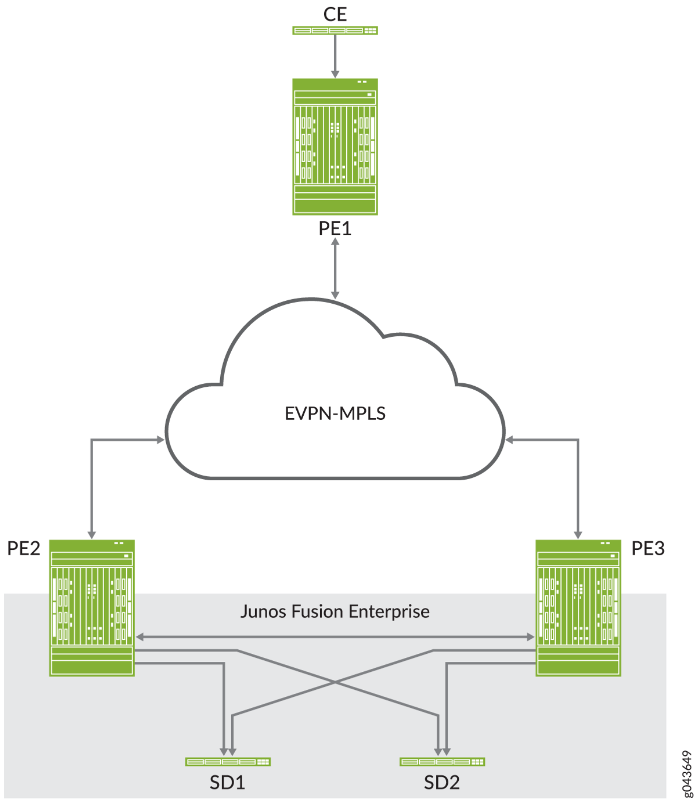
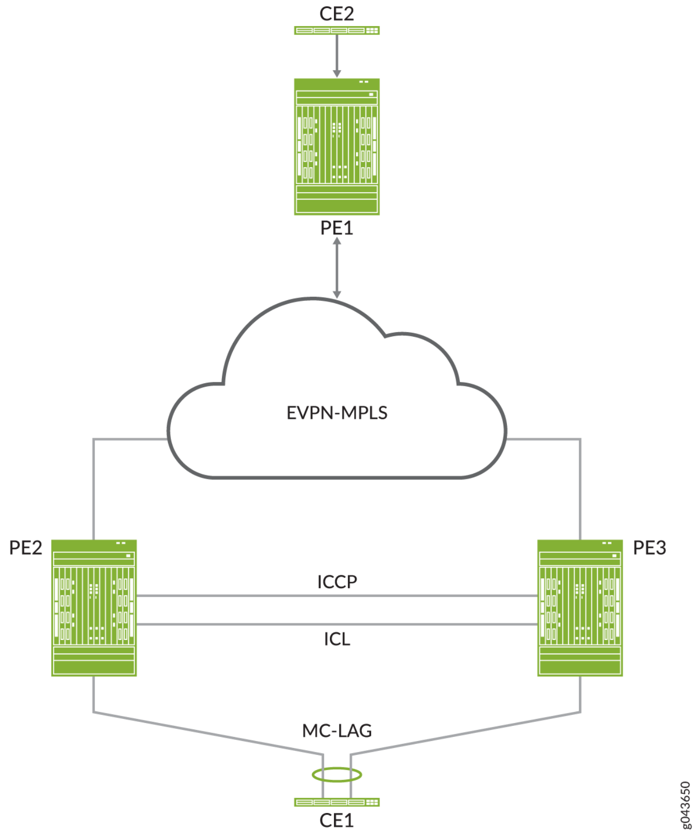


Figure 15 on page 197 shows an MC-LAG topology in which customer edge (CE) device CE1 is multihomed to PE2 and PE3. PE2 and PE3 use an ICL and the ICCP protocol from MC-LAG to connect and maintain the topology. PE1 in the EVPN-MPLS environment interworks with PE2 and PE3 in the MC-LAG environment.

Figure 15: EVPN-MPLS Interworking with MC-LAG



Throughout this topic, Figure 14 on page 196 and Figure 15 on page 197 serve as references to illustrate various scenarios and points.

The use cases depicted in Figure 14 on page 196 and Figure 15 on page 197 require the configuration of both EVPN multihoming in active-active mode and MC-LAG on PE2 and PE3. EVPN with multihoming active-active and MC-LAG have their own forwarding logic for handling traffic, in particular, broadcast, unknown unicast, and multicast (BUM) traffic. At times, the forwarding logic for EVPN with multihoming active-active and MC-LAG contradict each other and causes issues. This topic describes the issues and how the EVPN-MPLS interworking feature resolves these issues.

NOTE: Other than the EVPN-MPLS interworking-specific implementations described in this topic, EVPN-MPLS, Junos Fusion Enterprise, and MC-LAG offer the same functionality and function the same as the standalone features.

Benefits of Using EVPN-MPLS with Junos Fusion Enterprise and MC-LAG

Use EVPN-MPLS with Junos Fusion Enterprise and MC-LAG to interconnect dispersed campus and data center sites to form a single Layer 2 virtual bridge.

BUM Traffic Handling

In the use cases shown in Figure 14 on page 196 and Figure 15 on page 197, PE1, PE2, and PE3 are EVPN peers, and PE2 and PE3 are MC-LAG peers. Both sets of peers exchange control information and forward traffic to each other, which causes issues. Table 15 on page 198 outlines the issues that arise, and how Juniper Networks resolves the issues in its implementation of the EVPN-MPLS interworking feature.

Table 15: BUM Traffic: Issues and Resolutions

BUM Traffic Direction	EVPN Interworking with Junos Fusion Enterprise and MC-LAG Logic	Issue	Juniper Networks Implementation Approach
North bound (PE2 receives BUM packet from a locally attached single- or dual-homed interfaces).	PE2 floods BUM packet to the following: • All locally attached interfaces, including the ICL, for a particular broadcast domain. • All remote EVPN peers for which PE2 has received inclusive multicast routes.	Between PE2 and PE3, there are two BUM forwarding paths—the MC-LAG ICL and an EVPN-MPLS path. The multiple forwarding paths result in packet duplication and loops.	• BUM traffic is forwarded on the ICL only. • Incoming traffic from the EVPN core is not forwarded on the ICL. • Incoming traffic from the ICL is not forwarded to the EVPN core.
South bound (PE1 forwards BUM packet to PE2 and PE3).	PE2 and PE3 both receive a copy of the BUM packet and flood the packet out of all of their local interfaces, including the ICL.	PE2 and PE3 both forward the BUM packet out of the ICL, which results in packet duplication and loops.	

Split Horizon

In the use cases shown in Figure 14 on page 196 and Figure 15 on page 197, split horizon prevents multiple copies of a BUM packet from being forwarded to a CE device (satellite device). However, the EVPN-MPLS and MC-LAG split horizon implementations contradict each other, which causes an issue. Table 16 on page 199 explains the issue and how Juniper Networks resolves it in its implementation of the EVPN-MPLS interworking feature.

Table 16: BUM Traffic: Split Horizon-Related Issue and Resolution

BUM Traffic Direction	EVPN Interworking with Junos Fusion Enterprise and MC-LAG Logic	Issue	Juniper Networks Implementation Approach
North bound (PE2 receives BUM packet from a locally attached dual-homed interface).	• Per EVPN-MPLS forwarding logic: • Only the designated forwarder (DF) for the Ethernet segment (ES) can forward BUM traffic. • The local bias rule, in which the local peer forwards the BUM packet and the remote peer drops it, is not supported. • Per MC-LAG forwarding logic, local bias is supported.	The EVPN-MPLS and MC-LAG forwarding logic contradicts each other and can prevent BUM traffic from being forwarded to the ES.	Support local bias, thereby ignoring the DF and non-DF status of the port for locally switched traffic.
South bound (PE1 forwards BUM packet to PE2 and PE3).	Traffic received from PE1 follows the EVPN DF and non-DF forwarding rules for a mulithomed ES.	None.	Not applicable.

MAC Learning

EVPN and MC-LAG use the same method for learning MAC addresses—namely, a PE device learns MAC addresses from its local interfaces and synchronizes the addresses to its peers. However, given that both EVPN and MC-LAG are synchronizing the addresses, an issue arises.

Table 17 on page 200 describes the issue and how the EVPN-MPLS interworking implementation prevents the issue. The use cases shown in Figure 14 on page 196 and Figure 15 on page 197 illustrate the issue. In both use cases, PE1, PE2, and PE3 are EVPN peers, and PE2 and PE3 are MC-LAG peers.

Table 17: MAC Learning: EVPN and MC-LAG Synchronization Issue and Implementation Details

MAC Synchronization Use Case	EVPN Interworking with Junos Fusion Enterprise and MC-LAG Logic	Issue	Juniper Networks Implementation Approach
MAC addresses learned locally on single- or dual-homed interfaces on PE2 and PE3.	• Between the EVPN peers, MAC addresses are synchronized using the EVPN BGP control plane. • Between the MC-LAG peers, MAC addresses are synchronized using the MC-LAG ICCP control plane.	PE2 and PE3 function as both EVPN peers and MC-LAG peers, which result in these devices having multiple MAC synchronization paths.	• For PE1: use MAC addresses synchronized by EVPN BGP control plane. • For PE2 and PE3: use MAC addresses synchronized by MC-LAG ICCP control plane.
MAC addresses learned locally on single- or dual-homed interfaces on PE1.	Between the EVPN peers, MAC addresses are synchronized using the EVPN BGP control plane.	None.	Not applicable.

Handling Down Link Between Cascade and Uplink Ports in Junos Fusion Enterprise

NOTE: This section applies only to EVPN-MPLS interworking with a Junos Fusion Enterprise.

In the Junos Fusion Enterprise shown in Figure 14 on page 196, assume that aggregation device PE2 receives a BUM packet from PE1 and that the link between the cascade port on PE2 and the corresponding uplink port on satellite device SD1 is down. Regardless of whether the BUM packet is handled by MC-LAG or EVPN multihoming active-active, the result is the same—the packet is forwarded via the ICL interface to PE3, which forwards it to dual-homed SD1.

To further illustrate how EVPN with multihoming active-active handles this situation with dual-homed SD1, assume that the DF interface resides on PE2 and is associated with the down link and that the non-DF interface resides on PE3. Typically, per EVPN with multihoming active-active forwarding logic, the non-DF interface drops the packet. However, because of the down link associated with the DF interface, PE2 forwards the BUM packet via the ICL to PE3, and the non-DF interface on PE3 forwards the packet to SD1.

Layer 3 Gateway Support

The EVPN-MPLS interworking feature supports the following Layer 3 gateway functionality for extended bridge domains and VLANs:

- Integrated routing and bridging (IRB) interfaces to forward traffic between the extended bridge domains or VLANs.
- Default Layer 3 gateways to forward traffic from a physical (bare-metal) server in an extended bridge domain or VLAN to a physical server or virtual machine in another extended bridge domain or VLAN.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.4R1	Starting with Junos OS Release 17.4R1, you can use Ethernet VPN (EVPN) to extend a Junos Fusion Enterprise or multichassis link aggregation group (MC-LAG) network over an MPLS network to a data center or campus network.

Example: EVPN-MPLS Interworking With Junos Fusion Enterprise

IN THIS SECTION

This example shows how to use Ethernet VPN (EVPN) to extend a Junos Fusion Enterprise over an MPLS network to a geographically distributed campus or enterprise network.

EVPN-MPLS interworking is supported with a Junos Fusion Enterprise, which is based on a multichassis link aggregation group (MC-LAG) infrastructure to provide redundancy for the EX9200 switches that function as aggregation devices.

The aggregation devices in the Junos Fusion Enterprise are connected to a provider edge (PE) device in an MPLS network. The PE device can be either an MX Series router or an EX9200 switch.

This example shows how to configure the aggregation devices in the Junos Fusion Enterprise and the PE device in the MPLS network to interwork with each other.

Requirements

This example uses the following hardware and software components:

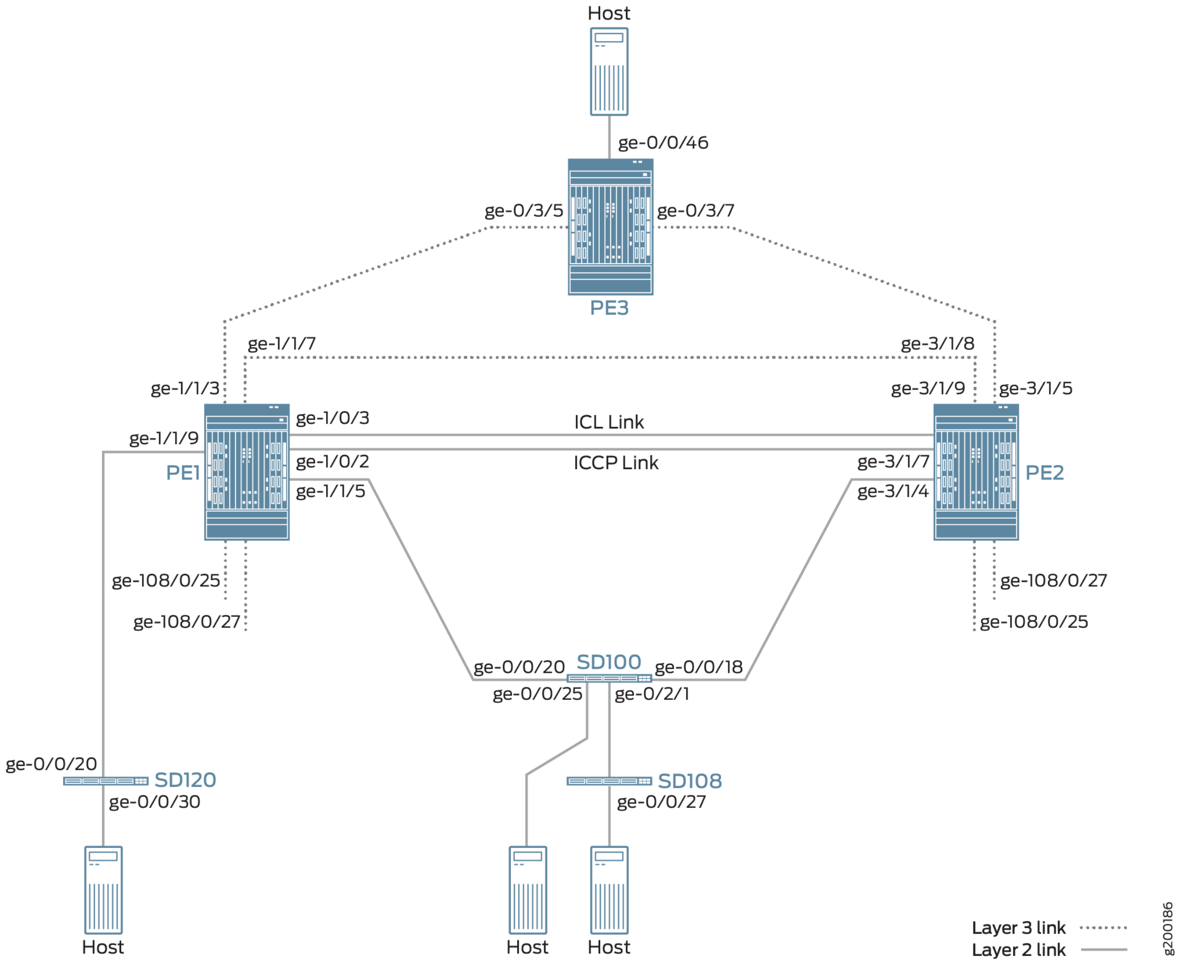
- Three EX9200 switches:
  - PE1 and PE2, which both function as aggregation devices in the Junos Fusion Enterprise and EVPN BGP peers in the EVPN-MPLS overlay network.
  - PE3, which functions as an EVPN BGP peer in the EVPN-MPLS overlay network.
- The EX9200 switches are running Junos OS Release 17.4R1 or later software.

NOTE: Although the Junos Fusion Enterprise includes three satellite devices, this example focuses on the configuration of the PE1, PE2, and PE3. For more information about configuring satellite devices, see Configuring or Expanding a Junos Fusion Enterprise.

Overview and Topology

Figure 16 on page 203 shows a Junos Fusion Enterprise with dual aggregation devices PE1 and PE2. The aggregation devices are connected using an interchassis link (ICL) and communicate with each other using the Inter-Chassis Control Protocol (ICCP).

Figure 16: EVPN-MPLS Interworking with Junos Fusion Enterprise



The Junos Fusion Enterprise also includes three satellite devices. Satellite device SD120 is a standalone satellite device that has a single-homed connection to PE1. Satellite devices SD100 and SD108 are included in a cluster named Cluster_100_108. SD100 is the only cluster member with a connection to an aggregation device, in this case, multhomed connections to PE1 and PE2.

The topology in Figure 16 on page 203 also includes PE3, which is positioned at the edge of an MPLS network. PE3 functions as the gateway between the Junos Fusion Enterprise network and a geographically distributed campus or enterprise network. PE1, PE2, and PE3 run EVPN, which enables hosts in the Junos Fusion Enterprise network to communicate with hosts in the campus or enterprise network by way of the intervening MPLS network.

From the perspective of the EVPN-MPLS interworking feature, PE3 functions solely as an EVPN BGP peer, and PE1 and PE2 in the Junos Fusion Enterprise have dual roles:

- Aggregation devices in the Junos Fusion Enterprise.
- EVPN BGP peers in the EVPN-MPLS network.

Because of the dual roles, PE1 and PE2 are configured with Junos Fusion Enterprise, EVPN, BGP, and MPLS attributes.

Table 18 on page 204 outlines key Junos Fusion Enterprise and EVPN (BGP and MPLS) attributes configured on PE1, PE2, and PE3.

Table 18: Key Junos Fusion Enterprise and EVPN (BGP and MPLS) Attributes Configured on PE1, PE2, and PE3

Key Attributes	PE1	PE2	PE3
Junos Fusion Enterprise Attributes			
Interfaces	ICL: ge-1/0/3 ICCP: ge-1/0/2	ICL: ge-3/1/9 ICCP: ge-3/1/7	Not applicable
EVPN-MPLS			
Interfaces	Connection to PE3: ge-1/1/3 Connection to PE2: ge-1/1/7	Connection to PE3: ge-3/1/5 Connection to PE1: ge-3/1/8	Connection to PE1: ge-0/3/5 Connection to PE2: ge-0/3/7
IP addresses	BGP peer address: 10.25.0.1	BGP peer address: 10.25.0.2	BGP peer address: 10.25.0.3
Autonomous system	100	100	100
Virtual switch routing instances	evpn1	evpn1	evpn1

Note the following about the EVPN-MPLS interworking feature and its configuration:

- You must configure Ethernet segment identifiers (ESIs) on the dual-homed extended ports in the Junos Fusion Enterprise. The ESIs enable EVPN to identify the dual-homed extended ports.
- The only type of routing instance that is supported is the virtual switch instance (`set routing-instances` *`name`* `instance-type virtual-switch`).
- Only one virtual switch instance is supported with Junos Fusion Enterprise.

- On the aggregation devices in the Junos Fusion Enterprise, you must include the `bgp-peer` configuration statement in the `[edit routing-instances` *`name`* `protocols evpn mclag]` hierarchy level. This configuration statement enables the interworking of EVPN-MPLS with Junos Fusion Enterprise on the aggregation devices.

- Address Resolution Protocol (ARP) suppression is not supported.

Aggregation Device (PE1 and PE2) Configuration

IN THIS SECTION

To configure aggregation devices PE1 and PE2, perform these tasks.

NOTE: This section focuses on enabling EVPN-MPLS on PE1 and PE2. As a result, the Junos Fusion Enterprise configuration on PE1 and PE2 is performed without the use of the configuration synchronization feature. For information about configuration synchronization, see Understanding Configuration Synchronization.

CLI Quick Configuration

PE1: Junos Fusion Enterprise Configuration

```
set interfaces ge-1/1/9 cascade-port
set interfaces ge-1/1/5 cascade-port
set chassis satellite-management fpc 120 cascade-ports ge-1/1/9
set chassis satellite-management cluster Cluster_100_108 cluster-id 2
set chassis satellite-management cluster Cluster_100_108 cascade-ports ge-1/1/5
set chassis satellite-management cluster Cluster_100_108 fpc 100 alias SD100
set chassis satellite-management cluster Cluster_100_108 fpc 100 system-id 88:e0:f3:1f:3d:50
set chassis satellite-management cluster Cluster_100_108 fpc 108 alias SD108
set chassis satellite-management cluster Cluster_100_108 fpc 108 system-id 88:e0:f3:1f:c8:d1
set chassis satellite-management cluster Cluster_100_108 fpc 100 member-id 1
set chassis satellite-management cluster Cluster_100_108 fpc 108 member-id 8
set chassis satellite-management upgrade-groups upgrade_120 satellite 120
set chassis satellite-management upgrade-groups upgrade_100 satellite 100
set chassis satellite-management redundancy-groups rg1 redundancy-group-id 2
set chassis satellite-management redundancy-groups chassis-id 1
set chassis satellite-management redundancy-groups rg1 peer-chassis-id 2 inter-chassis-link
ge-1/0/3
set chassis satellite-management redundancy-groups rg1 cluster Cluster_100_108
set interfaces ge-1/0/2 description iccp-link
set interfaces ge-1/0/2 unit 0 family inet address 10.20.20.1/24
set interfaces ge-1/0/3 description icl-link
set interfaces ge-1/0/3 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-1/0/3 unit 0 family ethernet-switching vlan members 100
set switch-options service-id 1
```

PE1: EVPN-MPLS Configuration

```
set interfaces lo0 unit 0 family inet address 10.25.0.1/32
set interfaces ge-1/1/3 unit 0 family inet address 10.0.1.1/30
set interfaces ge-1/1/3 unit 0 family mpls
set interfaces ge-1/1/7 unit 0 family inet address 10.0.3.1/30
set interfaces ge-1/1/7 unit 0 family mpls
set interfaces ge-108/0/25 unit 0 esi 00:01:02:03:04:00:01:02:04:26
set interfaces ge-108/0/25 unit 0 esi all-active
set interfaces ge-108/0/25 unit 0 family ethernet-switching vlan members v100
set interfaces ge-108/0/27 unit 0 esi 00:01:02:03:04:00:01:02:04:28
set interfaces ge-108/0/27 unit 0 esi all-active
set interfaces ge-108/0/27 unit 0 family ethernet-switching vlan members v100
set routing-options router-id 10.25.0.1
set routing-options autonomous-system 100
set protocols mpls interface lo0.0
set protocols mpls interface ge-1/1/3.0
set protocols mpls interface ge-1/1/7.0
set protocols bgp local-address 10.25.0.1
set protocols bgp peer-as 100
set protocols bgp local-as 100
set protocols bgp group evpn-mes type internal
set protocols bgp group evpn-mes family evpn signaling
set protocols bgp group evpn-mes peer-as 100
set protocols bgp group evpn-mes neighbor 10.25.0.2
set protocols bgp group evpn-mes neighbor 10.25.0.3
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-1/1/3.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface ge-1/1/7.0
set protocols ldp interface lo0.0
set protocols ldp interface ge-1/1/3.0
set protocols ldp interface ge-1/1/7.0
set routing-instances evpn1 instance-type virtual-switch
set routing-instances evpn1 interface ge-108/0/25.0
set routing-instances evpn1 interface ge-108/0/27.0
set routing-instances evpn1 interface ge-1/0/3.0
set routing-instances evpn1 route-distinguisher 10.25.0.1:1
set routing-instances evpn1 vrf-target target:100:1
set routing-instances evpn1 protocols evpn label-allocation per-instance
set routing-instances evpn1 protocols evpn extended-vlan-list 100
set routing-instances evpn1 protocols evpn mclag bgp-peer 10.25.0.2
set routing-instances evpn1 switch-options service-id 2
set routing-instances evpn1 vlans v100 vlan-id 100
```

PE2: Junos Fusion Enterprise Configuration

```
set interfaces ge-3/1/4 cascade-port
set chassis satellite-management cluster Cluster_100_108 cluster-id 2
set chassis satellite-management cluster Cluster_100_108 cascade-ports ge-3/1/4
set chassis satellite-management cluster Cluster_100_108 fpc 100 alias SD100
set chassis satellite-management cluster Cluster_100_108 fpc 100 system-id 88:e0:f3:1f:3d:50
set chassis satellite-management cluster Cluster_100_108 fpc 108 alias SD108
set chassis satellite-management cluster Cluster_100_108 fpc 108 system-id 88:e0:f3:1f:c8:d1
set chassis satellite-management cluster Cluster_100_108 fpc 100 member-id 1
set chassis satellite-management cluster Cluster_100_108 fpc 108 member-id 8
set chassis satellite-management upgrade-groups upgrade_100 satellite 100
set chassis satellite-management redundancy-groups rg1 redundancy-group-id 2
set chassis satellite-management redundancy-groups chassis-id 2
set chassis satellite-management redundancy-groups rg1 peer-chassis-id 1 inter-chassis-link
ge-3/1/9
set chassis satellite-management redundancy-groups rg1 cluster Cluster_100_108
set interfaces ge-3/1/7 description iccp-link
set interfaces ge-3/1/7 unit 0 family inet address 10.20.20.2/24
set interfaces ge-3/1/9 description icl-link
set interfaces ge-3/1/9 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-3/1/9 unit 0 family ethernet-switching vlan members 100
set switch-options service-id 1
```

PE2: EVPN-MPLS Configuration

```
set interfaces lo0 unit 0 family inet address 10.25.0.2/32
set interfaces ge-3/1/5 unit 0 family inet address 10.0.4.2/30
set interfaces ge-3/1/5 unit 0 family mpls
set interfaces ge-3/1/8 unit 0 family inet address 10.0.3.2/30
set interfaces ge-3/1/8 unit 0 family mpls
set interfaces irb unit 0 family inet address 10.5.5.1/24 virtual-gateway-address 10.5.5.5
set interfaces ge-108/0/25 unit 0 esi 00:01:02:03:04:00:01:02:04:26
set interfaces ge-108/0/25 unit 0 esi all-active
set interfaces ge-108/0/25 unit 0 family ethernet-switching vlan members v100
set interfaces ge-108/0/27 unit 0 esi 00:01:02:03:04:00:01:02:04:28
set interfaces ge-108/0/27 unit 0 esi all-active
set interfaces ge-108/0/27 unit 0 family ethernet-switching vlan members v100
set routing-options router-id 10.25.0.2
set routing-options autonomous-system 100
set protocols mpls interface lo0.0
set protocols mpls interface ge-3/1/5.0
set protocols mpls interface ge-3/1/8.0
set protocols bgp local-address 10.25.0.2
set protocols bgp peer-as 100
set protocols bgp local-as 100
set protocols bgp group evpn-mes type internal
set protocols bgp group evpn-mes family evpn signaling
set protocols bgp group evpn-mes peer-as 100
set protocols bgp group evpn-mes neighbor 10.25.0.1
set protocols bgp group evpn-mes neighbor 10.25.0.3
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-3/1/5.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface ge-3/1/8.0
set protocols ldp interface lo0.0
set protocols ldp interface ge-3/1/5.0
set protocols ldp interface ge-3/1/8.0
set routing-instances evpn1 instance-type virtual-switch
set routing-instances evpn1 interface ge-108/0/25.0
set routing-instances evpn1 interface ge-108/0/27.0
set routing-instances evpn1 interface ge-3/1/9.0
set routing-instances evpn1 route-distinguisher 10.25.0.2:1
set routing-instances evpn1 vrf-target target:100:1
set routing-instances evpn1 protocols evpn label-allocation per-instance
set routing-instances evpn1 protocols evpn extended-vlan-list 100
set routing-instances evpn1 protocols evpn mclag bgp-peer 10.25.0.1
set routing-instances evpn1 switch-options service-id 2
set routing-instances evpn1 vlans v100 vlan-id 100
set routing-instances evpn1 vlans v100 l3-interface irb.0
```

PE1: Configuring Junos Fusion Enterprise

Step-by-Step Procedure

1. Configure the cascade ports.

   ```
   [edit]
   user@switch# set interfaces ge-1/1/9 cascade-port
   user@switch# set interfaces ge-1/1/5 cascade-port
   ```

2. Configure the FPC slot ID for standalone satellite device SD120 and map it to a cascade port.

   ```
   [edit]
   user@switch# set chassis satellite-management fpc 120 cascade-ports ge-1/1/9
   ```

3. Create a satellite device cluster, and assign a name and a cluster ID to it.

   ```
   [edit]
   user@switch# set chassis satellite-management cluster Cluster_100_108 cluster-id 2
   ```

4. Define the cascade ports associated with the satellite device cluster.

   ```
   [edit]
   user@switch# set chassis satellite-management cluster Cluster_100_108 cascade-ports ge-1/1/5
   user@switch# set chassis satellite-management cluster Cluster_100_108 cascade-ports ge-1/1/9
   ```

5. Configure the FPC slot ID number, and map it to the MAC address of satellite devices SD100 and SD108, respectively.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 alias SD100
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 system-id
88:e0:f3:1f:3d:50
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 alias SD108
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 system-id
88:e0:f3:1f:c8:d1
```

6. Assign a member ID to each satellite device in the satellite device cluster.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 member-id 1
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 member-id 8
```

7. Create two satellite software upgrade groups—one that includes satellite device SD120 and another that includes satellite device SD100.

```
[edit]
user@switch# set chassis satellite-management upgrade-groups upgrade_120 satellite 120
user@switch# set chassis satellite-management upgrade-groups upgrade_100 satellite 100
```

8. Create and configure a redundancy group, which includes the aggregation devices and satellite devices in Cluster_100_108.

```
[edit]
user@switch# set chassis satellite-management redundancy-groups rg1 redundancy-group-id 2
user@switch# set chassis satellite-management redundancy-groups chassis-id 1
user@switch# set chassis satellite-management redundancy-groups rg1 peer-chassis-id 2 inter-
chassis-link ge-1/0/3
user@switch# set chassis satellite-management redundancy-groups rg1 cluster Cluster_100_108
```

9. Configure the ICL and ICCP links.

```
[edit]
user@switch# set interfaces ge-1/0/2 description iccp-link
```

```
user@switch# set interfaces ge-1/0/2 unit 0 family inet address 10.20.20.1/24
user@switch# set interfaces ge-1/0/3 description icl-link
user@switch# set interfaces ge-1/0/3 unit 0 family ethernet-switching interface-mode trunk
user@switch# set interfaces ge-1/0/3 unit 0 family ethernet-switching vlan members 100
user@switch# set switch-options service-id 1
```

NOTE: While this step shows the configuration of interface ge-1/0/2, which is designated as the ICCP interface, it does not show how to configure the ICCP attributes on interface ge-1/0/2. By default, ICCP is automatically provisioned in a Junos Fusion Enterprise using dual aggregation devices. For more information about the automatic provisioning of ICCP, see Configuring or Expanding a Junos Fusion Enterprise.

PE1: Configuring EVPN-MPLS

Step-by-Step Procedure

1. Configure the loopback interface and the interfaces connected to the other PE devices.

```
[edit]
user@switch# set interfaces lo0 unit 0 family inet address 10.25.0.1/32
user@switch# set interfaces ge-1/1/3 unit 0 family inet address 10.0.1.1/30
user@switch# set interfaces ge-1/1/3 unit 0 family mpls
user@switch# set interfaces ge-1/1/7 unit 0 family inet address 10.0.3.1/30
user@switch# set interfaces ge-1/1/7 unit 0 family mpls
```

2. Configure the extended ports with EVPN multihoming in active-active mode, an ESI, and map the ports to VLAN v100..

```
[edit]
user@switch# set interfaces ge-108/0/25 unit 0 esi 00:01:02:03:04:00:01:02:04:26
user@switch# set interfaces ge-108/0/25 unit 0 esi all-active
user@switch# set interfaces ge-108/0/25 unit 0 family ethernet-switching vlan members v100
user@switch# set interfaces ge-108/0/27 unit 0 esi 00:01:02:03:04:00:01:02:04:28
user@switch# set interfaces ge-108/0/27 unit 0 esi all-active
user@switch# set interfaces ge-108/0/27 unit 0 family ethernet-switching vlan members v100
```

3. Assign a router ID and the autonomous system in which PE1, PE2, and PE3 reside.

```
[edit]
user@switch# set routing-options router-id 10.25.0.1
user@switch# set routing-options autonomous-system 100
```

4. Enable MPLS on the loopback interface and interfaces ge-1/1/3.0 and ge-1/1/7.0.

```
[edit]
user@switch# set protocols mpls interface lo0.0
user@switch# set protocols mpls interface ge-1/1/3.0
user@switch# set protocols mpls interface ge-1/1/7.0
```

5. Configure an IBGP overlay that includes PE1, PE2, and PE3.

```
[edit]
user@switch# set protocols bgp local-address 10.25.0.1
user@switch# set protocols bgp peer-as 100
user@switch# set protocols bgp local-as 100
user@switch# set protocols bgp group evpn-mes type internal
user@switch# set protocols bgp group evpn-mes family evpn signaling
user@switch# set protocols bgp group evpn-mes peer-as 100
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.2
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.3
```

6. Configure OSPF as the internal routing protocol for EVPN by specifying an area ID and interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ospf traffic-engineering
user@switch# set protocols ospf area 0.0.0.0 interface ge-1/1/3.0
user@switch# set protocols ospf area 0.0.0.0 interface lo0.0
user@switch# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
user@switch# set protocols ospf area 0.0.0.0 interface ge-1/1/7.0
```

7. Configure the Label Distribution Protocol (LDP) on the loopback interface and the interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ldp interface lo0.0
user@switch# set protocols ldp interface ge-1/1/3.0
user@switch# set protocols ldp interface ge-1/1/7.0
```

8. Configure a virtual switch routing instance for VLAN v100, and include the interfaces and other entities associated with the VLAN.

```
[edit]
user@switch# set routing-instances evpn1 instance-type virtual-switch
user@switch# set routing-instances evpn1 interface ge-108/0/25.0
user@switch# set routing-instances evpn1 interface ge-108/0/27.0
user@switch# set routing-instances evpn1 interface ge-1/0/3.0
user@switch# set routing-instances evpn1 route-distinguisher 10.25.0.1:1
user@switch# set routing-instances evpn1 vrf-target target:100:1
user@switch# set routing-instances evpn1 protocols evpn label-allocation per-instance
user@switch# set routing-instances evpn1 protocols evpn extended-vlan-list 100
user@switch# set routing-instances evpn1 protocols evpn mclag bgp-peer 10.25.0.2
user@switch# set routing-instances evpn1 switch-options service-id 2
user@switch# set routing-instances evpn1 vlans v100 vlan-id 100
```

PE2: Configuring Junos Fusion Enterprise

Step-by-Step Procedure

1. Configure the cascade port.

```
[edit]
user@switch# set interfaces ge-3/1/4 cascade-port
```

2. Create a satellite device cluster, and assign a name and a cluster ID to it.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 cluster-id 2
```

3. Define the cascade port associated with the satellite device cluster.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 cascade-ports ge-3/1/4
```

4. Configure the FPC slot ID number, and map it to the MAC address of satellite devices SD100 and SD108, respectively.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 alias SD100
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 system-id
88:e0:f3:1f:3d:50
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 alias SD108
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 system-id
88:e0:f3:1f:c8:d1
```

5. Assign a member ID to each satellite device in the satellite device cluster.

```
[edit]
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 100 member-id 1
user@switch# set chassis satellite-management cluster Cluster_100_108 fpc 108 member-id 8
```

6. Create a satellite software upgrade group that includes satellite device SD100.

```
[edit]
user@switch# set chassis satellite-management upgrade-groups upgrade_100 satellite 100
```

7. Create and configure a redundancy group, which includes the aggregation devices and satellite devices in Cluster_100_108.

```
[edit]
user@switch# set chassis satellite-management redundancy-groups rg1 redundancy-group-id 2
user@switch# set chassis satellite-management redundancy-groups chassis-id 2
user@switch# set chassis satellite-management redundancy-groups rg1 peer-chassis-id 1inter-
chassis-link ge-3/1/9
user@switch# set chassis satellite-management redundancy-groups rg1 cluster Cluster_100_108
```

8. Configure the ICL and ICCP links.

```
[edit]
user@switch# set interfaces ge-3/1/7 description iccp-link
user@switch# set interfaces ge-3/1/7 unit 0 family inet address 10.20.20.2/24
user@switch# set interfaces ge-3/1/9 description icl-link
user@switch# set interfaces ge-3/1/9 unit 0 family ethernet-switching interface-mode trunk
user@switch# set interfaces ge-3/1/9 unit 0 family ethernet-switching vlan members 100
user@switch# set switch-options service-id 1
```

> **NOTE**: While this step shows the configuration of interface ge-3/1/7, which is designated as the ICCP interface, it does not show how to configure the ICCP attributes on interface ge-3/1/7. By default, ICCP is automatically provisioned in a Junos Fusion Enterprise using dual aggregation devices. For more information about the automatic provisioning of ICCP, see Configuring or Expanding a Junos Fusion Enterprise.

PE2: Configuring EVPN-MPLS

Step-by-Step Procedure

1. Configure the loopback interface, the interfaces connected to the other PE devices, and an IRB interface that is also configured as a default Layer 3 gateway.

```
[edit]
user@switch# set interfaces lo0 unit 0 family inet address 10.25.0.2/32
user@switch# set interfaces ge-3/1/5 unit 0 family inet address 10.0.4.2/30
user@switch# set interfaces ge-3/1/5 unit 0 family mpls
user@switch# set interfaces ge-3/1/8 unit 0 family inet address 10.0.3.2/30
user@switch# set interfaces ge-3/1/8 unit 0 family mpls
user@switch# set interfaces irb unit 0 family inet address 10.5.5.1/24 virtual-gateway-
address 10.5.5.5
```

2. Configure the extended ports with EVPN multihoming in active-active mode, an ESI, and map the ports to VLAN v100..

```
[edit]
user@switch# set interfaces ge-108/0/25 unit 0 esi 00:01:02:03:04:00:01:02:04:26
user@switch# set interfaces ge-108/0/25 unit 0 esi all-active
```

```
user@switch# set interfaces ge-108/0/25 unit 0 family ethernet-switching vlan members v100
user@switch# set interfaces ge-108/0/27 unit 0 esi 00:01:02:03:04:00:01:02:04:28
user@switch# set interfaces ge-108/0/27 unit 0 esi all-active
user@switch# set interfaces ge-108/0/27 unit 0 family ethernet-switching vlan members v100
```

3. Assign a router ID and the autonomous system in which PE1, PE2, and PE3 reside.

```
[edit]
user@switch# set routing-options router-id 10.25.0.2
user@switch# set routing-options autonomous-system 100
```

4. Enable MPLS on the loopback interface and interfaces ge-3/1/5.0 and ge-3/1/8.0.

```
[edit]
user@switch# set protocols mpls interface lo0.0
user@switch# set protocols mpls interface ge-3/1/5.0
user@switch# set protocols mpls interface ge-3/1/8.0
```

5. Configure an IBGP overlay that includes PE1, PE2, and PE3.

```
[edit]
user@switch# set protocols bgp local-address 10.25.0.2
user@switch# set protocols bgp peer-as 100
user@switch# set protocols bgp local-as 100
user@switch# set protocols bgp group evpn-mes type internal
user@switch# set protocols bgp group evpn-mes family evpn signaling
user@switch# set protocols bgp group evpn-mes peer-as 100
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.1
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.3
```

6. Configure OSPF as the internal routing protocol for EVPN by specifying an area ID and interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ospf traffic-engineering
user@switch# set protocols ospf area 0.0.0.0 interface ge-3/1/5.0
user@switch# set protocols ospf area 0.0.0.0 interface lo0.0
```

```
user@switch# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
user@switch# set protocols ospf area 0.0.0.0 interface ge-3/1/8.0
```

7. Configure the LDP on the loopback interface and the interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ldp interface lo0.0
user@switch# set protocols ldp interface ge-3/1/5.0
user@switch# set protocols ldp interface ge-3/1/8.0
```

8. Configure a virtual switch routing instance for VLAN v100, and include the interfaces and other entities associated with the VLAN.

```
[edit]
user@switch# set routing-instances evpn1 instance-type virtual-switch
user@switch# set routing-instances evpn1 interface ge-108/0/25.0
user@switch# set routing-instances evpn1 interface ge-108/0/27.0
user@switch# set routing-instances evpn1 interface ge-3/1/9.0
user@switch# set routing-instances evpn1 route-distinguisher 10.25.0.2:1
user@switch# set routing-instances evpn1 vrf-target target:100:1
user@switch# set routing-instances evpn1 protocols evpn label-allocation per-instance
user@switch# set routing-instances evpn1 protocols evpn extended-vlan-list 100
user@switch# set routing-instances evpn1 protocols evpn mclag bgp-peer 10.25.0.1
user@switch# set routing-instances evpn1 switch-options service-id 2
user@switch# set routing-instances evpn1 vlans v100 vlan-id 100
user@switch# set routing-instances evpn1 vlans v100 l3-interface irb.0
```

PE3 Configuration

IN THIS SECTION

CLI Quick Configuration

PE3: EVPN-MPLS Configuration

```
set interfaces lo0 unit 0 family inet address 10.25.0.3/32
set interfaces ge-0/3/5 unit 0 family inet address 10.0.1.2/30
set interfaces ge-0/3/5 unit 0 family mpls
set interfaces ge-0/3/7 unit 0 family inet address 10.0.4.1/30
set interfaces ge-0/3/7 unit 0 family mpls
set interfaces ge-0/0/46 unit 0 esi 00:01:02:03:04:00:01:02:04:12
set interfaces ge-0/0/46 unit 0 esi all-active
set interfaces ge-0/0/46 unit 0 family ethernet-switching vlan members 100
set routing-options router-id 10.25.0.3
set routing-options autonomous-system 100
set routing-options forwarding-table export evpn-pplb
set policy-options policy-statement evpn-pplb from protocol evpn
set policy-options policy-statement evpn-pplb then load-balance per-packet
set protocols mpls interface lo0.0
set protocols mpls interface ge-0/3/5.0
set protocols mpls interface ge-0/3/7.0
set protocols bgp local-address 10.25.0.3
set protocols bgp peer-as 100
set protocols bgp local-as 100
set protocols bgp group evpn-mes type internal
set protocols bgp group evpn-mes family evpn signaling
set protocols bgp group evpn-mes peer-as 100
set protocols bgp group evpn-mes neighbor 10.25.0.2
set protocols bgp group evpn-mes neighbor 10.25.0.1
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-0/3/5.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface ge-0/3/7.0
set protocols ldp interface lo0.0
set protocols ldp interface ge-0/3/5.0
set protocols ldp interface ge-0/3/7.0
set routing-instances evpn1 instance-type virtual-switch
set routing-instances evpn1 interface ge-0/0/46.0
set routing-instances evpn1 route-distinguisher 10.25.0.3:1
set routing-instances evpn1 vrf-target target:100:1
set routing-instances evpn1 protocols evpn label-allocation per-instance
set routing-instances evpn1 protocols evpn extended-vlan-list 100
set routing-instances evpn1 switch-options service-id 2
set routing-instances evpn1 vlans v100 vlan-id 100
```

PE3: Configuring EVPN-MPLS

Step-by-Step Procedure

1. Configure the interfaces on EVPN-MPLS interworking occurs.

```
[edit]
user@switch# set interfaces lo0 unit 0 family inet address 10.25.0.3/32
user@switch# set interfaces ge-0/3/5 unit 0 family inet address 10.0.1.2/30
user@switch# set interfaces ge-0/3/5 unit 0 family mpls
user@switch# set interfaces ge-0/3/7 unit 0 family inet address 10.0.4.1/30
user@switch# set interfaces ge-0/3/7 unit 0 family mpls
```

2. Configure interface ge-0/0/46 with EVPN multihoming in active-active mode, an ESI, and map the ports to VLAN v100..

```
[edit]
user@switch# set interfaces ge-0/0/46 unit 0 esi 00:01:02:03:04:00:01:02:04:12
user@switch# set interfaces ge-0/0/46 unit 0 esi all-active
user@switch# set interfaces ge-0/0/46 unit 0 family ethernet-switching vlan members 100
```

3. Assign a router ID and the autonomous system in which the PE1, PE2, and PE3 reside.

```
[edit]
user@switch# set routing-options router-id 10.25.0.2
user@switch# set routing-options autonomous-system 100
```

4. Enable per-packet load-balancing for EVPN routes when EVPN multihoming active-active mode is used.

```
[edit]
user@switch# set routing-options forwarding-table export evpn-pplb
user@switch# set policy-options policy-statement evpn-pplb from protocol evpn
user@switch# set policy-options policy-statement evpn-pplb then load-balance per-packet
```

5. Enable MPLS on the loopback interface and interfaces ge-0/3/5.0 and ge-0/3/7.0.

```
[edit]
user@switch# set protocols mpls interface lo0.0
user@switch# set protocols mpls interface ge-0/3/5.0
user@switch# set protocols mpls interface ge-0/3/7.0
```

6. Configure an IBGP overlay that includes PE1, PE2, and PE3.

```
[edit]
user@switch# set protocols bgp local-address 10.25.0.3
user@switch# set protocols bgp peer-as 100
user@switch# set protocols bgp local-as 100
user@switch# set protocols bgp group evpn-mes type internal
user@switch# set protocols bgp group evpn-mes family evpn signaling
user@switch# set protocols bgp group evpn-mes peer-as 100
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.2
user@switch# set protocols bgp group evpn-mes neighbor 10.25.0.1
```

7. Configure OSPF as the internal routing protocol for EVPN by specifying an area ID and interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ospf traffic-engineering
user@switch# set protocols ospf area 0.0.0.0 interface ge-0/3/5.0
user@switch# set protocols ospf area 0.0.0.0 interface lo0.0
user@switch# set protocols ospf area 0.0.0.0 interface fxp0.0 disable
user@switch# set protocols ospf area 0.0.0.0 interface ge-0/3/7.0
```

8. Configure the LDP on the loopback interface and the interfaces on which EVPN-MPLS is enabled.

```
[edit]
user@switch# set protocols ldp interface lo0.0
user@switch# set protocols ldp interface ge-0/3/5.0
user@switch# set protocols ldp interface ge-0/3/7.0
```

9. Configure a virtual switch routing instance for VLAN v100, and include the interfaces and other entities associated with the VLAN.

```
[edit]
user@switch# set routing-instances evpn1 instance-type virtual-switch
user@switch# set routing-instances evpn1 interface ge-0/0/46.0
user@switch# set routing-instances evpn1 route-distinguisher 10.25.0.3:1
user@switch# set routing-instances evpn1 vrf-target target:100:1
user@switch# set routing-instances evpn1 protocols evpn label-allocation per-instance
user@switch# set routing-instances evpn1 protocols evpn extended-vlan-list 100
user@switch# set routing-instances evpn1 switch-options service-id 2
user@switch# set routing-instances evpn1 vlans v100 vlan-id 100
```

RELATED DOCUMENTATION

Understanding EVPN-MPLS Interworking with Junos Fusion Enterprise and MC-LAG

CHAPTER 18

Storm Control on a Junos Fusion Enterprise

IN THIS CHAPTER

Understanding Storm Control on a Junos Fusion Enterprise

Storm control enables the switch to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—known as the storm control level or storm control bandwidth—is exceeded, preventing the packets from proliferating and degrading service. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces when the storm control level is exceeded.

Storm control configuration in a Junos Fusion Enterprise is identical for a standalone EX9200 switch. For more information, see Understanding Storm Control for Managing Traffic Levels on Switching Devices.

In a Junos Fusion Enterprise with dual aggregation devices there are special considerations that impact storm control functionality. The following requirements should be understood when configuring storm control for a Junos Fusion Enterprise:

- Broadcast, multicast, and unknown unicast packets received on the extended port of a satellite device can be forwarded to two different aggregation devices, so the storm control profile is applied to the cumulative traffic reaching a particular aggregation device, not the cumulative traffic received on the extended port of the satellite device.

- If the storm control level is exceeded and the resulting action is to shut down the port, the aggregation device which detects the storm brings down the extended port, and the status is synced to the peer aggregation device.

- The shutdown is applied at the physical interface level; in a standalone EX9200 switch, storm control shutdown is applied at the logical interface level.

- Executing the `clear ethernet-switching recovery-timeout` command on one aggregation device also clears the error on the other aggregation device.

- In the event of a shutdown, if the recovery timer is configured, the error is cleared on both aggregation devices when the timer expires.

CHAPTER 19

DHCP Snooping and Port Security on a Junos Fusion Enterprise

IN THIS CHAPTER

Understanding Port Security Features on a Junos Fusion Enterprise

Port security features help protect the access ports on your device against attacks such as address spoofing (forging) and Layer 2 denial of service. The switching device monitors DHCP messages sent from untrusted hosts and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database. Only hosts that can be verified using this database are allowed access to the network.

The following port security features are supported in a Junos Fusion Enterprise:

- DHCP snooping
- DHCPv6 snooping
- Dynamic ARP inspection (DAI)
- IP source guard
- IPv6 source guard
- IPv6 neighbor discovery (ND) inspection
- IPv6 router advertisement (RA) guard

Configuration for DHCP snooping and other port security features in a Junos Fusion Enterprise is identical for a standalone EX9200 switch. The range of port security configuration options are beyond the scope of this document. For additional information, see Configuring Port Security Features and the Port Security User Guide for EX9200 Switches.

In a Junos Fusion Enterprise with dual aggregation devices, there are special considerations that impact the DHCP snooping database. The following requirements should be understood when configuring DHCP port security features for a Junos Fusion Enterprise:

- The DHCP snooping database is synchronized across aggregation devices. Synchronization is automatic for all dual-homed clients; there is no manual configuration required to sync the DHCP snooping database.

  NOTE: DHCP relay and DHCP server bindings are not synchronized.

- DAI and ND inspection statistics are synchronized on both aggregation devices.

- DHCP port security configuration must match on both aggregation devices, so DHCP port security features should be configured using configuration groups that are applied to both aggregation devices using commit synchronization. See "Understanding Configuration Synchronization in a Junos Fusion" on page 27 and "Enabling Configuration Synchronization Between Aggregation Devices in a Junos Fusion" on page 88.

- Executing the `clear dhcp-security binding` command on one aggregation device also clears the bindings on the other aggregation device.

- DHCP port security features are not supported for single-homed clients in a dual-aggregation device topology, since the DHCP snooping database is synchronized only for dual-homed clients.

CHAPTER 20

MAC Limiting and Persistent MAC Learning on a Junos Fusion Enterprise

IN THIS CHAPTER

Understanding MAC Address Limiting and Persistent MAC Learning on a Junos Fusion Enterprise

IN THIS SECTION

MAC limiting enhances port security by limiting the number of MAC addresses that can be learned within a VLAN, which prevents flooding of the Ethernet switching table. You can configure MAC limiting to drop packets or to shut down interfaces when the MAC limit is exceeded.

Persistent MAC learning—also called sticky MAC addresses—enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online, preventing traffic loss for trusted workstations.

MAC limiting and persistent MAC learning configuration in a Junos Fusion Enterprise is identical for a standalone EX9200 switch. For more information on MAC limiting, see Understanding MAC Limiting. For more information on persistent MAC learning, see Understanding Persistent MAC Learning (Sticky MAC).

In a Junos Fusion Enterprise, there are special considerations that impact MAC limiting and persistent MAC learning functionality.

MAC Address Limiting on a Junos Fusion Enterprise

The following actions are possible when the MAC limit is reached on an interface:

- None—No impact on functionality of the aggregation device or the satellite device. Traffic is forwarded from the satellite device to the aggregation device.
- Shutdown—The extended port on the satellite device is shutdown when the MAC limit is reached on the aggregation device.
- Drop—The unlearnt source MAC packet is forwarded by the satellite device and dropped on the aggregation device.

The following requirements should be understood when configuring MAC address limiting for a Junos Fusion Enterprise with dual aggregation devices:

- There is the potential for MAC addresses received on an extended port to be forwarded to different aggregation devices. To prevent inconsistency, the learned MAC addresses are synchronized across both aggregation devices. If one aggregation device is not able to install a MAC address due to MAC limiting, that MAC address is deleted from the peer aggregation device.
- For the shutdown action, the shutdown on extended ports is applied at the physical interface level; in a standalone EX9200 switch, MAC limiting shutdown is applied at the logical interface level.
- Executing the `clear ethernet-switching recovery-timeout` command on one aggregation device also clears the error on the other aggregation device.
- In the event of a shutdown, if the recovery timer is configured, the error is cleared on both aggregation devices when the timer expires.

Persistent MAC Learning on a Junos Fusion Enterprise

The following requirements should be understood when configuring persistent MAC learning for a Junos Fusion Enterprise with dual aggregation devices:

- MAC addresses learnt locally or remotely are treated as persistent entries and saved in the persistent file on both aggregation devices.
- Persistent MAC learning cannot be enabled on the ICL interface. This is enforced by commit check.
- When persistent MAC learning is configured on extended ports of a single-homed satellite device, MAC addresses learned locally are learned as persistent addresses, and MAC addresses learned on the peer are learned as remote dynamic addresses.
- Clearing the `persistent-mac` on one aggregation device also deletes the entry from other aggregation device.

If you move a device within your network that has a persistent MAC address entry on the switch, use the `clear ethernet-switching table persistent-mac` command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port on which it was learned, then the new port will not learn the MAC address of the device and the device will not be able to connect.

If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.