

Junos Fusion Provider Edge User Guide

Published
2025-12-16

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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 Provider Edge User Guide
Copyright © 2025 Juniper Networks, Inc. All rights reserved.

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

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | vii

1

Junos Fusion Provider Edge

Junos Fusion Provider Edge Overview | 2

Junos Fusion Provider Edge Overview | 2

Understanding Junos Fusion Provider Edge Components | 4

Understanding Satellite Device Clustering in a Junos Fusion | 10

Understanding Junos Fusion Ports | 14

Understanding Port-Based Authentication in a Junos Fusion Provider Edge | 19

Understanding Software in a Junos Fusion Provider Edge | 19

Understanding Junos Fusion Provider Edge Software and Hardware Requirements | 23

Understanding the Flow of Data Packets in a Junos Fusion Topology | 29

Understanding Satellite Policies in a Junos Fusion | 34

Junos Fusion Provider Edge Supported Protocols | 35

Local Switching on Junos Fusion Provider Edge | 44

Broadband Subscription Services on Junos Fusion | 48

Junos Fusion Provider Edge Configuration | 51

Configuring Junos Fusion Provider Edge | 51

Preparing the Aggregation Device | 51

Configuring the Cascade Ports on the Aggregation Device | 53

Configuring the FPC Slot Identifiers | 54

Configuring Software Upgrade Groups on the Aggregation Device | 55

Preparing the Satellite Device | 57

Adding Satellite Devices to the Junos Fusion Provider Edge | 59

Autoconverting a Switch into a Satellite Device | 59

Manually Converting a Switch into a Satellite Device | 62

Configuring a Switch into a Satellite Device Before Interconnecting It into a Junos Fusion Provider Edge | 65

Configuring Satellite Device Alarm Handling Using an Environment Monitoring Satellite Policy in a Junos Fusion | 67

Junos Fusion Provider Edge Administration | 71

Managing Satellite Software Upgrade Groups in a Junos Fusion | 71

- Creating a Satellite Software Upgrade Group | 72
- Adding Satellite Devices to a Satellite Software Upgrade Group | 72
- Removing a Satellite Device from a Satellite Software Upgrade Group | 73
- Modifying the Satellite Software Used by a Satellite Software Upgrade Group | 74
- Deleting Associated Satellite Software from a Satellite Software Upgrade Group | 75
- Deleting Satellite Software on the Aggregation Device | 76

Verifying Connectivity, Device States, Satellite Software Versions, and Operations in a Junos Fusion | 76

- Verifying a Junos Fusion Configuration | 77
- Verifying Basic Junos Fusion Connectivity | 78
- Verifying the Satellite Device Hardware Model | 80
- Verifying Cascade Port and Uplink Port State | 81
- Verifying That a Cascade Port Recognizes a Satellite Device | 85
- Verifying Extended Port Operation | 88
- Verifying the Satellite Software Version | 90
- Verifying the Devices and Software Used in a Satellite Software Upgrade Group | 92

Converting a Satellite Device in a Junos Fusion to a Standalone Device | 93

- Download Junos OS Software | 94
- Disable the Automatic Conversion Configuration | 95
- Install Junos OS Software on the Satellite Device | 96

Installing Junos OS Software on a Standalone Device Running Satellite Software | 98

Power over Ethernet, LLDP, and LLDP-MED on a Junos Fusion Provider Edge | 100

Understanding Power over Ethernet in a Junos Fusion | 100

Understanding LLDP and LLDP-MED on a Junos Fusion | 103

Configuring Power over Ethernet in a Junos Fusion | 105

- PoE Configurable Options | 105

- Enabling PoE | 107

- Disabling PoE | 107

- Setting the Power Management Mode | 108

- Setting the Maximum Power That Can Be Delivered from a PoE Interface | 109

- Setting the Guard Band | 109

- Setting the PoE Interface Priority | 110

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure) | 110

- PoE Power Budgets, Consumption, and Mode on Satellite Devices | 111

- PoE Interface Configuration and Status | 112

Monitoring Junos Fusion Provider Edge | 115

Connectivity Fault Management in Junos Fusion | 115

SNMP MIB Support on Junos Fusion Provider Edge | 117

Chassis MIB Support (Junos Fusion) | 117

Link Aggregation and Link Aggregation Control Protocol on Junos Fusion Provider Edge | 122

Understanding Link Aggregation and Link Aggregation Control Protocol in a Junos Fusion | 122

Configuring an Aggregated Ethernet Interface | 124

Configuring Junos OS for Supporting Aggregated Devices | 126

- Configuring Virtual Links for Aggregated Devices | 126

- Configuring LACP Link Protection at the Chassis Level | 128

- Enabling LACP Link Protection | 129

- Configuring System Priority | 129

- Configuring the Maximum Links Limit | 130

- Configuring PPM on Junos Fusion | 130

Uplink Failure Detection on Junos Fusion Provider Edge | 132

Overview of Uplink Failure Detection on a Junos Fusion | 132

Configuring Uplink Failure Detection on a Junos Fusion | 134

- Enabling Uplink Failure Detection on a Junos Fusion | 134

- Configuring a Candidate Uplink Port Policy | 136

- Configuring Candidate Uplink Port Policy Default Configuration | 136

- Configuring Candidate Uplink Port Policy Terms | 137

- Configuring an Uplink Port Group | 139

Multicast Replication on Junos Fusion Provider Edge | 140

Understanding Multicast Replication in a Junos Fusion | 140

Ingress Replication at the Aggregation Device to Satellite Devices | 144

Egress (Local) Replication on the Satellite Devices | 145

Configuring Egress (Local) Replication on a Junos Fusion | 151

Class of Service on Junos Fusion Provider Edge | 152

Understanding CoS on an MX Series Aggregation Device in Junos Fusion Provider Edge | 152

Configuring CoS on an MX Series Aggregation Device in Junos Fusion | 160

Configuring Behavior Aggregate Classifiers on Satellite Device Extended Ports | 160

Configuring Rewrite Rules on Satellite Device Extended Ports | 162

Configuring CoS Hierarchical Port Scheduling with Enhanced Transmission Selection on Satellite Device Ports | 163

Changing the Default Scheduling Policy on an Aggregated Device Cascade Port | 166

2

Configuration Statements and Operational Commands

Junos CLI Reference Overview | 172

About This Guide

Junos Fusion Provider Edge simplifies network administration by enabling customers to configure an aggregation device to manage thousands of ports on satellite devices. Use the topics on this page to understand Junos Fusion, configure the aggregation device , and to manage satellite devices.

1

PART

Junos Fusion Provider Edge

- Junos Fusion Provider Edge Overview | **2**
 - Junos Fusion Provider Edge Configuration | **51**
 - Junos Fusion Provider Edge Administration | **71**
 - Power over Ethernet, LLDP, and LLDP-MED on a Junos Fusion Provider Edge | **100**
 - Monitoring Junos Fusion Provider Edge | **115**
 - SNMP MIB Support on Junos Fusion Provider Edge | **117**
 - Link Aggregation and Link Aggregation Control Protocol on Junos Fusion Provider Edge | **122**
 - Uplink Failure Detection on Junos Fusion Provider Edge | **132**
 - Multicast Replication on Junos Fusion Provider Edge | **140**
 - Class of Service on Junos Fusion Provider Edge | **152**
-

Junos Fusion Provider Edge Overview

IN THIS CHAPTER

- Junos Fusion Provider Edge Overview | 2
- Understanding Junos Fusion Provider Edge Components | 4
- Understanding Satellite Device Clustering in a Junos Fusion | 10
- Understanding Junos Fusion Ports | 14
- Understanding Port-Based Authentication in a Junos Fusion Provider Edge | 19
- Understanding Software in a Junos Fusion Provider Edge | 19
- Understanding Junos Fusion Provider Edge Software and Hardware Requirements | 23
- Understanding the Flow of Data Packets in a Junos Fusion Topology | 29
- Understanding Satellite Policies in a Junos Fusion | 34
- Junos Fusion Provider Edge Supported Protocols | 35
- Local Switching on Junos Fusion Provider Edge | 44
- Broadband Subscription Services on Junos Fusion | 48

Junos Fusion Provider Edge Overview

Junos Fusion provides a method of significantly expanding the number of available network interfaces on a device—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*. Junos Fusion simplifies network administration because it appears to the larger network as a single, port-dense device that is managed using one IP address.

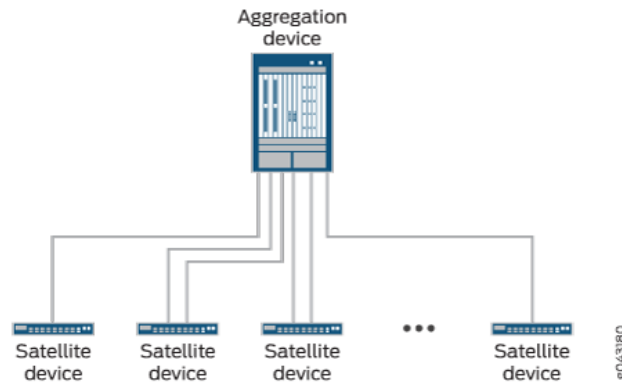
Junos Fusion Provider Edge brings the Junos Fusion technology to the service provider edge. For example in a Junos Fusion Provider Edge, MX Series 5G Universal Routing Platforms act as aggregation devices while EX4300 Series and QFX5100, QFX 5110, or QFX5200 Series switches act as satellite devices.

In a Junos Fusion Provider Edge topology, 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 Provider Edge. 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 Provider Edge topology.

Figure 1: Basic Junos Fusion Provider Edge Topology



The MX Series 5G Universal Routing Platform acting as the aggregation device in Junos Fusion Provider Edge 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 Provider Edge, and the network-facing interfaces on the satellite devices—*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 Provider Edge using multiple internal satellite management protocols. Network traffic can be forwarded between satellite devices through the aggregation device. Junos Fusion Provider Edge supports the IEEE 802.1BR standard.

Junos Fusion Provider Edge 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 Provider Edge 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 Provider Edge.

- Flexibility—You can easily expand the size of your Junos Fusion Provider Edge by adding satellite devices to it as your networking needs grow.
- Investment protection—In environments that need to expand because the capabilities of the aggregation device are maximized, a Junos Fusion Provider Edge can be a logical upgrade option because it enables the system to evolve with minimal disruption to the existing network and without having to remove the existing, previously purchased devices from the network.

RELATED DOCUMENTATION

[Understanding Junos Fusion Provider Edge Components | 4](#)

Understanding Junos Fusion Ports

Understanding the Flow of Data Packets in a Junos Fusion Topology

[Configuring Junos Fusion Provider Edge | 51](#)

Understanding Junos Fusion Provider Edge Components

IN THIS SECTION

- [Junos Fusion Topology | 5](#)
- [Aggregation Devices | 5](#)
- [Satellite Devices | 6](#)
- [Cascade Ports | 6](#)
- [Uplink Ports | 7](#)
- [Extended Ports | 8](#)
- [Understanding FPC Identifiers and Assignment in a Junos Fusion Fabric | 8](#)
- [Understanding Software in a Junos Fusion | 9](#)
- [Understanding Interface Naming in a Junos Fusion | 9](#)

This topic describes the components of a Junos Fusion Provider Edge.

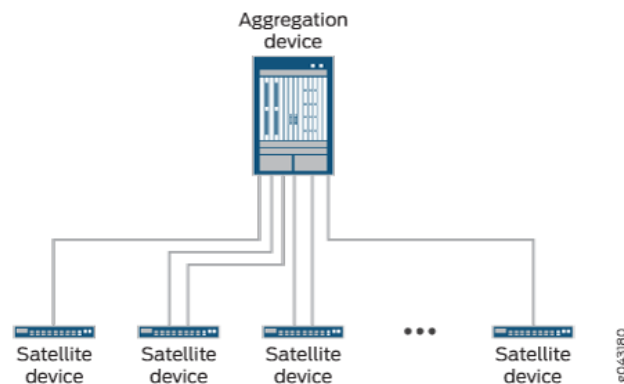
This topic covers:

Junos Fusion Topology

The 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.

See [Figure 2 on page 5](#) for an illustration of the Junos Fusion topology.

Figure 2: Junos Fusion Topology



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 single point of management 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 support features that are supported by the version of Junos OS running on the aggregation device.

Aggregation Devices

An aggregation device:

- Has at least one connection to each satellite device.
- Runs Junos OS software for the entire Junos Fusion.
- Manages the entire Junos Fusion. All Junos Fusion configuration management is handled on the aggregation device, including interface configuration of the satellite device interfaces.

The hardware specifications for aggregation devices in a Junos Fusion Provider Edge are discussed in greater detail in [Understanding Junos Fusion Provider Edge Software and Hardware Requirements](#).

Satellite Devices

A satellite device:

- Runs a version of satellite software after being converted into a satellite device.
- Has at least one direct connection to the 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 Provider Edge are discussed in greater detail in [Understanding Junos Fusion Provider Edge Software and Hardware Requirements](#).

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. All traffic passed between a satellite device and the aggregation device in a Junos Fusion traverses the cascade port.

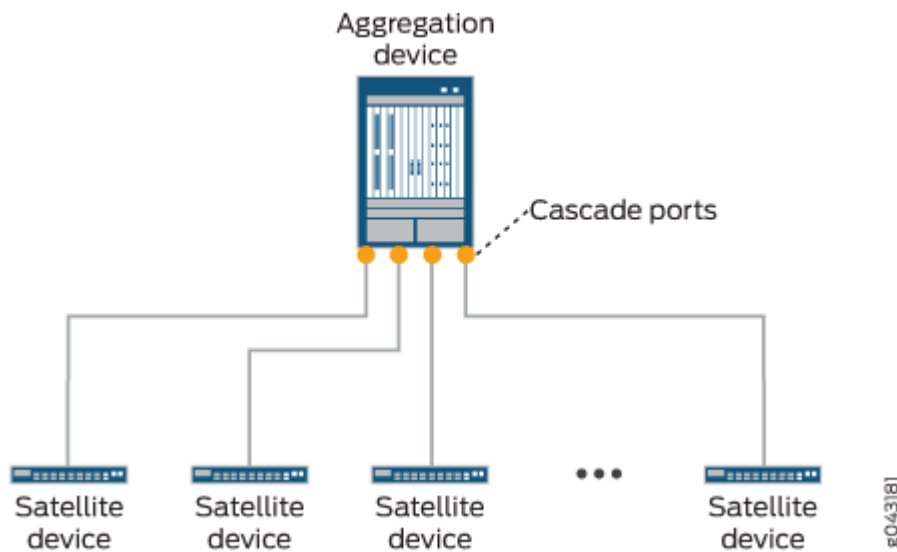
The link that connects an aggregation device to a satellite device has an interface on each end of the link. The interface on the aggregation device end of the link is a cascade port. The interface on the satellite device end of the link is an uplink port.

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 but not limited to a 10-Gbps SFP+ interface or a 40-Gbps QSFP+ interface, but any interface on the aggregation device that connects to the satellite device can be converted into a cascade port.

The location of the cascade ports in a Junos Fusion are illustrated in [Figure 3 on page 7](#).

Figure 3: Cascade Ports



The hardware specifications for cascade ports in a Junos Fusion Provider Edge are discussed in greater detail in [Understanding Junos Fusion Provider Edge 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.

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

An uplink port is typically but not limited to a 10-Gbps SFP+ interface or a 40-Gbps QSFP+ interface, but any 1-Gbps interface on the aggregation device that connects to the satellite device can also be converted into a cascade port.

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.

Understanding FPC Identifiers and Assignment in a Junos Fusion Fabric

In a Junos Fusion, each satellite device must have an FPC identifier (FPC ID).

The FPC ID 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 **ABCDEFGHJKLM** was assigned to FPC ID 110 using unique-ID based FPC identification, the satellite device with the serial number **ABCDEFGHJKLM** will always be associated with FPC ID 110 in the Junos Fusion. If the satellite device with the serial number **ABCDEFGHJKLM** 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.

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 due to an FPC ID association issue.

Understanding Software in a Junos Fusion

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 the feature set 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 Provider Edge" on page 19](#).

The software specifications for a Junos Fusion Provider Edge are discussed in greater detail in [Understanding Junos Fusion Provider Edge 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 an *xe* interface, for instance, remains *xe* regardless of whether the interface is or isn't 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 Fabric" on page 8](#).

For instance, built-in port 2 on PIC 0—a gigabit Ethernet interface that is acting as an extended port—on an EX4300 switch that is acting as FPC slot 101 would be identified as:

ge-101/0/2

RELATED DOCUMENTATION

Understanding Satellite Device Clustering in a Junos Fusion

IN THIS SECTION

- [Satellite Device Clustering Overview | 10](#)
- [Satellite Device Cluster Topology | 10](#)
- [Satellite Device Cluster Names and Identifiers | 11](#)
- [Satellite Device Cluster Uplink Interfaces | 11](#)
- [Cluster Interfaces | 12](#)
- [Satellite Device Cluster Software Management | 12](#)
- [FPC Identifiers and Extended Port Interfaces in a Satellite Device Cluster | 12](#)
- [Understanding 40-Gbps Interfaces with QSFP+ Transceiver Roles for Satellite Devices in a Satellite Device Cluster | 13](#)

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.

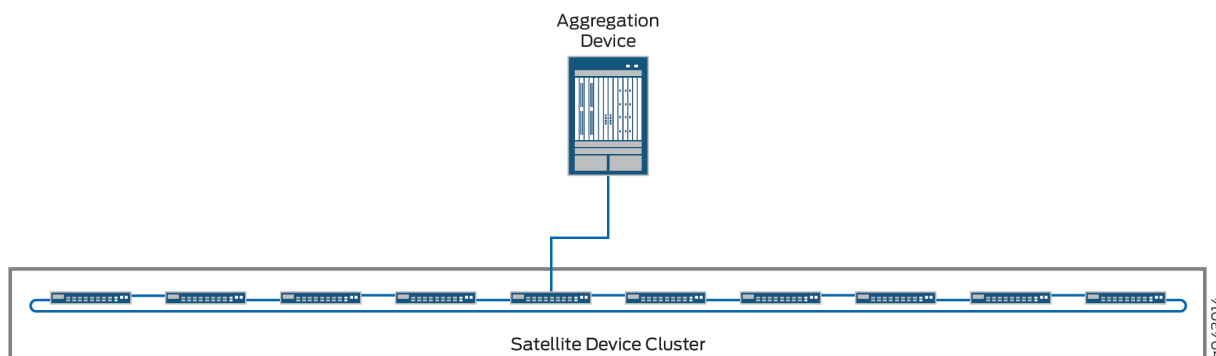
Satellite device clustering is particularly useful in scenarios where optical cabling options between buildings are limited and in scenarios where you want to preserve optical interfaces for other purposes. If you have, for instance, two buildings that have limited optical interfaces between each other 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 4 on page 11](#) shows a picture of a sample satellite device cluster connected to a single aggregation device.

Figure 4: 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 13](#) for 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

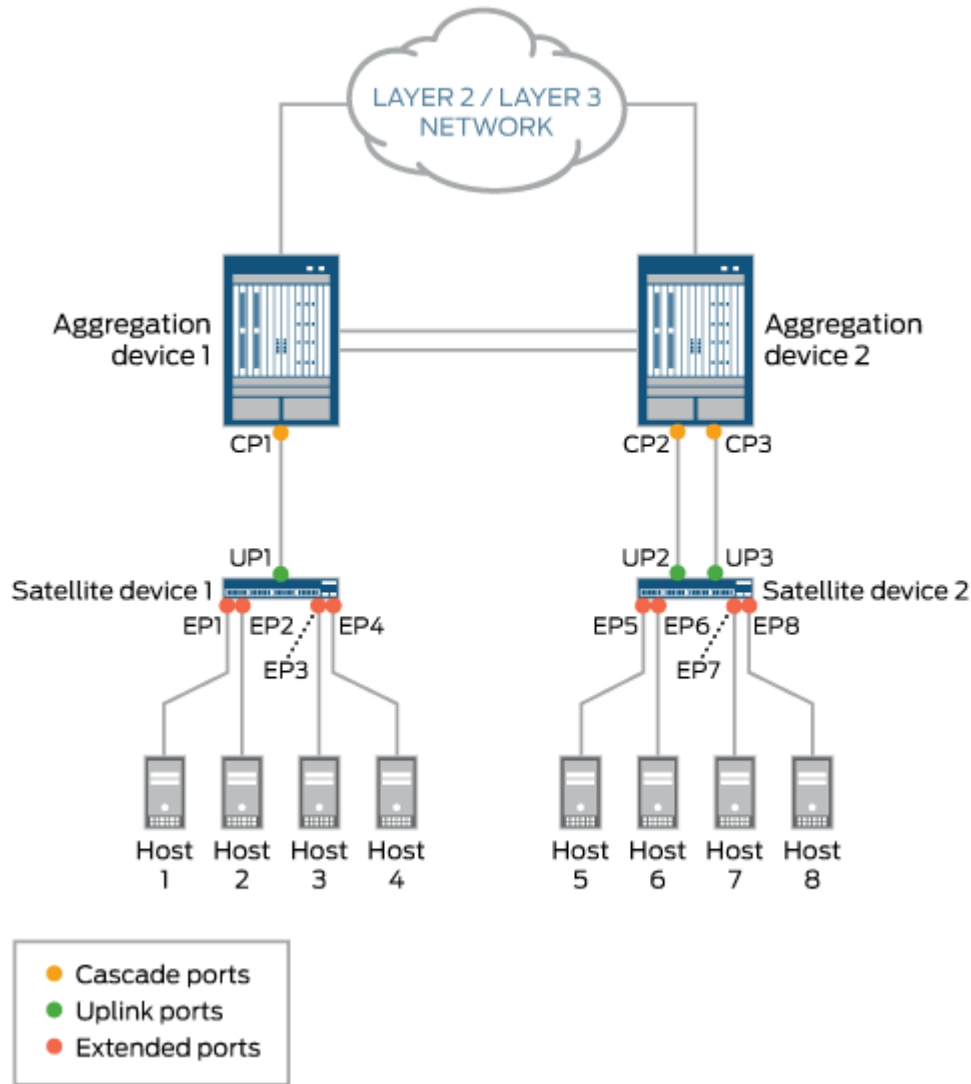
- [Understanding Cascade Ports | 16](#)
- [Understanding Uplink Ports | 17](#)
- [Understanding Extended Ports | 18](#)

In a Junos Fusion topology, cascade, uplink, and extended ports are components that play key roles. [Figure 5 on page 16](#) 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 5 on page 16](#), 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 5: 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 5 on page 16](#), 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 5 on page 16](#), 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 5 on page 16](#), 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 5 on page 16](#), 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. When configuring an extended port, the FPC slot number must be in the range of 65 through 254. This applies to all currently supported versions of Junos OS.

For example, for the four extended ports shown on Satellite device 1 in [Figure 5 on page 16](#), 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

[hash-key](#)

Understanding Port-Based Authentication in a Junos Fusion Provider Edge

Junos Fusion supports port-based authentication as defined by IEEE 802.1X standard to prevent unauthorized network access on the extended ports of the satellite devices. The satellite device blocks all packets to and from the supplicant (client) except for Extensible Authentication Protocol over LAN (EAPoL) packets at the interface. EAPoL allows the client to authenticate to an authentication server, such as a RADIUS server. Once the authentication server validates the supplicant's credentials, the switch opens the interface to the supplicant and allows access to the network. For more information on 802.1x authentication, see [Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode](#).

Junos fusion also supports central Web authentication. Central Web authentication redirects Web browser requests to a central Web authentication server that manages the authentication and authorization process. Upon successful authorization, the user is allowed access to the network. For more information on central Web authentication, see [Understanding Central Web Authentication](#).



NOTE: The authentication server in a Junos Fusion should be connected directly to the aggregation device and not to an extended port on a satellite device.

RELATED DOCUMENTATION

[IEEE 802.1x Port-Based Network Access Control Overview](#)

[Understanding Central Web Authentication](#)

[Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode](#)

Understanding Software in a Junos Fusion Provider Edge

IN THIS SECTION

● [Understanding Junos OS for the Aggregation Device in a Junos Fusion](#) | 20

- [Understanding Satellite Software for the Satellite Devices in a Junos Fusion | 20](#)
- [Understanding the Preboot eXecution Environment \(PXE\) Junos OS Software Package for QFX5100 Switches in a Junos Fusion | 21](#)
- [Understanding Minimum Software Requirements for a Junos Fusion | 21](#)
- [Understanding Satellite Software Upgrade Groups | 22](#)

This topic discusses the role of software in a Junos Fusion Provider Edge. 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, 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 the feature set 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 the satellite software. The satellite software, notably, applies features from the Junos OS software on the aggregation device onto the satellite device. The satellite software allows the satellite device to participate in the Junos Fusion, but does not provide any other software features for the satellite device.

You can run the same version of satellite software on satellite devices that are different hardware platforms. For instance, if your Junos Fusion included EX4300 and QFX5100 switches as satellite devices, the EX4300 and QFX5100 switches acting as satellite devices could install the satellite software from the same satellite software package.

Different satellite devices can run different versions of satellite software within the same Junos Fusion.

You can download satellite software from the software center for any satellite device. Additionally, you have the option to order some switches with the satellite software pre-installed 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 software on the aggregation device is upgraded. The satellite software packages on an individual satellite device can be updated manually using CLI commands on the aggregation device but are typically installed using 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 Junos OS onto the device before you can use it in your network as a standalone switch.

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

The satellite software requirements for a Junos Fusion Provider Edge are discussed in [Understanding Junos Fusion Provider Edge Software and Hardware Requirements](#).

Understanding the Preboot eXecution Environment (PXE) Junos OS Software Package for QFX5100 Switches in a Junos Fusion

The Preboot eXecution Environment (PXE) software is a version of Junos OS that must be used to convert a QFX5100 switch that is running satellite software as a satellite device into a standalone switch that is running Junos OS software.

The first version of PXE software that can be used to convert a QFX5100 switch from a satellite device to a standalone switch is introduced at Junos OS Release 14.1X53-D16. The PXE version of Junos OS software supports the same feature set as the other Junos OS software packages for a release, but is specifically engineered to install Junos OS onto a device running satellite software.

The PXE version of Junos OS software is required for QFX5100 switches only. Standard Junos OS software can be used to convert the other devices acting as satellite devices into standalone devices.

The PXE version of Junos OS software can be downloaded from the Software Center with the other QFX5100 switch software packages. For more information on PXE software images, see the *Junos OS Release Notes* for your software release. For information on using the PXE version of Junos OS software to convert a QFX5100 device into a standalone device, see *Converting a Satellite Device in a Junos Fusion to a Standalone Device*.

Understanding Minimum Software Requirements for a Junos Fusion

An aggregation device:

- Must be running Junos OS Release 14.2R3, or a later version of Junos OS Release 14.2.



NOTE: Junos Fusion is not supported in any Junos OS Release 15.1 release.

A satellite device:

- Must be running Junos OS Release 14.1X53-D16 or later prior to being converted into a satellite device.
- Must run a version of satellite software.

For more detailed information about satellite software support, see the Junos OS release notes for the version of Junos OS running on your aggregation device.

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 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 device is connected to a satellite device that is using an FPC ID that is part of a satellite software upgrade group, the device—unless it is already running the same version of satellite software—upgrades its satellite software using the satellite software associated with the satellite software upgrade group.

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 only a few satellite devices are updated at a time to minimize the effects of a traffic disruption due to too many satellite devices upgrading software simultaneously.

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 that a satellite software upgrade group is configured.

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

RELATED DOCUMENTATION

| [Configuring or Expanding a Junos Fusion Enterprise](#)

Understanding Junos Fusion Provider Edge Software and Hardware Requirements

IN THIS SECTION

- [Aggregation Devices | 23](#)
- [Satellite Devices | 27](#)

This topic describes the software and hardware requirements for a Junos Fusion Provider Edge.

It covers:

Aggregation Devices

This section details the hardware and software requirements for an aggregation device in a Junos Fusion Provider Edge.

It includes the following sections.

Aggregation Device Hardware Models

[Table 2 on page 24](#) lists the hardware platforms that are supported as aggregation devices, and the Junos OS release that introduced aggregation device support to Junos Fusion Provider Edge for the hardware.



BEST PRACTICE: We recommend installing a 64-bit version of Junos OS on the aggregation devices in a Junos Fusion, particularly in topologies that support a large number of satellite devices.



NOTE:

Table 2: Supported Aggregation Device Hardware and Initial Junos OS Release

| Hardware | Initial Junos OS Release |
|------------------------------------|--------------------------|
| MX5 Universal Routing Platform | 14.2R6 |
| MX10 Universal Routing Platform | 14.2R6 |
| MX40 Universal Routing Platform | 14.2R6 |
| MX80 Universal Routing Platform | 14.2R6 |
| MX104 Universal Routing Platform | 14.2R6 |
| MX204 Universal Routing Platform | 17.4R1 |
| MX240 Universal Routing Platform | 14.2R3 |
| MX480 Universal Routing Platform | 14.2R3 |
| MX960 Universal Routing Platform | 14.2R3 |
| MX2010 Universal Routing Platform | 14.2R3 |
| MX2020 Universal Routing Platform | 14.2R3 |
| MX10003 Universal Routing Platform | 17.3R1 |
| MX10008 Universal Routing Platform | 20.1R1 |
| MX10016 Universal Routing Platform | 20.1R1 |

Support for Junos Node Slicing

Starting in Junos OS Release 18.1R1, you can configure an aggregation device on a guest network function (GNF) on an MX480, MX960, MX2010, and MX2020 series router. Using Junos Node Slicing, you can create multiple partitions on a single MX router. These partitions are referred to as a guest network functions (GNFs). Each MX series router supports a maximum of 10 GNFs with each GNF supporting a separate aggregation device. The aggregation device on each GNF supports a maximum of 10 satellite devices.

For more information on Junos Node Slicing, see [Junos Node Slicing Overview](#).



NOTE: In a Junos Fusion Provider Edge topology that has a GNF configured as the aggregation device, only EX4300 and QFX 5110 switches are supported as satellite devices.



NOTE: In the GNF, you should use the following line cards to support the cascade port on the aggregation device:

- MPC7
- MPC8
- MPC9

Maximum Number of Aggregation Devices

A Junos Fusion supports one aggregation device.

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 26](#) provides a list of line cards on an MX Series 5G Universal Routing Platform that have interfaces that can be converted into cascade ports, and the initial Junos OS release when cascade port support was introduced for interfaces on the line card.



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

Table 3: MX Series 5G Universal Routing Platform Line Card Cascade Port Support

| Hardware | Initial Junos OS Release |
|-------------|--------------------------|
| 16x10GE MPC | 14.2R3 |
| MPC1 Q | 14.2R3 |
| MPC1E Q | 14.2R3 |
| MPC2 Q | 14.2R3 |
| MPC2E Q | 14.2R3 |
| MPC2 EQ | 14.2R3 |
| MPC2E EQ | 14.2R3 |
| MPC2E NG | 14.2R6 |
| MPC2E NG Q | 14.2R6 |
| MPC3E | 14.2R3 |
| MPC3E NG | 14.2R6 |
| MPC3E NG Q | 14.2R6 |
| MPC4E | 14.2R3 |
| MPC5E | 14.2R3 |
| MPC5EQ | 14.2R3 |

Table 3: MX Series 5G Universal Routing Platform Line Card Cascade Port Support (Continued)

| Hardware | Initial Junos OS Release |
|---|--------------------------|
| MPC6E | 14.2R3 |
| NOTE: MPC6E is supported with the 10-Gigabit Ethernet MIC with SFP+ (24 Ports) only | |
| MPC7E-10G | 16.1R1 |
| MPC7E-MRATE | 16.1R1 |
| NOTE: You can configure the 10-Gigabit Ethernet, 40-Gigabit Ethernet, or the 100-Gigabit Ethernet ports on the MPC7E-MRATE as cascade ports. | |
| MPC8E | 16.1R1 |
| MPC9E | 16.1R1 |

Satellite Devices

This section details the hardware and software requirements for a satellite device in a Junos Fusion Provider Edge.

It includes the following sections:

Satellite Device Hardware Models

[Table 4 on page 28](#) lists the hardware platforms that are supported as satellite devices, as well as the minimum Junos OS release that must be running on the satellite device before it can be converted from a standalone switch to a satellite device. A minimum version of Junos OS software is only required before a switch is converted into a satellite device. A satellite device in Junos Fusion Provider Edge runs satellite software after it is converted into a satellite device.

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.

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

| Hardware | Initial Junos OS Release —Satellite Device | Initial Junos OS Release—Aggregation Device | Minimum Satellite Software Version |
|---------------|--|---|------------------------------------|
| QFX5100-24Q | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| QFX5100-48S | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| QFX5100-48T | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| QFX5100-96S | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| QFX5110-48S | 18.1R1 | 18.1R1 | 3.4R1 |
| QFX5200-32C | 18.1R1 | 18.1R1 | 3.4R1 |
| EX4300-24P | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| EX4300-24T | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| EX4300-32F | 14.1X53-D30 | 14.2R5 | 1.0R2.2 |
| EX4300-32F-DC | 14.1X53-D30 | 14.2R5 | 1.0R2.2 |
| EX4300-48P | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| EX4300-48T | 14.1X53-D16 | 14.2R3 | 1.0R1 |
| EX4300-48T-DC | 14.1X53-D26 | 14.2R3 | 1.0R1 |



NOTE: The QFX5110-48S does not support channelized ports in a Junos Fusion environment.

Power over Ethernet Requirements for a Satellite Device

A satellite device that supports Power over Ethernet (PoE) must be running the minimum PoE controller software version. The EX4300 series switches must be running PoE controller software version 2.6.3.9.2.1 or higher.

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](#).

Maximum Number of Satellite Devices

Junos Fusion Provider Edge supports up to eighteen satellite devices on the MX5, MX10, MX40, MX80, and MX104 Universal Routing Platform. For all other MX Series routers, Junos Fusion Provider Edge supports up to sixty-four satellite devices.

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 |
|---------|--|
| 18.1R1 | Starting in Junos OS Release 18.1R1, you can configure an aggregation device on a guest network function (GNF) on an MX480, MX960, MX2010, and MX2020 series router. |

RELATED DOCUMENTATION

| | |
|--|-----------|
| Configuring Junos Fusion Provider Edge | 51 |
| Managing Satellite Software Upgrade Groups in a Junos Fusion | 71 |
| Converting a Satellite Device in a Junos Fusion to a Standalone Device | 93 |

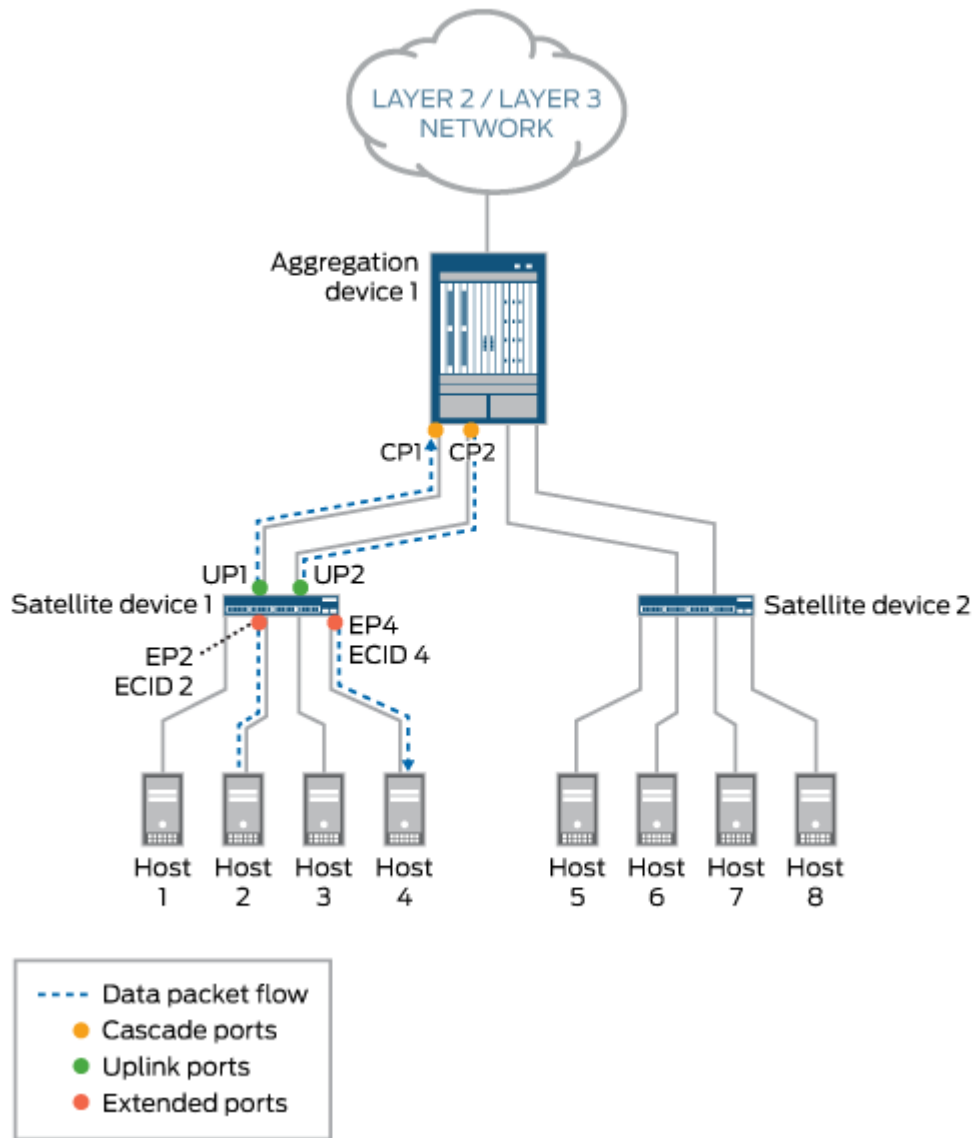
Understanding the Flow of Data Packets in a Junos Fusion Topology

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:

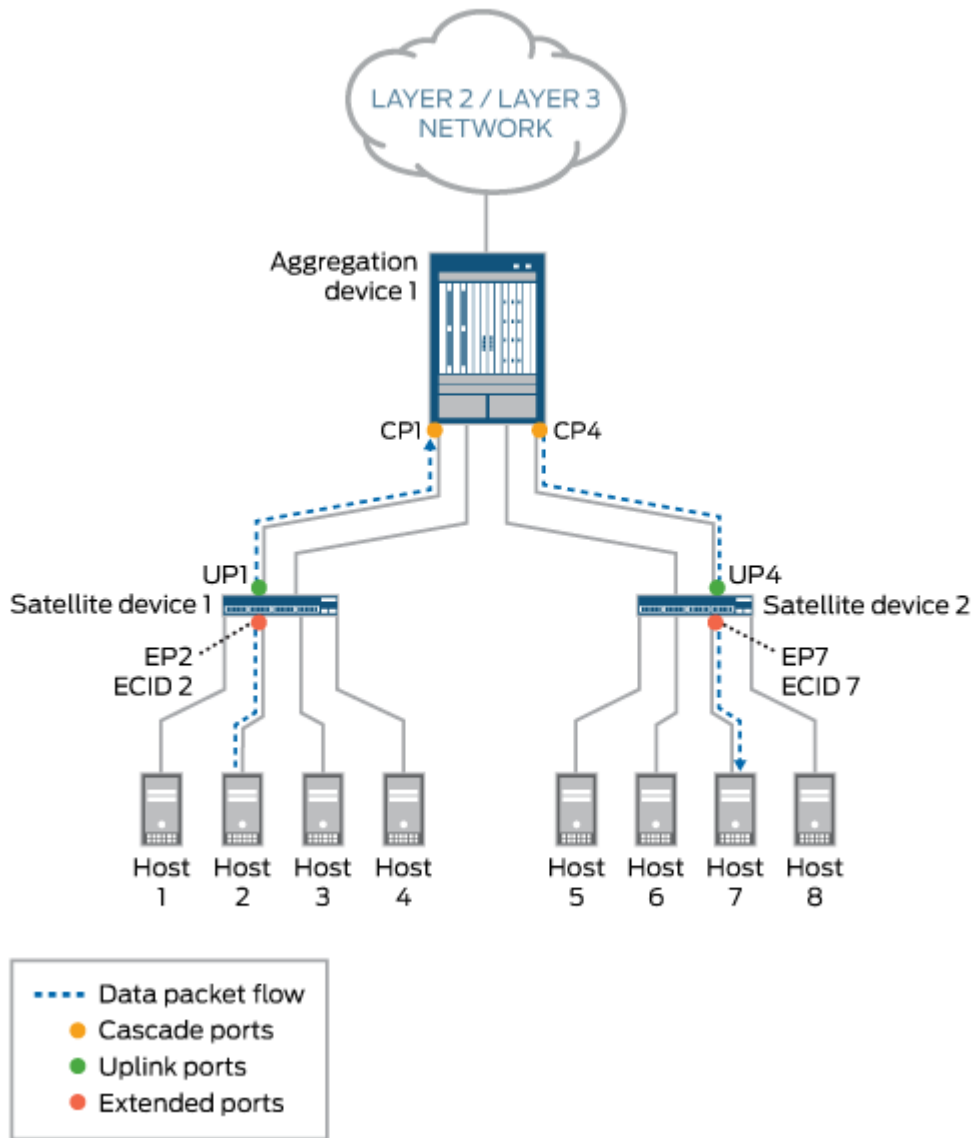
- Scenario 1—A host on one satellite device sends a packet to another host on the same satellite device. For example, Host 2 sends a unicast packet to Host 4. Both hosts are connected to Satellite device 1. (See [Figure 6 on page 31.](#))
- Scenario 2—A host on one satellite device sends a packet to 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 7 on page 32.](#))

Figure 6: Layer 2 Unicast Data Packet Flow Through a Junos Fusion Topology—Scenario 1



g043179

Figure 7: 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 | 4](#)

[Understanding Junos Fusion Enterprise Components](#)

Understanding Satellite Policies in a Junos Fusion

IN THIS SECTION

- [Satellite Policies Overview | 34](#)
- [Understanding Environment Monitoring Satellite Policies | 34](#)

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 | 51](#)

[Configuring or Expanding a Junos Fusion Enterprise](#)

Junos Fusion Provider Edge Supported Protocols

IN THIS SECTION

- [Layer 3 Protocols Supported on Junos Fusion Provider Edge | 36](#)
- [Multicast Protocols Supported on Junos Fusion Provider Edge | 38](#)
- [VPN Protocols Supported on Junos Fusion Provider Edge | 39](#)

Junos Fusion Provider Edge expands the number of available network interfaces on an aggregation device by connecting satellite devices that act as extensions of the aggregation device. The entire system—the interconnected aggregation device and satellite devices—is called a Junos Fusion. Junos Fusion Provider Edge simplifies network aggregation device administration because the aggregation device acts as a single, port-dense device, managed using one IP address.

Layer 3 Protocols Supported on Junos Fusion Provider Edge

Starting with Junos OS Release 14.2R4, many of the routing protocols supported on MX Series routers have been extended to the satellite devices in a Junos Fusion Provider Edge topology. You can configure the following Layer 3 routing protocols on satellite device extended ports:

- BFD (Centralized only)
- BGP
- BGP for IPv6
- IS-IS
- OSPF
- OSPF version 3
- LACP
- Segment Routing

You can configure the following Layer 3 routing protocols on satellite device extended ports that are included in link aggregation groups (LAGs):

- BGP
- IS-IS
- OSPF
- LACP

BFD Support on Junos Fusion Provider Edge

Bidirectional Forwarding Detection (BFD) is a protocol used to detect failure in the data path. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. BFD works with a wide variety of network environments and topologies.



NOTE: Junos Fusion Provider Edge only supports centralized BFD with the `no-delegate-processing` statement included in the `[edit routing-options ppm]` hierarchy. LACP does not work when `no-delegate-processing` is enabled.

For more information, see the following:

- [Understanding BFD for BGP](#)

- [Understanding BFD for IS-IS](#)
- *Understanding BFD for OSPF*

BGP Support on Junos Fusion Provider Edge

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol that exchanges routing and reachability information between autonomous systems on the Internet. The protocol can be a path vector protocol or a distance-vector routing protocol. BGP makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator for core routing decisions. For more information, see the [BGP User Guide](#) and the CLI statement `bgp`.

IS-IS Support on Junos Fusion Provider Edge

Intermediate System to Intermediate System (IS-IS) moves information within either a computer network, a group of physically connected computers, or between similar devices. It accomplishes this by determining the best route for traffic through a packet-switched network. For more information, see the [IS-IS User Guide](#).

OSPF Support on Junos Fusion Provider Edge

Open Shortest Path First (OSPF) is a routing protocol for IP networks using a link state routing algorithm. This interior routing protocol operates within a single autonomous system. For more information, see the [OSPF User Guide](#) and the CLI statements `ospf` and `ospf3`.

LACP Support on Junos Fusion Provider Edge

Link Aggregation Control Protocol (LACP) is one method of bundling several physical interfaces to form one logical aggregated Ethernet interface. For more information, see "[Understanding Link Aggregation and Link Aggregation Control Protocol in a Junos Fusion](#)" on page 122 and [Configuring Aggregated Ethernet Interfaces](#).

Segment Routing

Segment routing (SR) is a source-based routing technique that simplifies traffic engineering and management across network domains. It removes network state information from the transit routers and nodes in the network and places the path state information into packet headers at an ingress node. Segment routing traffic engineering (SR-TE) uses policies to steer traffic through the network. When you configure segment routing, keep in mind that the extended ports on satellite devices can only be configured as customer edge (CE) router interfaces. [Table 5 on page 38](#) lists the supported segment routing features on Junos fusion for provider edge:

Table 5: Supported Segment Routing Features

| Features | Additional Information |
|---|--|
| SR and SR-TE for Intermediate System-to-Intermediate System | <i>Understanding Source Packet Routing in Networking (SPRING)</i> |
| Layer 2 Circuits, Layer 2 VPNs, VPLS over SR-ISIS and uncolored SR-TE | <i>Static Segment Routing Label Switched Path</i> |
| Layer 3 VPNs over SR-ISIS and color and Uncolored SR-TE | <i>Static Segment Routing Label Switched Path</i> |
| Hierarchical Class of Service of VPNs over Segment Routing | "Understanding CoS on an MX Series Aggregation Device in Junos Fusion Provider Edge" on page 152 |
| EVPN MPLS with single-active and all -active multihoming redundancy. | <i>Segment Routing Traffic Engineering at BGP Ingress Peer Overview</i> |

Multicast Protocols Supported on Junos Fusion Provider Edge

You can configure the following multicast protocols on satellite device extended ports:

PIM on Junos Fusion Provider Edge

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols, in this case Internet Group Management Protocol (IGMP) on extended ports. All four PIM modes work on extended ports—PIM sparse Mode (default), PIM dense Mode, bidirectional PIM, and PIM source-specific multicast. For more information, see the [PIM Overview](#) and the CLI statement [pim](#).

IGMP on Junos Fusion Provider Edge

Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group membership. IGMP is an integral part of IP multicast, and is used for one-to-many networking applications such as online streaming video and gaming because it allows more efficient use of resources when supporting these types of applications. For more information, see [Understanding IGMP](#) and the CLI statement [igmp](#).

MLD on Junos Fusion Provider Edge

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. MLD uses ICMPv6 messaging in contrast to IGMP's bare IP encapsulation. For more information, see the [mld](#) CLI statement.

Junos Fusion supports multicast and broadcast packet replication on the aggregation device and the satellite devices. For more information on multicast replication, see ["Understanding Multicast Replication in a Junos Fusion" on page 140](#).

BGP MVPN on Junos Fusion Provider Edge

BGP multicast VPN (MVPN) is a method for implementing multiprotocol multicast services on a BGP MPLS Layer 3 VPN. BGP MVPNs use existing BGP and MPLS VPN infrastructure to support multicast traffic between sets of senders and sets of receivers. Junos Fusion supports the connection of BGP-based multicast VPN CE devices on the extended ports of the satellite device. For more information, see *Configuring BGP MVPNs*.

VPN Protocols Supported on Junos Fusion Provider Edge

You can configure the following VPN protocols on satellite device extended ports:



NOTE: Extended ports on satellite devices can only be configured as customer edge (CE) router interfaces in a VPN. Provider edge (PE) router interfaces must be configured directly on the native port of the aggregation device.

Layer 2 Circuits on Junos Fusion Provider Edge

You can configure a local switching interface to ignore the MTU configuration set for an associated physical interface. This enables you to bring up a circuit between two logical interfaces that are defined on physical interfaces with different MTU values. For more information, see the [Configuring Interfaces for Layer 2 Circuits Overview](#).

Layer 2 VPNs on Junos Fusion Provider Edge

Layer 2 VPNs provide communication between a provider network and a customer network. Provider edge routers or PEs at the edge of a provider network communicate with each customer edge or CE router. Customers configure their routers to carry all Layer 3 traffic, while the service provider needs to know only how much traffic the Layer 2 VPN needs to carry. For more information, see the [Layer 2 VPNs and VPLS User Guide for Routing Devices](#).

Layer 3 VPNs on Junos Fusion Provider Edge

Layer 3 VPNs also provide communication between a provider network and a customer network. However, in a Layer 3 VPN, routing occurs on the service provider's router. Therefore, Layer 3 VPNs require more configuration on the part of the service provider, because the service provider's PE routers must store and process the customer's routes. For more information, see the [Layer 3 VPNs User Guide for Routing Devices](#).

DHCP Relay Support on Layer 3 VPNs

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that is used to dynamically assign IP addresses and other related configuration information to network devices. The DHCP server automatically assigns IP addresses and other network parameters to client devices on the network. DHCP Relay Agent forwards the DHCP messages between the DHCP clients and the DHCP servers when the servers and clients are on different networks. Junos fusion for provider edge supports DHCP relay on EVPN-MPLS networks. It is not supported on an EVPN-MPLS network over segment routing. For more information, see [DHCP Relay Agent](#).

VPLS on Junos Fusion Provider Edge

Virtual Private LAN Service (VPLS) provides Ethernet-based multipoint to multipoint communication over IP or MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites with pseudowires. The technologies that can be used as pseudowire can be Ethernet over MPLS, L2TPv3 or even GRE. For more information, see the [Layer 2 VPNs and VPLS User Guide for Routing Devices](#).

EVPN with VXLAN

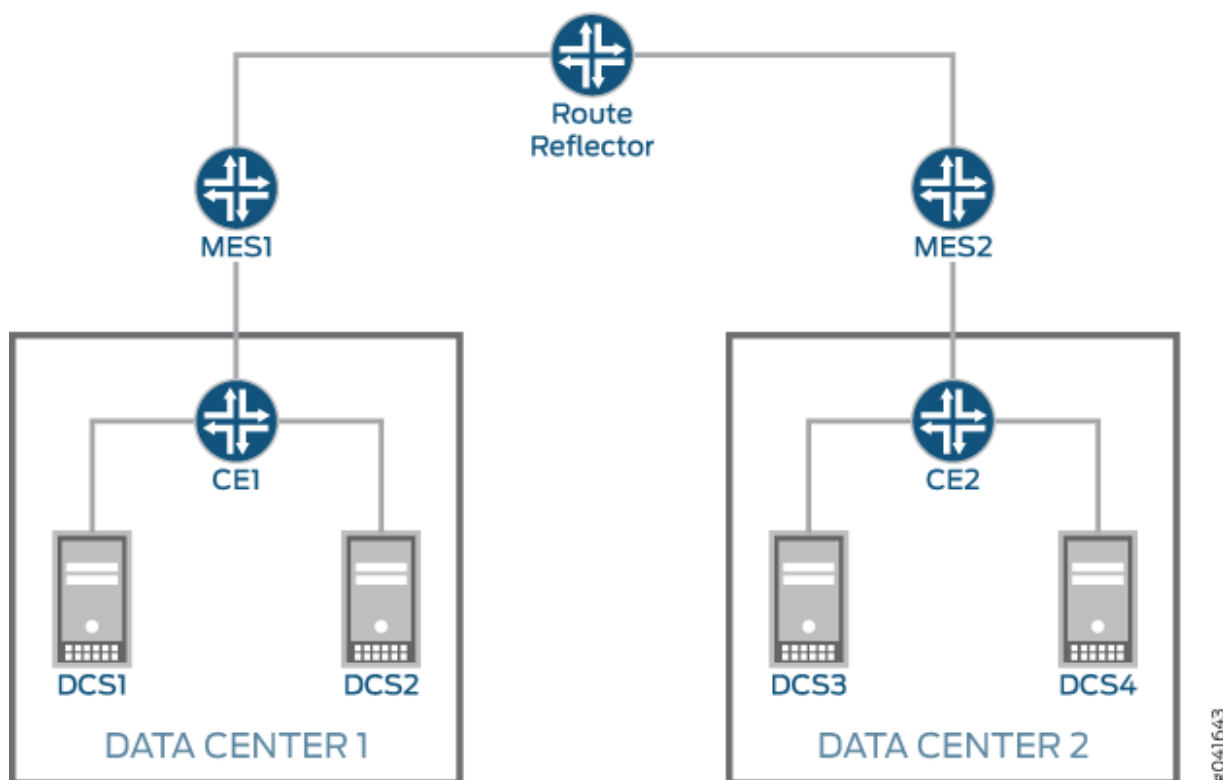
You can configure ports on the satellite devices managed by MX Series routers to support Ethernet VPNs (EVPNs) with Virtual Extensible LAN (VXLAN) encapsulation. EVPN provides layer 2 VPN services with advance multi-homing capabilities by using the BGP control plane to distribute routes over IP or IP/MPLS backbone. VXLAN is a tunneling scheme that overlays layer 2 ethernet frames on top of layer 3 UDP packets. EVPN with VXLAN encapsulation allows you to create a logical network for hosts that span across a physical network and supports up to 16 million VXLAN segments. For more information on EVPN and VXLAN, see *Understanding EVPN with VXLAN Data Plane Encapsulation*.

EVPN-MPLS

An Ethernet VPN (EVPN) enables you to connect dispersed customer sites using a Layer 2 virtual bridge. EVPN-MPLS extends layer 2 VPN services over an MPLS network. It consists of customer edge (CE) devices connecting to MPLS edge switches, often provider edge (PE) devices that provide MPLS label functionality, EVPN-MPLS Junos Fusion Provider Edge supports connecting a customer edge (CE) on the

extended ports of the satellite device. [Figure 8 on page 41](#) shows a typical EVPN deployment. For more information on EVPN-MPLS, see *EVPN Overview*.

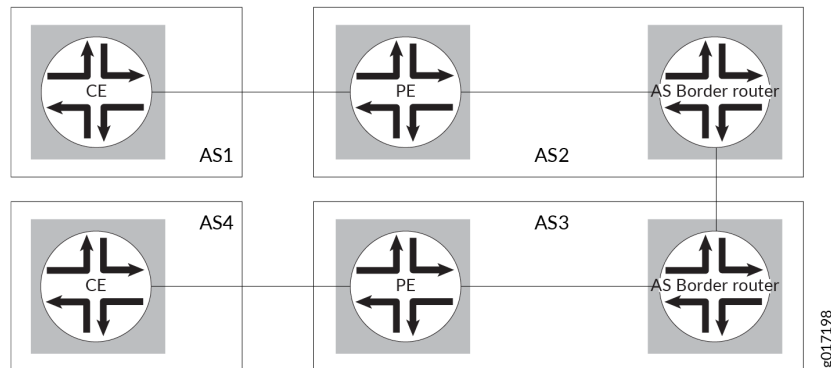
Figure 8: EVPN-MPLS Network



Interprovider and Carrier-of-Carrier VPNs

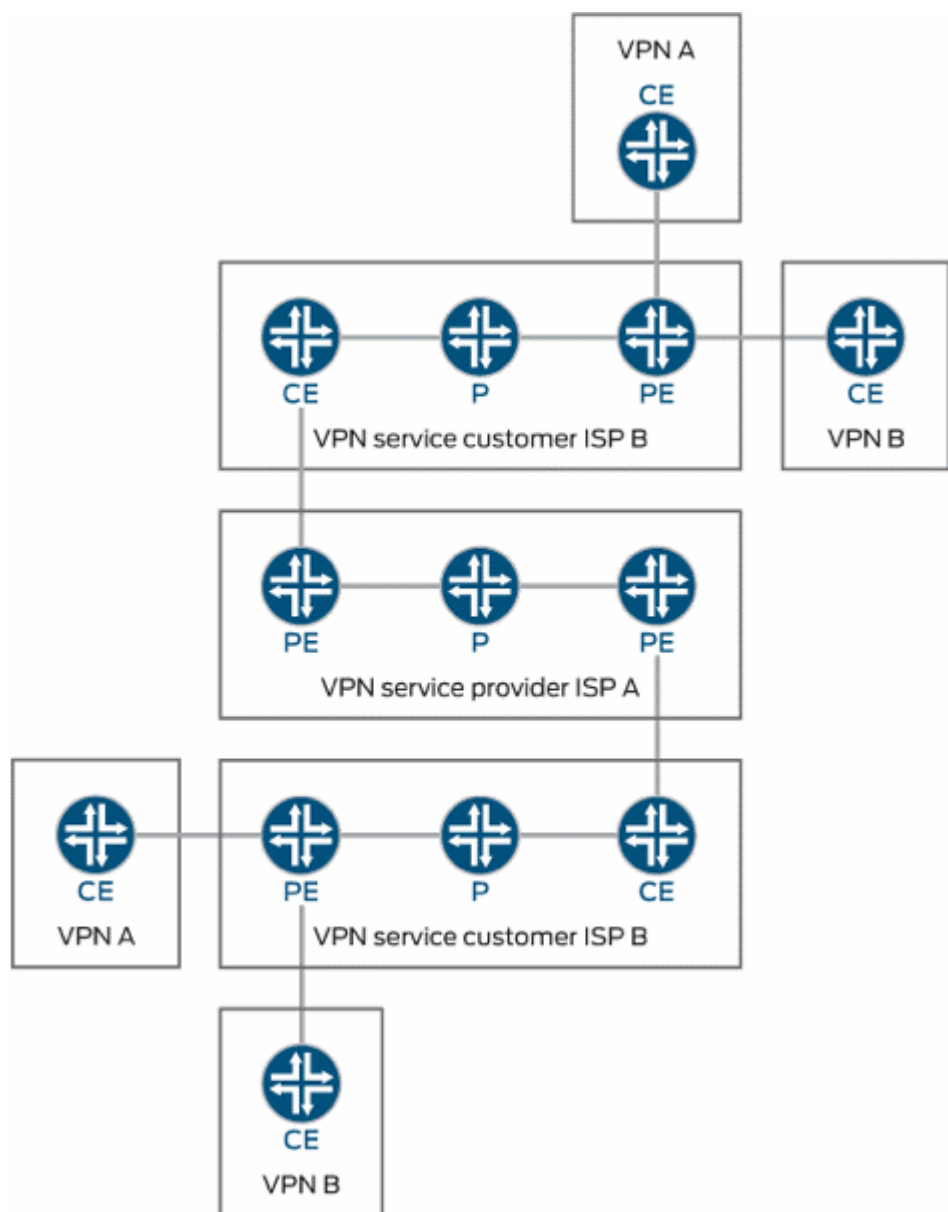
Interprovider VPNs provide connectivity between separate ASs. This functionality is used by a VPN customer who has connections to several different service providers, or different connections to the same service provider in different geographic regions, each of which has a different AS. For Interprovider VPNs, Junos Fusion only supports intra-AS connection on a Autonomous System Border Router (ASBR) to the extended port. For example, in [Figure 9 on page 42](#), extended ports can only be used on the ASBR towards the PE router within each AS.

Figure 9: Inteprovider VPN Network Topology



Carrier-of-Carrier VPN service describes a hierarchical VPN (also known as a recursive VPN) model where one carrier (VPN service customer) transports their VPN traffic inside another carrier's VPN (VPN service provider). [Figure 10 on page 43](#) shows the carrier-of-carrier model with a VPN service provider (ISP A) and a VPN service customer (ISP B). The VPN service provider is the backbone network carrier and provides VPN support for the VPN service customers. Junos Fusion PE currently supports PE routers for VPN service customers. In 21.1R1, Junos Fusion PE also supports PE routers for VPN service providers. VPN-IPv4 addresses for the VPN service customer are treated as external routes by the VPN service provider and are not imported into the VPN service provider's VRF table. The VPN service provider uses MPLS to route the VPN traffic, so it must be configured on the VPN service provider network. The VPN service customer only needs to configure MPLS in the CE device that is connected to the PE device of the VPN service provider. You can connect routers for Internet Service Provider as the customer and VPN Service Provider as the customer on the extended port.

Figure 10: Carrier-of-Carriers VPN Model



Junos Fusion Provider Edge supports 6vPE in both interprovider and carrier-of-carrier VPNs. For more information, see *Interprovider and Carrier-of-Carriers VPNs*.

RELATED DOCUMENTATION

[Understanding the Flow of Data Packets in a Junos Fusion Topology](#) | 29

[Junos Fusion Provider Edge Overview](#) | 2

Local Switching on Junos Fusion Provider Edge

IN THIS SECTION

- [Selective VLAN Local Switching | 44](#)
- [Policer | 45](#)
- [Example: Configuring Selective VLAN Local Switching | 45](#)

Junos Fusion supports packet forwarding both on the aggregation device and on satellite devices. The default behavior is to forward the packets received on the extended port to the aggregation device. The satellite device does not perform any processing on the incoming traffic. The aggregation device processes and directs the data traffic.

Local switching in Junos Fusion reduces the traffic that is exchanged between satellite devices and the aggregation device by handling some of the local switching. When you enable local switching, the satellite device handles the bridging traffic locally on the satellite device. The satellite device maintains a bridge forwarding table with the local MAC addresses for devices that are connected directly to the satellite device and forwards the data packets with local MAC addresses. Packets with unknown MAC addresses are sent to the aggregate device. Local switching applies to all the ports on the satellite device.

To configure local switching on a satellite device, include the `local-switching` statement in the forwarding options hierarchy:

```
[edit forwarding-options]
satellite {
  fpc slot {
    local-switching;
  }
}
```

Selective VLAN Local Switching

In some cases, you might want to enable local switching for only a select number of VLANs on the satellite device—for example, offloading data traffic based on the type of service. This will allow you to control traffic more precisely. To enable selective VLAN local switching on a satellite device, include

selected VLANs in a virtual switch routing instance. VLANs that are not included in the routing instance will default to forwarding data packets to the aggregate device.

To configure selective VLAN local switching on a satellite device, include the `selective-vlan-switching` statement in the forwarding options hierarchy with a virtual switch routing instance:

```
[edit forwarding-options]
satellite {
  fpc slot {
    selective-vlan-switching {
      routing-instance routing-instance-name;
    }
  }
}
```

When you have digital subscriber line access multiplexer (DSLAM) ports and broadband network gateway (BNG) ports on a satellite device, you should configure the satellite device to switch traffic locally from the DSLAM ports to the BNG port while restricting the traffic between two DSLAM ports. Configure the satellite device to switch traffic locally from a DSLAM port to a BNG port by including the `core-facing` keyword in all BNG port interfaces. Restrict switched traffic between DSLAM ports by including the `no-local switching` keyword in the bridge domain.

Policer

Traffic policing enables you to control the maximum rate of traffic that will be sent or received on an interface. A policer defines a set of traffic rate limits and sets the action for traffic that does not conform to the configured limits. Packets in a traffic flow that do not conform to traffic limits are either discarded or are marked with a different forwarding class or packet loss priority (PLP) level.

You can limit the flow of Layer 2 traffic that is sent to the aggregation device by applying an ingress policer at the satellite device. You configure the Layer 2 ingress policer by using the `input-policer` statement at the `[edit interfaces interface-name layer2-policer]` hierarchy level. Because the satellite device is only aware of locally switched logical interface, the ingress policer is applied to Layer 2 input traffic at the satellite device ports.

Example: Configuring Selective VLAN Local Switching

In this configuration example, the satellite device is configured with the following options:

- VLANs 101, 102, 103, and 104 are enabled for selective VLAN local switching.
- VLAN 101 and 102 have DSLAM traffic.

- Interface xe-100/0/0 is a BNG port.
- Interfaces xe-100/0/1 and xe-100/0/2

```

interfaces {
  xe-100/0/0 {
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list [100-110];
        core-facing;
      }
    }
  }
  xe-100/0/1 {
    layer2-policer {
      input-policer SD-policer-A;
    }
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list [100-110];
      }
    }
  }
  xe-100/0/2 {
    layer2-policer {
      input-policer SD-policer-A;
    }
    unit 0 {
      family bridge {
        interface-mode trunk;
        vlan-id-list [100-110];
      }
    }
  }
}

```

```

routing-instances {
  vs-1 {
    instance-type virtual-switch;
  }
}

```

```

interface xe-100/0/0.0;
interface xe-100/0/2.0;
interface xe-100/0/2.0;
bridge-domains {
    bd-1 {
        vlan-id 101;
        no-local-switching;
    }
    bd-2 {
        vlan-id 102;
        no-local-switching;
    }
    bd-3 {
        vlan-id 103;
    }
    bd-4 {
        vlan-id 104;
    }
}
}
forwarding-options {
    satellite {
        fpc 100 {
            sd-vlan-switching {
                routing-instance vs-1;
            }
        }
    }
}
}
}

```

RELATED DOCUMENTATION

[Two-Color Policer Configuration Overview](#)

Broadband Subscription Services on Junos Fusion

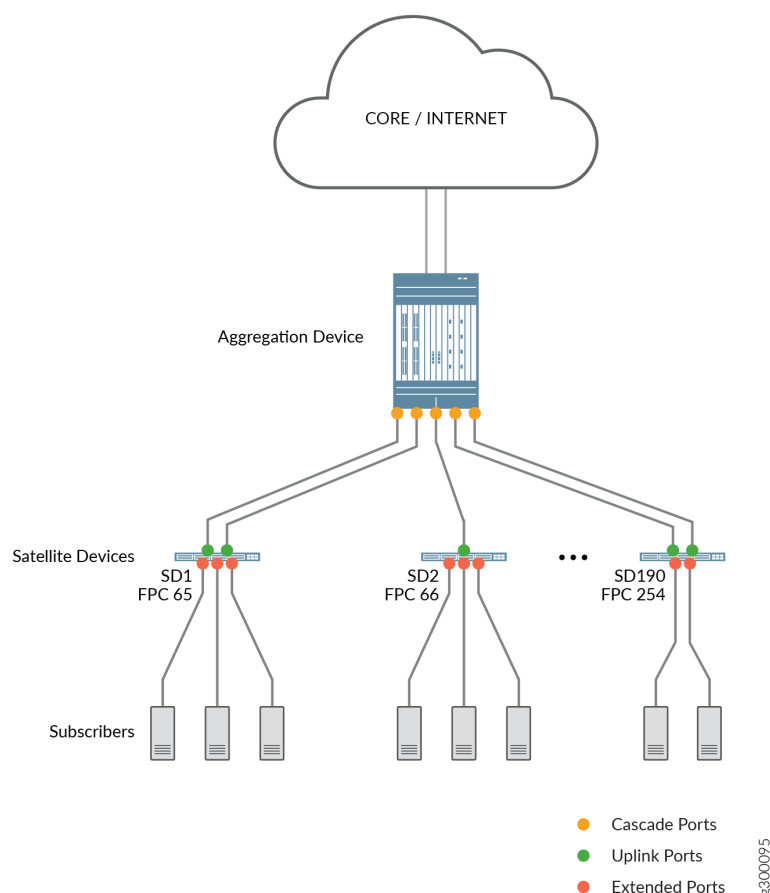
IN THIS SECTION

- [Benefits of Broadband Subscription on Junos Fusion](#) | 50

Starting in Junos OS Release 18.4R1, Junos Fusion Provider Edge supports Broadband Edge Subscriber Management. The aggregation device in Junos Fusion functions as Broadband Network Gateway (BNG) while the extended ports on the satellite devices function as ports on the BNG. From the standpoint of a broadband network, the extended ports appear to be local physical ports and follow the Junos Fusion naming convention for port interfaces. The Satellite device is identified with a Flexible PIC Concentrator (FPC) ID and the extended ports use the FPC ID as part of the interface name.

[Figure 11 on page 49](#) illustrates a basic subscriber network on a Junos Fusion Provider Edge. The first satellite device (satellite device 1) off the cascade port is identified with a FPC ID of 65 with the first extended port on satellite device 1 named as xe-65/0/0.

Figure 11: Broadband Network Gateway on Junos Fusion



NOTE: BNG on Junos Fusion Provider Edge is supported only with a MX204, MX240, MX480, MX960, MX2010, MX2020, or MX10003 Universal Routing Platform as an aggregation device with EX4300, QFX5100, QFX5110, or QFX5200 switches as satellite devices.

BNG on Junos Fusion Provider Edge supports the following:

- DHCP and PPPoE Subscribers.
- Static and Dynamic VLANs.
- Full support for broadband subscriber firewall services.
- Non-Fusion broadband subscribers are also supported on the aggregation device. This means that the customer premise equipment can connect directly to the MX router.
- Deep packet inspections of layer 4 through layer 7 payloads.

- Lawful-intercept.

BNG on Junos Fusion Provider Edge has the following limitations:

- Support for satellite Devices with only a single connection to a cascade port on aggregation device.
- Port mirroring is not supported.
- The line rate of the cascade port limits the number of extended ports that can be provisioned. To prevent oversubscription on a Junos Fusion, we recommend that you do not provision the sum of the bandwidth for the ports on the satellite device to exceed the bandwidth of the cascade port.

For more information on configuring, provisioning, and managing broadband subscribers, see [Junos OS Broadband Subscriber Management and Services Library](#)

Benefits of Broadband Subscription on Junos Fusion

Broadband subscription support on Junos Fusion allows you to use a single point of management on an aggregation device to configure and manage a large number of network-facing subscriber interfaces to operate as a group on satellite devices. As your network grows, you can easily expand the size of your subscriber access network by adding satellite devices as they are needed. Junos Fusion supports both Broadband Subscribers and Non-Fusion broadband subscribers on the aggregation device. Existing Junos Fusion deployments can migrate to Broadband Subscriber management gradually by adding new subscribers to current Junos Fusion Provider Edge deployment while adding new satellite devices.

RELATED DOCUMENTATION

| [Understanding CoS on an MX Series Aggregation Device in Junos Fusion Provider Edge](#) | 152

Junos Fusion Provider Edge Configuration

IN THIS CHAPTER

- [Configuring Junos Fusion Provider Edge | 51](#)
- [Configuring Satellite Device Alarm Handling Using an Environment Monitoring Satellite Policy in a Junos Fusion | 67](#)

Configuring Junos Fusion Provider Edge

IN THIS SECTION

- [Preparing the Aggregation Device | 51](#)
- [Configuring the Cascade Ports on the Aggregation Device | 53](#)
- [Configuring the FPC Slot Identifiers | 54](#)
- [Configuring Software Upgrade Groups on the Aggregation Device | 55](#)
- [Preparing the Satellite Device | 57](#)
- [Adding Satellite Devices to the Junos Fusion Provider Edge | 59](#)

This topic provides the instructions needed to configure a Junos Fusion Provider Edge. The instructions in this topic can also be used to add a new satellite device to a Junos Fusion Provider Edge after initial installation. It covers:

Preparing the Aggregation Device

This section provides instructions on the required steps to prepare a switch to become the aggregation device in a Junos Fusion Provider Edge.

This section does not discuss the cascade port, FPC slot identification, or the software upgrade group configuration, which are important elements of preparing your aggregation device for a Junos Fusion

Provider Edge installation and are discussed in ["Configuring the Cascade Ports on the Aggregation Device" on page 53](#), ["Configuring the FPC Slot Identifiers" on page 54](#), and ["Configuring Software Upgrade Groups on the Aggregation Device" on page 55](#). The instructions for adding satellite devices to the Junos Fusion Provider Edge are also provided later in this topic.

To prepare your aggregation device for a Junos Fusion Provider Edge:

1. Enable Enhanced IP:

```
[edit]
user@aggregation-device# set chassis network-services enhanced-ip
```

2. Configure the Junos Fusion into single home mode:

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



NOTE: Configuring the Junos Fusion into single home mode using this step is optional when the aggregation device is running Junos OS Release 14.2R5 or later. Configuring the Junos Fusion into single home mode is required when the aggregation device is running Junos OS Release 14.2R3 or 14.2R4.

3. Commit the configuration to both Routing Engines:

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

If you are using an aggregation device with a single Routing Engine:

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

4. Ensure your aggregation device is running a version of Junos OS software that is compatible with Junos Fusion Provider Edge, such as Junos OS Release 14.2R3 or later. If the aggregation device does not have the correct version installed, upgrade your aggregation device.

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

5. Reboot both Routing Engines:

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

A reboot is required to enable enhanced IP.

If you only want to reboot a single Routing Engine:

```
user@aggregation-device> request system reboot
```

Reboot the other Routing Engine at a later time to ensure it is ready to manage the Junos Fusion in the event of a Routing Engine switchover.

Configuring the Cascade Ports on the Aggregation Device

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

A cascade port must be configured before a satellite device is recognized by the Junos Fusion Provider Edge. Cascade port configuration, therefore, is always a required step for configuring a Junos Fusion Provider Edge.

To configure a cascade port or ports:

1. Log in to the aggregation device.
2. Configure the interface on the aggregation device side of the link into 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
```

3. Commit the configuration:

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

If you want to commit the configuration to both Routing Engines:

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

Configuring the FPC Slot Identifiers

In a Junos Fusion, each satellite device must be mapped to an FPC identifier (FPC ID). The FPC ID 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—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. The range for the FPC ID is 100 -255 in Junos OS Release 14.2 and 65 to 254 in Junos OS Release 16.1 and later.

A Junos Fusion Provider Edge provides two methods of assigning an FPC identifier: Unique-ID based FPC identification and connectivity-based FPC identification. Unique-ID based FPC identification maps an FPC slot ID to a satellite device's MAC address or serial number, while Unique-ID based FPC identification maps an FPC slot ID to a cascade port. Both options are discussed in ["Understanding Junos Fusion Provider Edge Components" on page 4](#).

- To configure the FPC slot ID using connectivity-based FPC identification, 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
```

- To configure the FPC slot ID using unique-ID based FPC identification, use one of the following options:

- To map the FPC slot ID to a 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 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
```

- To map the FPC slot ID to a 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 functions as the FPC slot identifier.

For example, to map FPC slot ID to 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
```

If a prospective satellite device is connected to a Junos Fusion Provider Edge without having a configured FPC slot ID, the prospective satellite device does not participate in the Junos Fusion Provider Edge 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 Provider Edge due to an FPC ID association issue.

Configuring Software Upgrade Groups on the Aggregation Device

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 device is connected to a satellite device that is using an FPC ID that is part of a satellite software upgrade group, the device—unless it is already running the same version of satellite software—upgrades its satellite software using the satellite software associated with the satellite software upgrade group.

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 only a few satellite devices are updated at a time to minimize the effects of a traffic disruption due to too many satellite devices upgrading software simultaneously.

The two most common methods of installing satellite software onto an aggregation 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 configured and managed from the aggregation device.

To configure a software upgrade group:

1. Log in to the aggregation device.
2. Create the software upgrade group, and add the satellite devices to the 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 FPC slot ID number or range of numbers, of the satellite devices that are being added to the upgrade group. If you enter an existing upgrade group name as the *upgrade-group-name*, you add new satellite devices 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
```

3. 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 4.

4. Associate a satellite software package with the 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-1.0R1.1-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-1.0R1.1-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.

Preparing the Satellite Device

This section discusses the steps that must be performed on a standalone switch before converting it into a satellite device in a Junos Fusion Provider Edge.

To perform this procedure:

These instructions assume your device is already running Junos OS Release 14.1X53-D16 or later.

1. Log in to the device using the console port.
2. Zeroize the device:

```
user@satellite-device> request system zeroize
```



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

If you are not logged in to 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, login using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces 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 QSFP+ interfaces 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
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos Fusion.

This step is needed because the built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is zeroized.

The number of built-in 40-Gbps QSFP+ interfaces varies by EX4300 switch model. See *EX4300 Switches Hardware Overview*.

Adding Satellite Devices to the Junos Fusion Provider Edge

IN THIS SECTION

- [Autoconverting a Switch into a Satellite Device | 59](#)
- [Manually Converting a Switch into a Satellite Device | 62](#)
- [Configuring a Switch into a Satellite Device Before Interconnecting It into a Junos Fusion Provider Edge | 65](#)

This section discusses the processes for adding satellite devices to a Junos Fusion Provider Edge.

A switch must be running the satellite software to operate as a satellite device. The instructions in this procedure include the required steps to install the satellite software onto your satellite device.

You can add satellite devices to your Junos Fusion Provider Edge using one of the following procedures:

Autoconverting a Switch into a Satellite Device

Use this procedure to automatically configure a switch into a satellite device when it is cabled into the aggregation device.

You can use the autoconversion procedure to add one or more satellite devices to your Junos Fusion topology. The autoconversion procedure is especially useful when you are adding multiple satellite devices to your Junos Fusion, because it allows you to easily configure the entire topology before or after cabling the satellite devices to the aggregation devices.

Before you begin:

- Ensure that your aggregation device is running Junos OS Release 14.2R3 or later, and that the satellite devices are running Junos OS Release 14.1X53-D16 or later.
- Ensure that you have prepared your satellite device for the installation, following the instructions in ["Preparing the Satellite Device" on page 57](#).

To autoconvert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device, if desired.



NOTE: You can cable the aggregation device to the satellite device at any point in this procedure.

When the aggregation device is cabled to the satellite device during this procedure, the process for converting a switch into a satellite device to finalize this process occurs immediately.

If the aggregation device is not cabled to the satellite device, the process for converting a switch into a satellite device to finalize this process starts when the satellite device is cabled to the aggregation device.

2. Log in to the aggregation device.
3. Configure the cascade ports. See ["Configuring the Cascade Ports on the Aggregation Device" on page 53](#).

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
```

4. Associate an FPC slot ID with each satellite device.

There are multiple methods of assigning FPC slot IDs. See ["Configuring the FPC Slot Identifiers" on page 54](#).

Examples:

- 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
```

- 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
```

- To map FPC slot ID to 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
```

5. (Recommended) Configure an alias name for the satellite device:

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

where *slot-id* is the FPC slot ID of the satellite device defined in the previous step, and *alias-name* is the alias.

For example, to configure the satellite device numbered 101 as **qfx5100-48s-1**:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 alias qfx5100-48s-1
```

6. Configure an FPC slot ID into a software upgrade group. See ["Configuring Software Upgrade Groups on the Aggregation Device" on page 55](#).

For example, to add the satellite device using FPC slot ID 101 to an existing software group named **group1**, or create a software upgrade group named **group1** and add the satellite device using FPC slot 101 to the software upgrade group:

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

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has already been created and a satellite software package association exists.

The configuration with the satellite software upgrade group must be committed before a satellite software image is associated with a satellite software upgrade group:

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

After committing the configuration, associate a satellite software image named **satellite-1.0R1.1-signed.tgz** to the upgrade group named **group1**:

```
user@aggregation-device> request system software add /var/tmp/satellite-1.0R1.1-signed.tgz
upgrade-group group1
```

7. Enable automatic satellite conversion:

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

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

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

8. Commit the configuration:

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

If you want to commit the configuration to both Routing Engines:

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

The satellite software upgrade on the satellite device begins after this final step is completed, or after you cable the satellite device to a cascade port using automatic satellite conversion if you have not already cabled the satellite device to the aggregation device.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion.

Manually Converting a Switch into a Satellite Device

Use this procedure to manually convert a switch into a satellite device after cabling it into the Junos Fusion Provider Edge.

This procedure should be used to convert a switch that is not currently acting as a satellite device into a satellite device. A switch might not be recognized as a satellite device for several reasons, including that the device was not previously autoconverted into a satellite device or that the switch had previously been reverted from a satellite device to a standalone switch.

Before you begin:

- Ensure that your aggregation device is running Junos OS Release 14.2R3 or later, and that the switches that will become satellite devices are running Junos OS Release 14.1X53-D16 or later.

- Ensure that you have prepared your switches that will become satellite devices for the installation, following the instructions in the ["Preparing the Satellite Device" on page 57](#) section.

To manually convert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device.
2. Log in to the aggregation device.
3. Configure the link on the aggregation device into a cascade port, if you have not done so already. See ["Configuring the Cascade Ports on the Aggregation Device" on page 53](#).

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
```

4. Associate an FPC slot ID with the satellite device.

There are multiple methods of assigning FPC slot IDs. See ["Configuring the FPC Slot Identifiers" on page 54](#).

Examples:

- 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
```

- 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
```

- To map FPC slot ID to 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
```

5. Configure the interface on the aggregation device into a software upgrade group. See ["Configuring Software Upgrade Groups on the Aggregation Device" on page 55](#).

For example, to add the satellite device using FPC slot ID 101 to an existing software group named **group1**, or create a software upgrade group named **group1** and add the satellite device using FPC slot 101 to the software upgrade group:

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

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has already been created and a satellite software package association exists.

The configuration with the satellite software upgrade group must be committed before a satellite software image is associated with the satellite software upgrade group:

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

After committing the configuration, associate a satellite software image named **satellite-1.0R1.1-signed.tgz** to the upgrade group named **group1**:

```
user@aggregation-device> request system software add /var/tmp/satellite-1.0R1.1-signed.tgz
upgrade-group group1
```

6. Commit the configuration:

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

If you want to commit the configuration to both Routing Engines:

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

7. Manually configure the switch into a satellite device:

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

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
```

The satellite software upgrade on the satellite device begins after this final step is completed.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion Provider Edge.

Configuring a Switch into a Satellite Device Before Interconnecting It into a Junos Fusion Provider Edge

Before you begin:

- Ensure that your switch that will become a satellite device is running Junos OS Release 14.1X53-D16 or later. See [Installing Software Packages on QFX Series Devices](#) for information on upgrading Junos OS on your device.
- Ensure that you have copied the satellite software onto the device that will become a satellite device.

Use this procedure to install the satellite software onto a switch before interconnecting it into the Junos Fusion Provider Edge as a satellite device. Installing the satellite software on a switch before interconnecting it into the Junos Fusion Provider Edge allows you to more immediately deploy the switch as a satellite device by avoiding the downtime associated with the satellite software installation procedure in the Junos Fusion Provider Edge.

You can manually install the satellite software onto a switch by entering the following command:

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

For instance, to install the satellite software package **satellite-1.0R1.1-signed.tgz** stored in the **/var/tmp/** folder on the switch:

```
user@satellite-device> request chassis device-mode satellite /var/tmp/satellite-1.0R1.1-signed.tgz
```

The device will reboot to complete the satellite software installation.

After the satellite software is installed, follow this procedure to connect the switch into the Junos Fusion Provider Edge:

1. Log in to the aggregation device.

2. Configure the link on the aggregation device into a cascade port, if you have not done so already. See ["Configuring the Cascade Ports on the Aggregation Device" on page 53](#).

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 assigning FPC slot IDs. See ["Configuring the FPC Slot Identifiers" on page 54](#).

Examples:

- 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
```

- 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
```

- To map FPC slot ID to 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. Configure the satellite switch into a satellite software upgrade group that is using the same version of satellite software that was manually installed onto the switch. See ["Configuring Software Upgrade Groups on the Aggregation Device" on page 55](#).

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 a link between the aggregation device and the satellite device.

RELATED DOCUMENTATION

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

[Understanding Junos Fusion Provider Edge Components | 4](#)

[Understanding Software in a Junos Fusion Provider Edge | 19](#)

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 | 51](#)

[Configuring or Expanding a Junos Fusion Enterprise](#)

Junos Fusion Provider Edge Administration

IN THIS CHAPTER

- [Managing Satellite Software Upgrade Groups in a Junos Fusion | 71](#)
- [Verifying Connectivity, Device States, Satellite Software Versions, and Operations in a Junos Fusion | 76](#)
- [Converting a Satellite Device in a Junos Fusion to a Standalone Device | 93](#)
- [Installing Junos OS Software on a Standalone Device Running Satellite Software | 98](#)

Managing Satellite Software Upgrade Groups in a Junos Fusion

IN THIS SECTION

- [Creating a Satellite Software Upgrade Group | 72](#)
- [Adding Satellite Devices to a Satellite Software Upgrade Group | 72](#)
- [Removing a Satellite Device from a Satellite Software Upgrade Group | 73](#)
- [Modifying the Satellite Software Used by a Satellite Software Upgrade Group | 74](#)
- [Deleting Associated Satellite Software from a Satellite Software Upgrade Group | 75](#)
- [Deleting Satellite Software on the Aggregation Device | 76](#)

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" on page 51](#) 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" on page 51](#) 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" on page 51](#) 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 | 51](#)
[Configuring or Expanding a Junos Fusion Enterprise](#)

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

IN THIS SECTION

- [Verifying a Junos Fusion Configuration | 77](#)
- [Verifying Basic Junos Fusion Connectivity | 78](#)
- [Verifying the Satellite Device Hardware Model | 80](#)
- [Verifying Cascade Port and Uplink Port State | 81](#)
- [Verifying That a Cascade Port Recognizes a Satellite Device | 85](#)
- [Verifying Extended Port Operation | 88](#)

- [Verifying the Satellite Software Version | 90](#)
- [Verifying the Devices and Software Used in a Satellite Software Upgrade Group | 92](#)

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 | 77](#)
- [Action | 77](#)
- [Meaning | 78](#)

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 | 78
- Action | 78
- Meaning | 79

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
```

| Alias | Slot | Device State | Cascade Ports | Port State | Extended Ports Total/Up |
|----------------|------|--------------|----------------------|------------------|-------------------------|
| qfx5100-24q-01 | 100 | Online | xe-0/0/1 xe-1/3/0 | online online | 9/2 |
| qfx5100-24q-02 | 101 | Online | xe-0/0/2 xe-1/3/1 | online online | 20/12 |

| | | | | | |
|----------------|-----|--------|----------|--------|-------|
| 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 | 80
- Action | 80
- Meaning | 81

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
```

| Slot | Device State | Model | Extended Ports 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 | 81
- Action | 81
- Meaning | 85

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 | 85](#)
- [Action | 85](#)
- [Meaning | 87](#)

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 | 88
- Action | 88
- Meaning | 90

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
```

| Name | State | Rx Request | Tx State | Admin/Op Request State | IFD 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 | 90
- Action | 90
- Meaning | 91

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
                  i386 ppc      group2
                  i386 ppc      group3
                  i386 ppc      group4
                  i386 ppc      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 | 92
- Action | 92
- Meaning | 93

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 | 51](#)

[Configuring or Expanding a Junos Fusion Enterprise](#)

Converting a Satellite Device in a Junos Fusion to a Standalone Device

IN THIS SECTION

- [Download Junos OS Software | 94](#)
- [Disable the Automatic Conversion Configuration | 95](#)
- [Install Junos OS Software on the Satellite Device | 96](#)

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*.



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*.

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
```

| Alias | Slot | Device State | Cascade Ports | Port State | Extended 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, uncalbe 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 | 19](#)

[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*, 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*.

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

CHAPTER 4

Power over Ethernet, LLDP, and LLDP-MED on a Junos Fusion Provider Edge

IN THIS CHAPTER

- [Understanding Power over Ethernet in a Junos Fusion | 100](#)
- [Understanding LLDP and LLDP-MED on a Junos Fusion | 103](#)
- [Configuring Power over Ethernet in a Junos Fusion | 105](#)
- [Verifying PoE Configuration and Status for a Junos Fusion \(CLI Procedure\) | 110](#)

Understanding Power over Ethernet in a Junos Fusion

IN THIS SECTION

- [Power over Ethernet in a Junos Fusion Overview | 101](#)
- [Understanding the Role of the Aggregation Devices for PoE Support in a Junos Fusion | 101](#)
- [Understanding the Role of the Satellite Devices for PoE Support in a Junos Fusion | 101](#)
- [Understanding PoE Configuration in a Junos Fusion | 102](#)
- [Understanding PoE Support Standards for Extended Ports in a Junos Fusion | 102](#)
- [Understanding Maximum PoE Power Budgets in a Junos Fusion | 102](#)
- [Understanding PoE Controller Software in a Junos Fusion | 103](#)
- [Understanding PoE Power Allocation Configuration Options in a Junos Fusion | 103](#)

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" on page 23](#)

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

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure)

Understanding LLDP and LLDP-MED on a Junos Fusion

IN THIS SECTION

- [LLDP and LLDP-MED in a Junos Fusion Overview | 104](#)
- [Understanding LLDP and LLDP-MED Configuration and Traffic Handling in a Junos Fusion | 104](#)

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 | 105](#)
- [Enabling PoE | 107](#)
- [Disabling PoE | 107](#)
- [Setting the Power Management Mode | 108](#)
- [Setting the Maximum Power That Can Be Delivered from a PoE Interface | 109](#)
- [Setting the Guard Band | 109](#)
- [Setting the PoE Interface Priority | 110](#)

PoE Configurable Options

[Table 6 on page 106](#) 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 6: 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: <ul style="list-style-type: none"> • 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 6: 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-extended
user@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)

Understanding Power over Ethernet in a Junos Fusion

Verifying PoE Configuration and Status for a Junos Fusion (CLI Procedure)

IN THIS SECTION

- [PoE Power Budgets, Consumption, and Mode on Satellite Devices | 111](#)
- [PoE Interface Configuration and Status | 112](#)

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 | 111
- Action | 111
- Meaning | 111

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 index | Maximum power | Power consumption | Guard band | Management | Status | Lldp 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 | 112

Action | 112

Meaning | 114

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 status | Oper status | Max power | Priority | Power consumption | Class |
| 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

Understanding Power over Ethernet in a Junos Fusion

Monitoring Junos Fusion Provider Edge

IN THIS CHAPTER

- [Connectivity Fault Management in Junos Fusion | 115](#)

Connectivity Fault Management in Junos Fusion

Connectivity fault management (CFM) allows the Ethernet network to be monitored according to IEEE 802.1AG and ITU-T Y.1731 standards. A CFM session monitors the maintenance endpoints (MEPs) in a maintenance association (MA). MEPS use continuity check messages (CCMs) to determine the connectivity status between MEPs in the MA.

Junos Fusion Provider Edge supports CFM sessions on the extended ports of the satellite devices via the cascade port on the aggregation device. The aggregation device handles and processes the transmission and reception of the CFM messages. From a CFM perspective, the satellite devices operate in a transparent mode.

CFM selects the cascade port that is associated with a satellite device as the anchor for the CFM sessions that are configured on the extended ports of the satellite device and it processes the sessions in the PFE that is associated with the cascade port. When a satellite device is connected to multiple cascade ports on the aggregation device, CFM selects the first available cascade port as the anchor. If the anchor cascade port fails, the next available cascade port is selected as anchor and the CFM sessions processing is moved to the PFE of newly selected anchor. The CFM sessions can flap when the sessions are re-anchored. During the switchover, the measurement interval in the CFM session restarts.

Junos Fusion Provider Edge supports the following CFM feature:

- Distributed and inline CFM sessions.
- CCM status for down MEPs and multiple up MEPs
- Support for link trace (LT) and loopback (LB).
- Delay measurement (DM) and synthetic loss measurement (SLM) as defined in ITU-T Y-1731 standard.

For more information on configuring CFM, see [IEEE 802.1ag OAM Connectivity Fault Management Overview](#)



NOTE: Junos Fusion Provider Edge only supports enhanced CFM mode.

SNMP MIB Support on Junos Fusion Provider Edge

IN THIS CHAPTER

- Chassis MIB Support (Junos Fusion) | 117

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 7 on page 117 shows the CIDXs used for satellite devices.

Table 7: CIDX's for Satellite Devices

| CIDX | Component Type |
|------|----------------|
| 102 | Power Supply |
| 104 | Fan |
| 107 | FPC |

Table 7: 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 8 on page 119](#) shows the SNMP traps that can be generated for satellite devices.

Table 8: 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 8: 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)
```


Link Aggregation and Link Aggregation Control Protocol on Junos Fusion Provider Edge

IN THIS CHAPTER

- [Understanding Link Aggregation and Link Aggregation Control Protocol in a Junos Fusion | 122](#)
- [Configuring an Aggregated Ethernet Interface | 124](#)
- [Configuring Junos OS for Supporting Aggregated Devices | 126](#)

Understanding Link Aggregation and Link Aggregation Control Protocol in a Junos Fusion

IN THIS SECTION

- [Link Aggregation in Junos Fusion | 122](#)
- [Link Aggregation Control Protocol in Junos Fusion | 123](#)
- [Configuring Link Aggregation and LACP in Junos Fusion | 123](#)
- [Software and Hardware Guidelines when Configuring Link Aggregation and LACP in Junos Fusion | 124](#)

Link Aggregation in Junos Fusion

Link aggregation is used to aggregate Ethernet interfaces between two devices. The aggregated Ethernet interfaces that participate in a *link aggregation group (LAG)* are called *member links*. Because a LAG is composed of multiple member links, even if one member link fails, the LAG continues to carry traffic over the remaining links.

Link Aggregation Control Protocol in Junos Fusion

Link Aggregation Control Protocol (LACP) is one method of bundling several physical interfaces to form one logical aggregated Ethernet interface. LACP is a subcomponent of the IEEE 802.3ad standard and is used as a discovery protocol. The LACP mode can be active or passive. The transmitting link is known as the *actor*, and the receiving link is known as the *partner*. If the actor and partner are both in passive mode, they do not exchange LACP packets, and the aggregated Ethernet links do not come up. If either the actor or partner is active, they do exchange LACP packets. By default, LACP is in passive mode on aggregated Ethernet interfaces. To initiate transmission of LACP packets and response to LACP packets, you must enable LACP active mode. You can configure Ethernet links to actively transmit protocol data units (PDUs), or you can configure the links to passively transmit them, sending out LACP PDUs only when they receive them from another link. You can configure both VLAN-tagged and untagged aggregated Ethernet interfaces without LACP enabled. 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 LAG without user intervention.
- Link monitoring to check whether both ends of the bundle are connected to the correct group.

The satellite devices provide network interfaces that send and receive network traffic and process the periodic transmission of LACP packets. You can include extended ports (physical interface on a satellite device that provides a connection to servers or endpoints) or local ports in LAGs and MC-LAGs, but not both.

When a dual-homed end device is deployed with Junos Fusion, the network interface cards form a LAG with the Junos Fusion. During a Junos Fusion upgrade, the end device may not be able to exchange LACP PDUs. In such a situation you can configure an interface to be in the up state even if no PDUs are exchanged. Use the `force-up` statement to configure an interface when the peer has limited LACP capability. The interface selects the associated LAG by default, whether the LACP mode is active or passive. When there are no received PDUs, the partner is considered to be working in the passive mode. Therefore, LACP PDU transmissions are controlled by the transmitting link.

Configuring Link Aggregation and LACP in Junos Fusion

1. Create a logical aggregated Ethernet interface.
2. Define the parameters associated with the logical aggregated Ethernet interface, such as a logical unit, interface properties, and Link Aggregation Control Protocol (LACP).
3. Define the member links to be contained within the aggregated Ethernet interface—for example, two local 10-Gigabit Ethernet interfaces on the aggregation device or two extended ports on the aggregation device.

- LAGs and MC-LAGs cannot include a mix of extended ports and local ports on the aggregation device.
- LAGs can span across multiple satellite devices in Junos Fusion Provider Edge.
- LAGs cannot contain both single-homed and multihomed members.
- Existing restrictions that apply to LAGs and MC-LAGs also apply to LAGs and MC-LAGs that include extended ports.

4. Configure LACP for link detection.

Software and Hardware Guidelines when Configuring Link Aggregation and LACP in Junos Fusion

Keep in mind these hardware and software guidelines:

- Up to 1750 LAGs are supported in Junos Fusion Provider Edge and Junos Fusion Enterprise, and the LAGs are numbered from ae0 through ae4091.
- Up to 16 members are supported in a LAG in Junos Fusion Provider Edge and Junos Fusion Enterprise.
- Configure the LAG 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.
- Configure LACP for dual-homed extended ports identically on both of the aggregation devices; otherwise LACP will not be in a forwarding state.

RELATED DOCUMENTATION

[Junos Fusion Provider Edge Overview | 2](#)

[Understanding Junos Fusion Ports](#)

[Configuring Junos OS for Supporting Aggregated Devices](#)

Configuring an Aggregated Ethernet Interface

On Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces on M Series and T Series routers, you can associate a physical interface with an aggregated Ethernet interface.



NOTE: On a Junos Fusion, you can include extended ports (physical interface on a satellite device that provides a connection to servers or endpoints) or local ports in link aggregation groups (LAGs) and MC-LAGs, but not both. For information on extended ports, see *Understanding Junos Fusion Ports*.

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 (fastether-options | gigether-options) 802.3ad aex
```

You specify the interface instance number x to complete the link association; x can be from 0 through 127, for a total of 128 aggregated interfaces on M Series and T Series routers and can be from 1 through 480, for a total of 480 aggregated interfaces on MX Series routers. For MX Series routers running Junos release 14.2R3 and later you can configure a maximum of 1000 aggregated interfaces. Aggregated interfaces are numbered from ae0 through ae4092.



NOTE: On MX2010 and MX2020 routers you can configure a maximum of 800 aggregated interfaces.

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](#), and for a sample configuration, see [Example: Configuring Aggregated Ethernet Interfaces](#).



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.

Configuring Junos OS for Supporting Aggregated Devices

IN THIS SECTION

- [Configuring Virtual Links for Aggregated Devices | 126](#)
- [Configuring LACP Link Protection at the Chassis Level | 128](#)
- [Enabling LACP Link Protection | 129](#)
- [Configuring System Priority | 129](#)
- [Configuring the Maximum Links Limit | 130](#)
- [Configuring PPM on Junos Fusion | 130](#)

Junos OS supports the aggregation of physical devices into defined virtual links, such as the link aggregation of Ethernet interfaces defined by the IEEE 802.3ad standard.

Tasks for configuring aggregated devices are:

Configuring Virtual Links for Aggregated Devices

To define virtual links, you need to specify the associations between physical and logical devices within the [edit interfaces] hierarchy, and assign the correct number of logical devices by including the device-count statement at the [edit chassis aggregated-devices ethernet] and [edit chassis aggregated-devices sonet] hierarchy levels:

```
[edit chassis]
aggregated-devices {
  ethernet {
    device-count number;
```

```

    }
    sonet {
        device-count number;
    }
}

```

The aggregated interfaces are numbered from ae0 through ae4091. The maximum number of aggregated interfaces supported by different routers is listed below:

- For PTX Series routers, you can configure a maximum of 128 aggregated interfaces.
- For M Series and T Series routers, you can configure a maximum of 128 aggregated interfaces (LAG bundles).
- In Junos release 14.2R2 and earlier, you can configure a maximum of 480 aggregated interfaces on MX Series routers.
- In Junos release 14.2R3 and later, you can configure a maximum of 1000 aggregated interfaces on MX240, MX480, and MX960 routers.
- In Junos release 14.2R3 and later, you can configure a maximum of 800 aggregated interfaces on MX2010 and MX2020 routers.
- In Junos OS 15.1F5 and 15.1F6 releases, you can configure a maximum of 480 aggregated interfaces on MX240, MX480, and MX960 routers.
- In Junos OS 15.1F5 and 15.1F6 releases, you can configure a maximum of 800 aggregated interfaces on MX2010 and MX2020 routers.

For SONET/SDH, starting with Junos OS Release 13.2, the maximum number of logical interfaces is 64, numbered from as0 through as63. In releases before Junos OS Release 13.2, the maximum was 16.

[Table 9 on page 127](#) lists the MX Series routers and the maximum number of interfaces per LAG and the maximum number of LAG groups they support. MX Series routers can support up to 64 LAGs.

Table 9: Maximum Interface Per LAG and Maximum LAGs per MX Router

| MX Series Routers | Maximum Interfaces per LAG | Maximum LAG Groups |
|----------------------------------|----------------------------|---|
| MX5, MX10, MX40, MX80, and MX104 | 16 | Limited by the interface capacity. 80 on MX104. |

Table 9: Maximum Interface Per LAG and Maximum LAGs per MX Router (Continued)

| MX Series Routers | Maximum Interfaces per LAG | Maximum LAG Groups |
|--|----------------------------|--------------------|
| MX240, MX480, MX960, MX10003, MX2010, and MX2020 | 64 | 1000 |

Configuring LACP Link Protection at the Chassis Level

Link Aggregation Control Protocol (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. 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 link protection enables you to force active and standby links within an aggregated Ethernet. You configure LACP link protection by using the `link-protection` and `system-priority` statements at either the chassis or interface level and by configuring port priority at the interface level using the `system-priority` statement. Configuring LACP parameters at the chassis level results in all aggregated Ethernet interfaces using the defined values unless overridden by the LACP configuration on a specific interface.

```
[edit chassis]
aggregated-devices {
  ethernet {
    lacp {
      link-protection {
        non-revertive;
      }
      system-priority priority;
    }
  }
}
```



NOTE: LACP link protection also uses port priority. You can configure port priority at the Ethernet interface `[gigether-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).

Enabling LACP Link Protection

To enable LACP link protection for aggregated Ethernet interfaces on the chassis, use the `link-protection` statement at the `[edit chassis aggregated-devices ethernet lacp]` hierarchy level:

```
[edit chassis aggregated-devices ethernet lacp]
link-protection {
    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, after 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.



BEST PRACTICE: (MX Series) In a highly scaled configuration over aggregated Ethernet, we recommend that you prevent the router from performing such a switch by including the `non-revertive` statement. Failure to do so may result in some traffic loss if a MIC on which a member interface is located reboots. Using the `non-revertive` statement for this purpose is not effective if both the primary and secondary interfaces are on the MIC that reboots.



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.

Configuring System Priority

To configure LACP system priority for aggregated Ethernet interfaces on the chassis, use the `system-priority` statement at the `[edit chassis aggregated-devices ethernet lacp]` hierarchy level:

```
[edit chassis aggregated-devices ethernet lacp]
system-priority 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 through 65,535.

Configuring the Maximum Links Limit

To configure the maximum links limit, use the `maximum-links` statement at the `[edit chassis aggregated-devices]` hierarchy level:

```
[edit chassis aggregated-devices]
maximum-links maximum-links-limit;
```

Configuring PPM on Junos Fusion

If you use Junos Fusion with Junos OS Release 14.2R3, you need to ensure that link aggregation (and STP) work properly by configuring timers for the periodic packet management (PPM) daemons on the aggregation and satellite devices. We recommend using the following timer values:

```
[edit routing-options ppm]
redistribution-timer 120;
tcp-keepalive-interval 3000;
tcp-keepalive-idle 3000;
```

Starting in Junos OS Release 14.2R4, the timer values that ensure proper link aggregation and STP functions are configured by default if you use Junos Fusion with Junos OS.

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 |
|---------|--|
| 15.1F5 | In Junos OS 15.1F5 and 15.1F6 releases, you can configure a maximum of 480 aggregated interfaces on MX240, MX480, and MX960 routers. |
| 15.1F5 | In Junos OS 15.1F5 and 15.1F6 releases, you can configure a maximum of 800 aggregated interfaces on MX2010 and MX2020 routers. |
| 14.2R4 | Starting in Junos OS Release 14.2R4, the timer values that ensure proper link aggregation and STP functions are configured by default if you use Junos Fusion with Junos OS. |
| 14.2R3 | In Junos release 14.2R3 and later, you can configure a maximum of 1000 aggregated interfaces on MX240, MX480, and MX960 routers. |

| | |
|--------|---|
| 14.2R3 | In Junos release 14.2R3 and later, you can configure a maximum of 800 aggregated interfaces on MX2010 and MX2020 routers. |
| 14.2R3 | If you use Junos Fusion with Junos OS Release 14.2R3, you need to ensure that link aggregation (and STP) work properly by configuring timers for the periodic packet management (PPM) daemons on the aggregation and satellite devices. |
| 14.2R2 | In Junos release 14.2R2 and earlier, you can configure a maximum of 480 aggregated interfaces on MX Series routers. |
| 13.2 | For SONET/SDH, starting with Junos OS Release 13.2, the maximum number of logical interfaces is 64, numbered from as0 through as63. |

Uplink Failure Detection on Junos Fusion Provider Edge

IN THIS CHAPTER

- Overview of Uplink Failure Detection on a Junos Fusion | 132
- Configuring Uplink Failure Detection on a Junos Fusion | 134

Overview of Uplink Failure Detection on a Junos Fusion

The uplink failure detection feature on a Junos Fusion enables satellite devices to detect link failures on the uplink interfaces used to connect to aggregation devices. When uplink failure detection detects uplink failure on a satellite device, all of the device's extended ports (which connect to host devices) are shut down. Shutting down the extended ports allows downstream host devices to more quickly identify and adapt to the outage. For example, when a host device is connected to two satellite devices, and uplink failure detection shuts down the extended ports on one satellite device, the host device can more quickly recognize the uplink failure and redirect traffic through the other, active satellite device.

You can configure uplink failure detection globally, for all satellite devices of a Junos Fusion, and for individual satellite devices. Uplink failure detection configuration at the satellite device level overrides the global uplink failure detection configuration.

Uplink failure detection configuration allows you to configure these options:

- The minimum number of active uplink ports a satellite device must have to remain active. The default is one active uplink port. You can use this option to specify more minimum active ports.
- The amount of time uplink failure detection waits to try to re-enable disabled extended ports. This wait time is called a hold-down period. It is intended to avoid port flapping on the extended ports when uplink port connectivity is unstable. The default hold-down period is six seconds.

Uplink failure detection must know which ports on a satellite device can be used as uplink ports. These are called candidate uplink ports. [Table 10 on page 133](#) shows the default set of candidate uplink ports that uplink failure detection selects for failure detection. If you choose not to use the default uplink ports for your satellite devices, you need to specify which uplink ports you want to use for uplink failure

detection by creating a candidate uplink port profile and applying it to the satellite device's uplink failure detection configuration.



CAUTION: The physically connected uplink ports on a satellite device must be defined as candidate uplink ports in the Junos Fusion configuration. If the uplink ports on a satellite device are not configured as candidate uplink ports, uplink failure detection cannot be enabled on the device, and a system log message is generated.

Table 10: UFD Default Uplink Interfaces for Satellite Devices

| Device Type | Default Uplink Interfaces |
|--|---|
| 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 |
| EX4300-48T (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 |
| QFX5100-24Q-2P (4 ports on PIC 0) | 0/20 through 0/23 |
| QFX5100-48S-6Q (6 QSFP+ ports) | 0/48 through 0/53 |
| QFX5100-48T-6Q (6 QSFP+ ports) | 0/48 through 0/53 |
| QFX5100-96S-8Q (8 QSFP+ ports) | 0/96 through 0/103 |

RELATED DOCUMENTATION

[Overview of Uplink Failure Detection on a Junos Fusion](#) | 132

Configuring Uplink Failure Detection on a Junos Fusion

IN THIS SECTION

- [Enabling Uplink Failure Detection on a Junos Fusion | 134](#)
- [Configuring a Candidate Uplink Port Policy | 136](#)
- [Configuring an Uplink Port Group | 139](#)

The uplink failure detection feature on a Junos Fusion enables satellite devices to detect link failures on the uplink interfaces used to connect to aggregation devices. When uplink failure detection detects uplink failure on a satellite device, all of the device's extended ports (which connect to host devices) are shut down.

The following topics describe how to configure uplink failure detection on a Junos Fusion:

Enabling Uplink Failure Detection on a Junos Fusion

You can enable uplink failure detection on a Junos Fusion at the following levels in the configuration hierarchy:

- To enable uplink failure detection globally, for all satellite devices in the Junos Fusion, include the uplink failure detection configuration at the `[edit chassis satellite-management]` level.
- To enable uplink failure detection on a specific satellite device, include the uplink failure detection configuration at the `[edit chassis satellite-management fpc slot-id]` level. Uplink failure detection configuration applied to a satellite device overrides the global uplink failure detection configuration.

Uplink failure detection configuration syntax is the same at all hierarchy levels. This topic shows how to configure uplink failure detection at the global level, but you can also apply uplink failure detection configuration at the satellite device level.

To enable uplink failure detection on a Junos Fusion, do the following on the fabric's aggregation device:

1. Enable uplink failure detection with default settings:

```
[edit chassis satellite-management]
user@switch# set uplink-failure-detection
```

The default configuration parameters are described in [Table 11 on page 135](#).

2. (Optional) Apply custom uplink failure detection settings by specifying a candidate uplink port policy:

```
[edit chassis satellite-management uplink-failure-detection]
user@switch# candidate-uplink-policy policy-name
```

For information about configuring candidate uplink policies, see ["Configuring a Candidate Uplink Port Policy" on page 136](#).

Table 11: Junos Fusion Uplink Failure Detection Default Configuration

| Configuration Parameter | Description | Default |
|-------------------------|---|--|
| holddown | Configures the interval of time uplink failure detection waits before trying to re-enable a satellite device's extended ports after shutting them down due to an uplink port failure. | 6 seconds |
| minimum-links | Configures the minimum number of active uplink ports a satellite device must have. If a satellite device has fewer than this number of active uplink ports, uplink failure detection shuts down its extended ports. | 1 link |
| uplink-port-group | Defines a set of candidate uplink ports to assign to satellite devices. | Each satellite device model has a set of default uplink ports. You only need to assign uplink ports if you do not want to use the default ports. See UFD Default Uplink Interfaces for Satellite Devices on page 133 for the default uplink ports by device. |

Configuring a Candidate Uplink Port Policy

IN THIS SECTION

- [Configuring Candidate Uplink Port Policy Default Configuration | 136](#)
- [Configuring Candidate Uplink Port Policy Terms | 137](#)

A candidate uplink port policy contains uplink failure detection uplink port configuration that you can apply to satellite devices to override the default uplink failure detection behavior.

You can enter configuration statements in a candidate uplink port policy at these levels of the hierarchy:

- Enter configuration statements at the level `[edit policy-options satellite-policies candidate-uplink-port-policy policy-name]` to override the default uplink failure detection behavior. Statements configured at this level are applied if the policy is applied to a satellite device that does not match a `product-model` statement in any term in the policy. If the policy contains no terms, the statements at this level are applied to every satellite device to which the policy is applied.
- Create terms within the candidate uplink port policy at the level `[edit policy-options satellite-policies candidate-uplink-port-policy policy-name term term-name]`. Use terms to apply different uplink failure detection configurations to certain satellite devices, based on their product model. Each term contains match criteria that is compared against the model name of each satellite device to which the policy is applied. If the criteria matches the device model, the configuration specified in the term is applied to the device. Terms are evaluated in the order they appear in the configuration. The first term that matches a satellite device is applied to the device.

Configuring a candidate uplink port policy is described in the following sections:

Configuring Candidate Uplink Port Policy Default Configuration

Uplink failure detection has the following default configuration parameters that apply if you enable uplink failure detection with no additional configuration:

- The default configuration settings are described in [Table 11 on page 135](#).
- The default uplink ports that are assigned to each satellite device type are described in ["Overview of Uplink Failure Detection on a Junos Fusion" on page 132](#).

A candidate uplink port policy can contain configuration statements that override the defaults if the policy is applied to a satellite device that does not match a `product-model` statement in any term in the policy.

To configure a candidate uplink port policy default configuration:

1. (Optional) Specify the interval of time uplink failure detection waits before trying to re-enable a satellite device's extended ports after shutting them down due to an uplink port failure:

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

2. (Optional) Specify the minimum number of active uplink ports a satellite device must have. If a satellite device has fewer than this number of active uplink ports, uplink failure detection shuts down its extended ports:

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

3. (Optional) Specify an uplink port group to assign to satellite devices:

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

For information about configuring an uplink port group, see ["Configuring an Uplink Port Group" on page 139](#).

Configuring Candidate Uplink Port Policy Terms

You can configure terms in a candidate uplink port policy to apply uplink failure detection configuration to certain satellite devices, based on their device model. For example, you can create a term that matches all QFX 5100 Series switches. When the policy is applied to a QFX 5100 Series switch, the other configuration statements in the term are applied to the switch. If the policy is applied to satellite devices that are not QFX 5100 Series switches, the configuration statements in the term are not applied. When a candidate uplink port policy has multiple terms, the terms are evaluated in the order they appear in the configuration. The first term that matches a satellite device is applied to that satellite device.

To configure a candidate uplink port policy term:

1. Specify which device models the term will apply to:

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


The other configuration statements in the term are only applied to satellite devices whose device model matches the match term *model-name*.

The match term *model-name* can be a complete device model name, to match that device model exactly. You can also use the wildcard character (*) in the match term to match zero or more of any character.

Some examples of using the wildcard character in the match term:

- To apply the satellite policy to all EX 4300 Series switches in the satellite device role, enter EX4300* as the *model-name*.
- To apply the satellite policy to all QFX 5100 Series switches in the satellite device role, enter QFX5100* as the *model-name*.
- To apply the satellite policy to QFX 5100 Series switches with model names that start with QFX5100-96, enter QFX5100-96* as the *model-name*.

2. (Optional) Specify the interval of time uplink failure detection waits to re-enable a satellite device's extended ports after shutting them down due to an uplink port failure:

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

3. (Optional) Specify the minimum number of active uplink ports a satellite device must have. If a satellite device has fewer than this number of active uplink ports, uplink failure detection shuts down its extended ports:

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

4. (Optional) Specify an uplink port group to assign to satellite devices:

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

For information about configuring an uplink port group, see ["Configuring an Uplink Port Group" on page 139](#).

Configuring an Uplink Port Group

An 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. Every satellite device type has default candidate uplink ports, which are described in ["Overview of Uplink Failure Detection on a Junos Fusion" on page 132](#). You do not need to create uplink ports groups if you want to use the default candidate uplink ports on satellite devices.



CAUTION: The physically connected uplink ports on a satellite device must be defined as candidate uplink ports in the Junos Fusion configuration. If the uplink ports on a satellite device are not configured as candidate uplink ports, uplink failure detection cannot be enabled on the device, and a system log message is generated.

To create an uplink port group:

1. Specify the uplink port group name:

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

2. Configure the PICs that will 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 that will 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]
```

RELATED DOCUMENTATION

| [Overview of Uplink Failure Detection on a Junos Fusion](#) | 132

Multicast Replication on Junos Fusion Provider Edge

IN THIS CHAPTER

- [Understanding Multicast Replication in a Junos Fusion | 140](#)
- [Ingress Replication at the Aggregation Device to Satellite Devices | 144](#)
- [Egress \(Local\) Replication on the Satellite Devices | 145](#)
- [Configuring Egress \(Local\) Replication on a Junos Fusion | 151](#)

Understanding Multicast Replication in a Junos Fusion

IN THIS SECTION

- [Junos Fusion Multicast Replication Overview | 140](#)
- [ECIDs for Multicast Traffic | 142](#)
- [Multicast Replication Limitations in a Junos Fusion | 143](#)

This topic introduces how multicast packets are replicated in a Junos Fusion and forwarded to multicast subscribers on satellite device extended ports.

Junos Fusion Multicast Replication Overview

Aggregation devices and satellite devices work together to manage the traffic flow from multicast sources to multicast destination ports in a Junos Fusion, resolving a source packet forwarding path to multiple destination ports.

Multicast source packets might be received through a network port on the aggregation device or an extended port on a satellite device. When a multicast source packet ingresses at a satellite device, the satellite device sends the source packet on an uplink port to the aggregation device. The satellite device load-balances forwarded source traffic over the available uplink ports to the aggregation device.

The aggregation device that initially receives the source traffic to be forwarded is referred to as the *ingress aggregation device*. All multicast destination resolution is done on the aggregation devices. In Junos Fusion architectures with multiple aggregation devices, the ingress aggregation device also forwards the multicast traffic to the other aggregation device or devices to reach multicast subscribers that are only accessible through those other devices, or to support the forwarding behavior of a particular Junos Fusion architecture.

To forward multicast traffic to destinations on satellite device extended ports, the aggregation device uses E-channel Identifier (ECID) mappings to determine the forwarding paths to the destination extended ports, including which cascade ports link to the corresponding satellite devices. (See ["ECIDs for Multicast Traffic" on page 142](#).) Multicast traffic flowing from the aggregation device to destination satellite devices is load-balanced over the available cascade ports to each destination satellite device. Satellite devices use the ECID in the multicast packets from the aggregation device to determine which local port or ports should receive the multicast traffic.



NOTE: This behavior applies similarly to flooding unknown unicast traffic within a VLAN in a Junos Fusion.

By default, the ingress aggregation device replicates multicast and broadcast packets to forward to each destination extended port. This behavior is referred to as *ingress multicast replication*. The aggregation device sends multiple copies of the packet to each satellite device, one copy for each destination extended port on that satellite device, identified by the extended port's unicast ECID. See ["Ingress Replication at the Aggregation Device to Satellite Devices" on page 144](#) for more information.

Junos Fusion supports enabling *egress multicast replication*, also referred to as *local replication*, where satellite devices replicate the multicast and broadcast packets destined for their local ports. Egress or local replication uses special multicast ECIDs corresponding to one or more extended ports to which a satellite device should forward the traffic. (See ["ECIDs for Multicast Traffic" on page 142](#).) Local replication helps to distribute most of the replication load from aggregation devices to the satellite devices where the traffic egresses, and reduces traffic on cascade ports. When enabled, local replication applies to all satellite devices in the Junos Fusion; you cannot enable it only for individual satellite devices.

Local replication behavior differs slightly for different types of multicast and broadcast traffic, and for different Junos Fusion architectures. See ["Egress \(Local\) Replication on the Satellite Devices" on page 145](#) for details.

To avoid creating loops and broadcast storms, for both ingress and egress multicast replication, both the aggregation devices and satellite devices maintain split-horizon next-hop information to prevent resending multicast or broadcast packets back out of the ingress port.

ECIDs for Multicast Traffic

Traffic sent between aggregation devices and satellite devices is sent over a logical path, called an *e-channel*. The packets sent between the aggregation device and satellite device include the IEEE 802.1BR E-channel tag (ETAG) header with an E-channel identifier (ECID). The ECID identifies the path that will be used in forwarding traffic packets. Each extended port is identified by a unique ECID value. Junos Fusion reserves ECID values 1 through 4095 for unicast data packets. ECID values from 4096 through 16382, also called *multicast ECIDs*, are reserved for multicast, VLAN flooding, and broadcast data packets. Multicast ECIDs correspond to one or more destination extended ports on a satellite device.

The aggregation device automatically creates virtual interfaces named *sd-fpc-id/0/0* (where *fpc-id* is the satellite device ID) to represent satellite devices, and uses these virtual interfaces as the next-hop interface when forwarding traffic to a satellite device.

When local replication is disabled, similar to unicast packet flow (see *Understanding the Flow of Data Packets in a Junos Fusion Topology*), the aggregation device assigns a unicast ECID value for each destination extended port on a satellite device for both unicast traffic and multicast traffic. The aggregation device replicates multicast packets, tags them with the assigned ECID for the destination, and sends a copy to each destination extended port by way of the corresponding satellite device interface.

When local replication is enabled, Junos Fusion uses ECID values greater than 4095 to identify multicast traffic and associate one or more extended ports on a satellite device as the multicast destination. Junos Fusion dynamically assigns multicast ECID values. When the aggregation device requires a new multicast ECID value for a group of ports or if it needs to add a port to an existing ECID, the process is as follows:

1. The aggregation device sends a request to the satellite device to assign an ECID value (or update an existing ECID mapping when multicast group or VLAN membership changes).
2. The satellite device assigns an ECID value and adds an entry to its ECID table to map the ECID value to the corresponding extended ports.
3. The satellite device sends a message back to the aggregation device with the ECID value that satisfies the request for the corresponding extended ports.
4. The aggregation device adds this information to its ECID table. It uses the *sd* virtual interface as the next-hop interface to send multicast traffic for those extended ports on the satellite device.

When the satellite device receives a data packet from the aggregation device with a multicast ECID value, the satellite device begins to replicate and forward packets to the extended ports associated with that ECID. Satellite devices do not do multicast lookups; they only maintain ECID tables to determine the port or ports corresponding to an ECID in a packet received from the aggregation device. The aggregation devices perform all multicast route maintenance and forwarding path resolution.

An ECID value is only unique locally on the satellite device. Another satellite device can use the same ECID value for its own extended ports. The aggregation device maintains a composite mapping of ECID values to the different satellite devices and the corresponding extended ports on those satellite devices.

Multicast Replication Limitations in a Junos Fusion

Junos Fusion strives to optimize data replication on satellite devices when local replication is enabled. However, for the following features, although local replication might be enabled, Junos Fusion does not trigger egress replication optimization, and instead defaults to using ingress replication:

- Multicast traffic on pure Layer 3 extended ports
- Multicast Listener Discovery (MLD) snooping on an IPv6 network

You might choose not to enable local replication because egress multicast replication is incompatible with some Junos OS protocol and traffic management features programmed on individual extended ports. The following features do not work when egress multicast replication is enabled; if you want to use these features, you cannot take advantage of egress replication optimizations:

- VLAN tag manipulations, such as VLAN tag translations, VLAN tag stacking, and VLAN per-port policies. Using egress multicast replication with this feature can cause dropped packets due to unexpected VLAN tags.
- Multicast support for the extended ports on the edge side of Pseudowire connection in a VPLS network.
- Multicast support for the extended ports on the edge side of EVPNs.
- Multicast VPN deployments.
- Features that perform egress actions on individual extended ports, such as egress local-port mirroring (port mirroring on endpoints connected to satellite device extended ports).

RELATED DOCUMENTATION

[Ingress Replication at the Aggregation Device to Satellite Devices | 144](#)

[Egress \(Local\) Replication on the Satellite Devices | 145](#)

[Configuring Egress \(Local\) Replication on a Junos Fusion | 151](#)

Understanding the Flow of Data Packets in a Junos Fusion Topology

Ingress Replication at the Aggregation Device to Satellite Devices

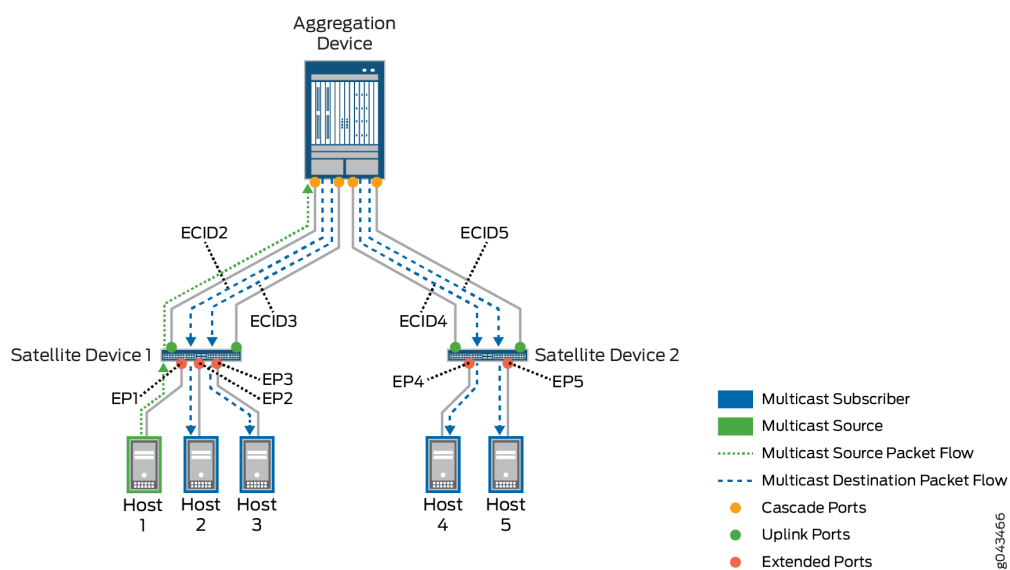
By default, Junos Fusion uses ingress replication on the aggregation devices to replicate and forward copies of packets to multicast destinations.

In ingress replication mode, the ingress aggregation device replicates the multicast packets and forwards them to every destination extended port. The data packet flow is similar to unicast data packet flow from the multicast source to each destination.

Figure 12 on page 144 shows multicast source data packets received from a multicast source on an extended port, EP1, with traffic destined for endpoints connected to extended ports EP2 through EP5. Each extended port has an associated E-channel Identifier (ECID) value that the aggregation device uses to forward the data packet to each destination extended port. The aggregation device replicates the data packets for all multicast destination extended ports on all attached satellite devices, as follows:

- Two copies for satellite device 1 (for EP2 and EP3)
- Two copies for satellite device 2 (for EP4 and EP5)

Figure 12: Ingress Replication at the Aggregation Device



The aggregation device sends each packet on the respective cascade ports to the satellite devices with destination extended ports. Multicast traffic destined for EP2 is tagged with ECID2, traffic destined for EP3 is tagged with ECID3, and so on for all the destination extended ports on both satellite devices. The satellite devices receive and forward the packets to their respective extended ports.

The aggregation device maintains multicast routing information and next-hop tables, including ECID label mappings to satellite devices and the corresponding extended ports. For a multicast destination on a satellite device, the aggregation device resolves the next-hop path through a corresponding cascade port that reaches the satellite device. When there are multiple cascade port links to a satellite device, the aggregation device load-balances the traffic to choose which cascade port to use.

Each receiving satellite device maintains tables that map the assigned ECIDs to the corresponding extended ports, and simply forwards outgoing multicast packets to the destination extended ports. The satellite devices do not maintain multicast routing information.

Other multicast destinations might be reached through local ports on the aggregation device, rather than through extended ports. For these destinations, the aggregation device creates and sends copies to those local ports directly.

Multicast support using ingress replication does not scale well for a large number of multicast destinations or higher bandwidth multicast traffic. Ingress replication increases aggregation device Packet Forwarding Engine processing load and consumes bandwidth on the links between cascade ports and uplink ports, potentially resulting in link oversubscription and latency among multicast recipients.

You can alternatively enable *egress multicast replication*, also referred to as *local replication*. Local replication optimizes multicast replication by distributing the replication load between the aggregation devices and the satellite devices that have multicast destination ports. However, local replication requires more control plane processing than ingress replication, which results in a slight increase in multicast group join and leave latency. See ["Egress \(Local\) Replication on the Satellite Devices" on page 145](#) for more information on how local replication works for different types of multicast or broadcast traffic.

RELATED DOCUMENTATION

[Understanding Multicast Replication in a Junos Fusion | 140](#)

[Egress \(Local\) Replication on the Satellite Devices | 145](#)

Understanding the Flow of Data Packets in a Junos Fusion Topology

Egress (Local) Replication on the Satellite Devices

IN THIS SECTION

● [Local Replication for Layer 2 Multicast Traffic with IGMP Snooping | 146](#)

- [Local Replication for VLAN Flooding | 148](#)
- [Local Replication for Layer 3 Multicast Traffic Over IRB Interfaces | 149](#)

Egress multicast replication in a Junos Fusion is referred to as *local replication*. In egress or local replication mode, the aggregation device optimizes replication by off-loading replication whenever possible to satellite devices that have destination extended ports. From the point of view of the aggregation device, replication is supported at an egress port, and from the point of view of the satellite device, replication is managed locally. Local replication alleviates some of the problems associated with ingress replication, reducing the potential for bandwidth oversubscription and replication latency when there are a large number of receivers.

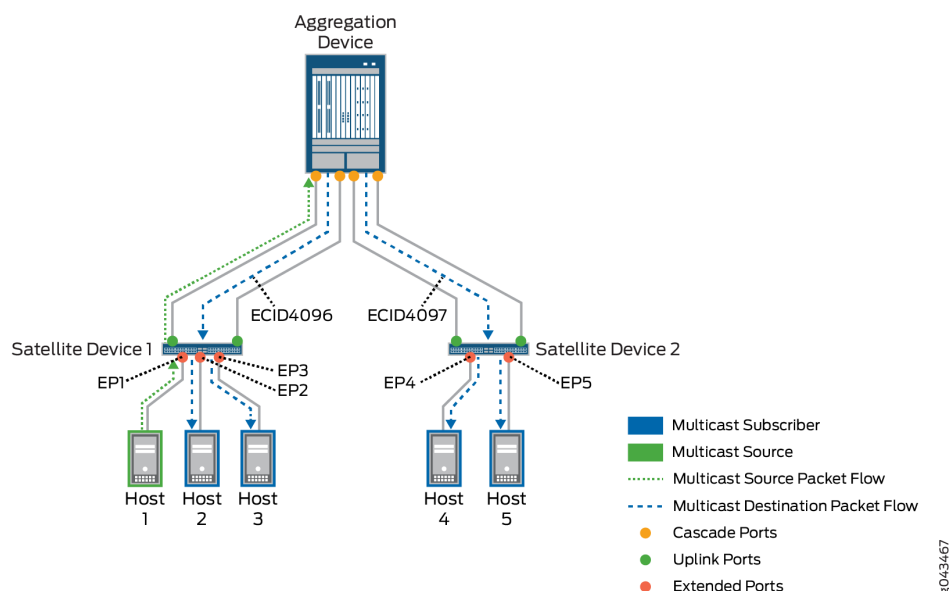
Local replication is performed at Layer 2. Each receiving satellite device maintains tables that map the assigned ECIDs to corresponding destination extended ports, and simply forward outgoing multicast or broadcast packets to local extended ports. For Layer 3 multicast traffic, such as when forwarding packets between VLANs, the aggregation device performs replication to resolve Layer 3 information not maintained by satellite devices.

This topic describes local replication behavior for multicast traffic forwarded to the access side both within and across VLANs and when flooding traffic within a VLAN.

Local Replication for Layer 2 Multicast Traffic with IGMP Snooping

[Figure 13 on page 147](#) illustrates Layer 2 multicast traffic flow with IGMP snooping when local replication is enabled.

Figure 13: Local Replication with Layer 2 Multicast and IGMP Snooping in Junos Fusion



A data packet is received from a multicast source on an extended port, EP1, with traffic destined for endpoints connected to extended ports EP2 through EP5. The aggregation device acquires *multicast* ECIDs from the satellite devices, which represent a set of multicast destination extended ports on each satellite device. The diagram shows ECID value ECID4096 is assigned to the multicast subscribers behind extended ports EP2 and EP3 on satellite device 1, and ECID4097 is assigned to the multicast subscribers behind extended ports EP4 and EP5 on satellite device 2. The aggregation device creates only one copy of the source packet for each satellite device that has multicast destination extended ports, inserts the corresponding satellite device multicast ECID value in the IEEE 802.1BR ETAG header of each copy, and forwards the copies to those satellite devices.

In this case, the aggregation device creates two copies, forwards one with ECID4096 to satellite device 1, and forwards the other with ECID4097 to satellite device 2. Each satellite device receives its copy and uses the multicast ECID value to determine which of its extended ports should receive the multicast traffic. Satellite device 1 replicates the packet and forwards copies to EP2 and EP3; satellite device 2 replicates the packet and forwards copies to EP4 and EP5.

When forwarding replicated multicast packets to satellite devices, the aggregation device resolves the next-hop path through a corresponding cascade port that reaches the satellite device. When there are multiple cascade port links to a satellite device, the aggregation device load-balances the traffic when choosing which cascade port to use.

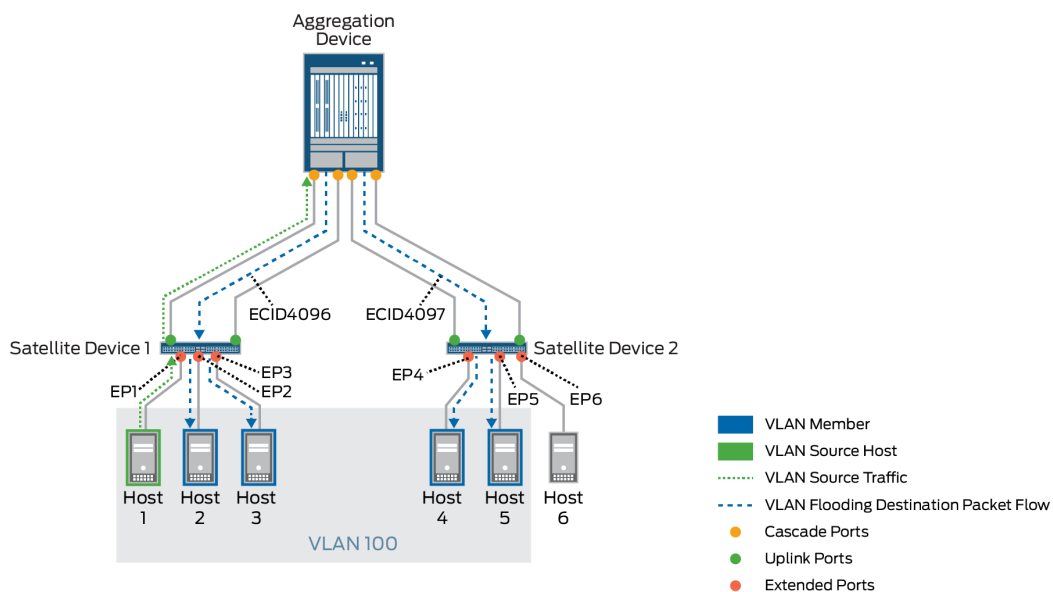
Other multicast destinations might be reached through ports on the aggregation devices, rather than through extended ports. For these destinations, the aggregation device creates and sends copies to those local ports directly.

Local Replication for VLAN Flooding

An aggregation device might initiate VLAN flooding (broadcasting or flooding the packet out to all interfaces in the VLAN) to learn the MAC address for a destination that is not already in its Ethernet switching tables. When local replication is not enabled, the aggregation device uses ingress replication, creating and sending copies to each destination extended port on each satellite device that has destination extended ports in the VLAN. With local replication enabled, the aggregation device requests multicast ECIDs to represent the extended ports in the VLAN on each satellite device. The aggregation device sends a copy of the source packet tagged with each ECID in the IEEE 802.1BR header to the corresponding satellite device. Each receiving satellite device does the replication locally for its extended ports in the VLAN.

Figure 14 on page 148 illustrates the packet flow for VLAN flooding when local replication is enabled.

Figure 14: Local Replication with VLAN Flooding



In this example, a multicast source packet for VLAN 100 ingresses on EP1, and satellite device 1 forwards the packet to the aggregation device. The aggregation device cannot resolve the destination MAC address, and decides to flood the packet to all extended port destinations in VLAN 100.



NOTE: When a source packet ingresses at a satellite device with uplink ports to dual aggregation devices, the satellite device load-balances forwarding the ingress traffic among the available uplink ports, so either aggregation device might receive the source packet and manage flooding the packet to destination VLAN members.

Multicast ECID4096 is allocated to represent extended ports on satellite device 1 that are members of VLAN 100—EP1, EP2 and EP3, and multicast ECID4097 represents extended ports on satellite device 2 that are also members of VLAN 100—EP4 and EP5. Host 6 behind extended port EP6 is not a member of VLAN 100 and is not a destination for the flooded traffic. The aggregation device creates one copy of the packet tagged with ECID4096 and sends it to satellite device 1, and sends one copy tagged with ECID4097 to satellite device 2. Satellite device 1 replicates and forwards the packet for its own destination ports in VLAN 100, EP2 and EP3. (The ingress ECID split-horizon mechanism prevents forwarding traffic to the ingress port, EP1.) Satellite device 2 replicates and forwards the packet for EP4 and EP5, its local destination ports in VLAN 100. The extended port mapping for ECID4097 does not include EP6, so satellite device 2 does not forward the packet to that port.

When there are multiple cascade port links to a satellite device, the aggregation device load-balances the traffic when choosing which cascade port to use.

For destination VLAN members reachable through aggregation device ports (rather than extended ports), the aggregation device creates and sends copies to those local ports directly.

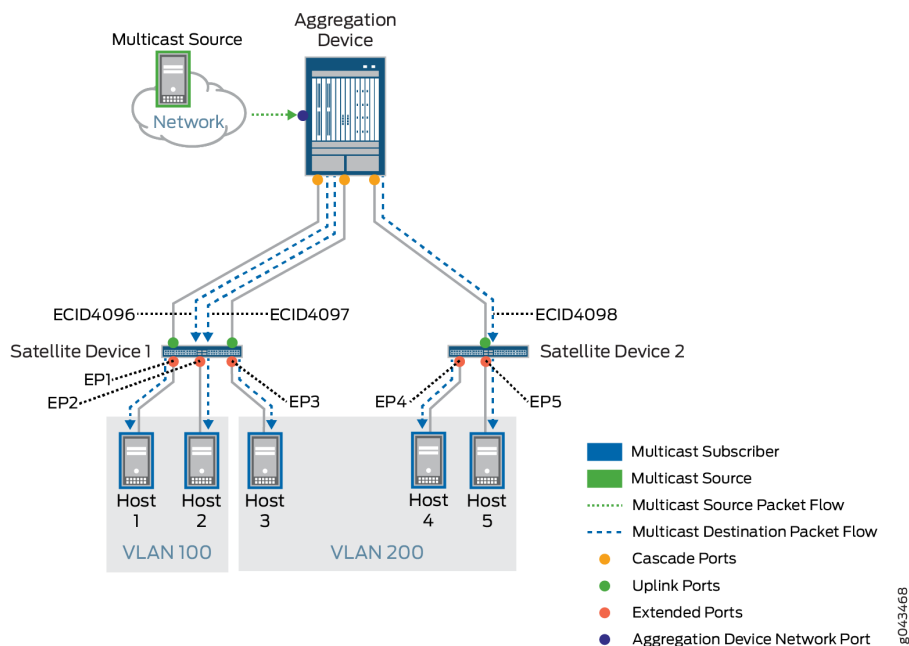
Local Replication for Layer 3 Multicast Traffic Over IRB Interfaces

Integrated Routing and Bridging (IRB) provides support for Layer 2 bridging and Layer 3 routing on the same interface, and IRB interfaces are used to route traffic between VLANs. Because satellite devices do not maintain Layer 3 routing information, local replication on the satellite devices only occurs for Layer 2 traffic, and the aggregation device manages the replication of multicast destination packets at Layer 3.

In Junos Fusion Enterprise or Junos Fusion Provider Edge architectures, the aggregation device forwarding the traffic replicates the multicast source packet for each IRB interface in the Layer 3 replication list for a multicast group, and performs a VLAN tag rewrite for each corresponding VLAN. When there are extended ports in multiple VLANs on a satellite device that are receivers in the same multicast group, the aggregation device sends copies to each IRB with its corresponding VLAN ID to that satellite device. If an IRB interface (VLAN membership) spans multiple satellite devices, the aggregation device creates and sends one copy to each satellite device that has multicast receivers that are members of that VLAN. Each satellite device then replicates and forwards copies of the received packet for its local multicast destination extended ports.

[Figure 15 on page 150](#) shows an example of Layer 3 multicast replication for VLANs over IRB interfaces in a Junos Fusion. In this case, two VLANs with corresponding IRB interfaces are configured on the aggregation device. In this case, multicast source packets ingress on an aggregation device port, and multicast subscribers are connected to extended ports EP1 through EP5, where extended ports EP1 and EP2 are in VLAN 100 and EP3 through EP5 are in VLAN 200.

Figure 15: Local Replication with Layer 3 Multicast



When the aggregation device receives a packet from the multicast source, it manages the Layer 3 replication by acquiring multicast ECIDs representing the destination extended ports in each VLAN on each satellite device, and creating, tagging, and forwarding copies on each VLAN's IRB interface to the satellite devices that have destination extended ports. As the figure shows, the aggregation device creates 3 copies of the source packet, as follows:

- Multicast ECID4096 represents EP1 and EP2 in VLAN 100 on satellite device 1. The aggregation device forwards one copy tagged with ECID4096 to satellite device 1 for the VLAN 100 IRB interface.
- Multicast ECID4097 represents EP3 in VLAN 200 on satellite device 1. The aggregation device forwards a second copy tagged with ECID4097 to satellite device 1 for the VLAN 200 IRB interface.
- Multicast ECID4098 represents EP4 and EP5 in VLAN 200 on satellite device 2. The aggregation device forwards a third copy tagged with ECID4098 for the VLAN 200 IRB interface to satellite device 2.

Each satellite device manages the Layer 2 processing by replicating the packets received from the aggregation device for the multicast subscribers behind its extended ports in each VLAN, as follows:

- Satellite device 1 replicates and forwards packets tagged with ECID4096 to extended ports EP1 and EP2, and forwards packets tagged with ECID4097 to EP3.
- Satellite device 2 replicates and forwards the packets tagged with ECID4096 to extended ports EP4 and EP5.

When there are multiple cascade port links to a satellite device, the aggregation device load-balances the traffic when choosing which cascade port to use.

For multicast destination VLAN members reachable through aggregation device ports (rather than extended ports), the aggregation device creates and sends copies to those local ports using the corresponding IRB interfaces.

RELATED DOCUMENTATION

[Understanding Multicast Replication in a Junos Fusion | 140](#)

[Ingress Replication at the Aggregation Device to Satellite Devices | 144](#)

[Configuring Egress \(Local\) Replication on a Junos Fusion | 151](#)

Configuring Egress (Local) Replication on a Junos Fusion

By default, egress replication (also called *local replication*) for multi-destination traffic is disabled, and Junos Fusion uses ingress replication on the access side. When you enable local replication, the feature is activated for all satellite devices that are connected to the aggregation device. You cannot enable local replication for just a few selected satellite devices, specific bridge domains, or specific route prefixes.

To enable local replication on the satellite devices, configure the `local-replication` statement at the `[edit forwarding-options satellite]` hierarchy level.

```
[edit forwarding-options satellite]
user@router1# set local-replication
```

The `show multicast summary satellite operational` command displays Egress replication: Enabled when this feature is configured.

See "[Understanding Multicast Replication in a Junos Fusion](#)" on page 140 for an overview of Junos Fusion multicast replication and the limitations to enabling this feature. Some Junos OS protocol and traffic management features are not supported with egress replication, and you should not plan to configure local replication if you want to use those features.

RELATED DOCUMENTATION

[Ingress Replication at the Aggregation Device to Satellite Devices | 144](#)

[Egress \(Local\) Replication on the Satellite Devices | 145](#)

Class of Service on Junos Fusion Provider Edge

IN THIS CHAPTER

- Understanding CoS on an MX Series Aggregation Device in Junos Fusion Provider Edge | 152
- Configuring CoS on an MX Series Aggregation Device in Junos Fusion | 160

Understanding CoS on an MX Series Aggregation Device in Junos Fusion Provider Edge

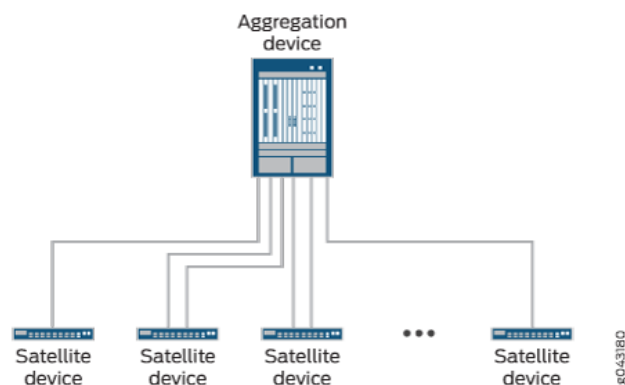
IN THIS SECTION

- Overview of CoS on Different Types of Ports in Junos Fusion | 153
- CoS on Extended Ports and Uplink Ports in Junos Fusion | 155
- Per-unit and Hierarchical Scheduling on Extended Ports | 156
- Broadband Subscriber Services Support | 157
- CoS Hierarchical Port Scheduling with Enhanced Transmission Selection in Junos Fusion | 158
- CoS on Cascade Ports in Junos Fusion | 158

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 16 on page 153](#) for an illustration of the Junos Fusion topology.

Figure 16: Junos Fusion Topology



An aggregation device can be an MX240, MX480, MX960, or MX2020 Universal Routing Platform running a supported Junos OS release.

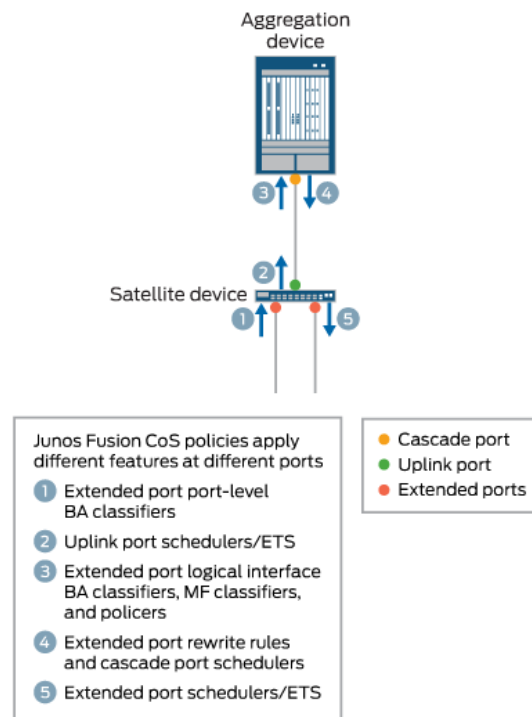
This topic describes class of service (CoS) on the different types of ports in Junos Fusion.

This topic covers:

Overview of CoS on Different Types of Ports in Junos Fusion

[Figure 17 on page 154](#) provides an overview of packet flow through Junos Fusion and how CoS features are applied at the different ports.

Figure 17: Junos Fusion CoS Feature Application



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 17 on page 154](#):

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, unless the rewrite rule is associated with an extended port logical interface. 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 MX Series aggregation device. Similarly, standard Junos OS CoS commands are issued on the MX Series aggregation device for retrieving extended port and uplink port CoS states and queue statistics. The MX Series 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
- Per-unit and hierarchical schedulers (extended ports only)
- Egress rewrite rules



NOTE: Configuring CoS policies on *satellite devices* (on both extended and uplink ports) has the following restrictions:

- Fixed classifiers are not supported.
- IP precedence classifiers are not supported. DSCP classifiers are supported, however.
- The `transmit-rate` option is supported for schedulers. However, the `remainder`, `rate-limit`, and `exact` options are not supported under `transmit-rate`.
- EX4300 Series devices used in a satellite role support up to two entries per segmented drop profile.

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: You cannot retrieve CoS statistics on extended ports through an SNMP query. To see CoS statistics on an extended port, use the `show interfaces queue interface-name extended-port-interface-name` and `show interfaces extended-port-interface-name extensive` commands.

Per-unit and Hierarchical Scheduling on Extended Ports

Junos Fusion Provider Edge supports per-unit and hierarchical schedulers on extended ports. To support per-unit or hierarchical scheduling on an extended port, all cascade ports on the aggregation device for that extended port must have a queueing chip.



NOTE: Multihomed satellite devices do not support per-unit and hierarchical scheduling.

To enable per-unit scheduling on an extended port, enable the `per-unit-scheduler` option at the `[edit interfaces interface-name]` hierarchy level for the extended port.

To enable hierarchical scheduling on an extended port, enable the `hierarchical-scheduler` option at the `[edit interfaces interface-name]` hierarchy level for the extended port.



NOTE: If you enable hierarchical scheduling on an extended port, you must also explicitly configure schedulers at the interface set or VLAN level.

Junos Fusion treats the cascade ports connecting the aggregation device to the satellite device as aggregated Ethernet ports with aggregation done automatically without configuration. By default the Junos Fusion implementation of hierarchical CoS applies the scheduler parameters across all cascade ports in scale mode. Because scale mode divides the configured shaper equally across the cascade ports, traffic drops can start before a customer reaches its committed rate for a particular flow. You can set all cascade ports on an aggregation device to be in replicate mode, thereby copying scheduler parameters to each level of the aggregated interface member links, and automatically target all of an extended port's traffic to a specific cascade port. To do this, simply enable `target-mode` for the satellite device at the `[edit chassis satellite-management fpc fpc-number]` hierarchy level. For example:

```
[edit]
user@host# show chassis satellite-management
fpc 100 {
    target-mode;
    cascade-ports [ xe-0/0/1:0 xe-1/0/0:1 xe-1/0/0:2 xe-1/0/1:1 ];
}
```



CAUTION: Enabling or disabling target-mode disrupts traffic on the satellite device while extended ports are deleted and re-added and cascade ports are reconfigured on the aggregate device.

Broadband Subscriber Services Support

Junos Fusion Provider Edge supports Broadband Edge Subscriber Management, including standard CoS functionality for Broadband Edge Subscriber Management.

BNG on Junos Fusion Provider Edge supports the following CoS scheduling hierarchies:

- Dynamic logical interface set/Static-VLAN-Demux/Extended port physical interface
- Dynamic logical interface/Extended port physical interface
- Dynamic logical interface set/Extended port physical interface
- Dynamic logical interface/Dynamic logical interface set/Extended port physical interface

To support 4 levels of hierarchical scheduling (for example, queue/dynamic logical interface/dynamic logical interface set/extended port physical interface), you need MPCs on the aggregation device that support at least 5 levels of hierarchical scheduling. This is because one level of scheduling is consumed by the cascade port. Every MPC on the aggregation device configured for Broadband Edge Subscriber Management must support at least 4 levels of hierarchical scheduling. Also, the `maximum-hierarchy-levels` option at the `[edit interfaces interface-name hierarchical-scheduler]` hierarchy for the extended port must be set to one less what the MPC for the associated cascade port supports because of the one level of scheduling the cascade port consumes.

Classifiers and rewrite rules are supported on subscriber logical interfaces.

Shaping calculations include the 801.BR overhead bytes.



NOTE: Multicast is supported through a separate VLAN on the extended port, but multicast is not supported using subscriber dynamic profiles and there is no CoS bandwidth adjustment support for the subscribers.

The `show class-of-service scheduler-hierarchy interface` command is supported and shows the cascade port as part of the hierarchy. For example:

```
user@host > show class-of-service scheduler-hierarchy interface demux0.3221225473
Interface/          Shaping    Guaranteed    Guaranteed/    Queue
Excess
```

| Resource name | rate | rate | Excess | | | |
|--------------------------|----------|----------|--------|-----|--|----|
| weight | weight | | | | | |
| | | kbits | kbits | | | |
| priority | high/low | | | | | |
| ge-100/0/0(xe-2/0/5) | 10000000 | | | | | |
| ge-100/0/0(xe-2/0/5) RTP | | 10000000 | | | | |
| demux0.3221225473 | 1000 | 0 | | | | |
| 500 500 | | | | | | |
| best-effort | 1000 | 0 | Low | Low | | 95 |
| network-control | 1000 | 0 | Low | Low | | 5 |

In the above sample output, ge-100/0/0 is the extended port and xe-2/0/5 is the cascade port.

CoS Hierarchical Port Scheduling with Enhanced Transmission Selection in Junos Fusion

In Junos Fusion, the satellite device can be either a QFX5100 or an EX4300 device. The QFX5100 supports enhanced transmission selection (ETS), which is described in IEEE 802.1Qaz. Configuration support for ETS has been added to the MX Series device only for satellite device ports that support this feature. If ETS is configured on the MX Series aggregation device for a satellite device port that does not support ETS, the satellite devices converts the ETS configuration to port scheduler.



NOTE: Local ports on the MX Series aggregation device do not support ETS.

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.



NOTE: If you are using a custom scheduler map, associate it with a traffic control profile that guarantees a minimum bandwidth of 90 percent. If the minimum guaranteed bandwidth is not configured, the in-band management logical interface will use buffer resources. This can lead to packet loss on the cascade port.

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 |
|---------|---|
| 18.4R1 | Starting in Junos OS Release 18.4R1, Junos Fusion Provider Edge supports Broadband Edge Subscriber Management, including standard CoS functionality for Broadband Edge Subscriber Management. |

RELATED DOCUMENTATION

- [Broadband Subscription Services on Junos Fusion | 48](#)
- [CoS for Subscriber Access Overview](#)
- [Understanding CoS Hierarchical Port Scheduling \(ETS\)](#)
- [CoS on Virtual Chassis Fabric \(VCF\) EX4300 Leaf Devices \(Mixed Mode\)](#)
- [Junos Fusion Provider Edge Overview | 2](#)
- [Understanding Junos Fusion Provider Edge Components | 4](#)
- [Configuring CoS on an MX Series Aggregation Device in Junos Fusion | 160](#)

Configuring CoS on an MX Series Aggregation Device in Junos Fusion

IN THIS SECTION

- [Configuring Behavior Aggregate Classifiers on Satellite Device Extended Ports | 160](#)
- [Configuring Rewrite Rules on Satellite Device Extended Ports | 162](#)
- [Configuring CoS Hierarchical Port Scheduling with Enhanced Transmission Selection on Satellite Device Ports | 163](#)
- [Changing the Default Scheduling Policy on an Aggregated Device Cascade Port | 166](#)

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 MX Series 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 device 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 MX Series 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@mx-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@mx-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@mx-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 | 14](#)

[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@mx-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@mx-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@mx-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 | 14](#)

[Rewriting Packet Headers to Ensure Forwarding Behavior](#)

Configuring CoS Hierarchical Port Scheduling with Enhanced Transmission Selection on Satellite Device Ports

You can configure enhanced transmission selection (ETS) for both extended ports and uplink ports on satellite devices. The configuration is done on the aggregation device. To configure ETS for a satellite device port in Junos Fusion:

1. Define the traffic control profiles.

```
[edit class-of-service]
user@mx-agg-device#set traffic-control-profiles be-tcp-1 scheduler-map be-map-1
user@mx-agg-device#set traffic-control-profiles be-tcp-1 shaping-rate percent 80
user@mx-agg-device#set traffic-control-profiles be-tcp-1 guaranteed-rate 4g
user@mx-agg-device#set traffic-control-profiles be-tcp-3 scheduler-map be-map-3
user@mx-agg-device#set traffic-control-profiles be-tcp-3 shaping-rate percent 80
user@mx-agg-device#set traffic-control-profiles be-tcp-3 guaranteed-rate 6g
```

2. Define the forwarding class sets.

```
[edit class-of-service]
user@mx-agg-device#set forwarding-class-sets FC-1 class best-effort-1
user@mx-agg-device#set forwarding-class-sets FC-1 class best-effort-2
user@mx-agg-device#set forwarding-class-sets FC-3 class best-effort-3
```

3. Apply the forwarding class sets to a satellite device port.

```
[edit class-of-service]
user@mx-agg-device#set interfaces xe-100/0/26 forwarding-class-set FC-1 output-traffic-
control-profile be-tcp-1
user@mx-agg-device#set interfaces xe-100/0/26 forwarding-class-set FC-3 output-traffic-
control-profile be-tcp-3
```

4. Commit the changes and then confirm the configuration.

```
[edit class-of-service]
user@mx-agg-device# show
traffic-control-profiles {
    be-tcp-1 {
        scheduler-map be-map-1;
        shaping-rate percent 80;
        guaranteed-rate 4g;
    }
    be-tcp-3 {
        scheduler-map be-map-3;
        shaping-rate percent 80;
        guaranteed-rate 6g;
    }
}
forwarding-class-sets {
    FC-1 {
        class best-effort-1;
        class best-effort-2;
    }
    FC-3 {
        class best-effort-3;
    }
}
interfaces {
    xe-100/0/26 {
        forwarding-class-set {
            FC-1 {
                output-traffic-control-profile be-tcp-1;
            }
            FC-3 {
                output-traffic-control-profile be-tcp-3;
            }
        }
    }
}
```

```

    }
}

```

5. Run `show interfaces queue egress interface name` to show the statistics of transmitted and dropped packets for each queue on the satellite device port.

```

user@mx-agg-device> show interfaces queue egress xe-100/0/26:0
Physical interface: xe-100/0/26:0 (Extended Port, Enabled, Physical link is Up)
  Interface index: 3040, SNMP ifIndex: 1085
Forwarding classes: 16 supported, 4 in use
Egress queues: 8 supported, 4 in use
Queue: 0, Forwarding classes: best-effort-1
  Queued:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
  Transmitted:
    Packets      :            7182746            24998 pps
    Bytes        :        4195267965        116853536 bps
    Tail-dropped packets :                0                0 pps
    RL-dropped packets  :                0                0 pps
    RL-dropped bytes    :                0                0 bps
    RED-dropped packets :                0                0 pps
    RED-dropped bytes   :                0                0 bps
Queue: 1, Forwarding classes: best-effort-2
  Queued:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
  Transmitted:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
    Tail-dropped packets :                0                0 pps
    RL-dropped packets  :                0                0 pps
    RL-dropped bytes    :                0                0 bps
    RED-dropped packets :                0                0 pps
    RED-dropped bytes   :                0                0 bps
Queue: 2, Forwarding classes: best-effort-3
  Queued:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
  Transmitted:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps

```

```

Tail-dropped packets :          0          0 pps
RL-dropped packets   :          0          0 pps
RL-dropped bytes     :          0          0 bps
RED-dropped packets  :          0          0 pps
RED-dropped bytes    :          0          0 bps
Queue: 3, Forwarding classes: network-control
  Queued:
    Packets           :          0          0 pps
    Bytes             :          0          0 bps
  Transmitted:
    Packets           :          14505        1 pps
    Bytes             :        11746583      1448 bps
    Tail-dropped packets :          0          0 pps
    RL-dropped packets  :          0          0 pps
    RL-dropped bytes    :          0          0 bps
    RED-dropped packets :          0          0 pps
    RED-dropped bytes   :          0          0 bps

```



NOTE: Queued statistics for each queue are not available for satellite device ports and will always show 0.

SEE ALSO

[Understanding CoS Hierarchical Port Scheduling \(ETS\)](#)

[CoS on Virtual Chassis Fabric \(VCF\) EX4300 Leaf Devices \(Mixed Mode\)](#)

[Example: Configuring CoS Hierarchical Port Scheduling \(ETS\)](#)

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@mx-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@mx-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@mx-agg-device# run show class-of-service scheduler-hierarchy interface xe-0/0/1
Interface/      Shaping Guaranteed  Guaranteed/  Queue  Excess
Resource name    rate    rate    Excess  weight  weight
                  kbits    kbits    priority
xe-0/0/1.32770   10000000  0
  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@mx-agg-device#set schedulers AF_SCH_CORE transmit-rate percent 40
user@mx-agg-device#set schedulers AF_SCH_CORE buffer-size percent 40
user@mx-agg-device#set schedulers AF_SCH_CORE priority medium-high
user@mx-agg-device#set schedulers BE_SCH_CORE transmit-rate percent 10
user@mx-agg-device#set schedulers BE_SCH_CORE buffer-size percent 10
user@mx-agg-device#set schedulers BE_SCH_CORE priority low
user@mx-agg-device#set schedulers EF_SCH_CORE transmit-rate percent 40
user@mx-agg-device#set schedulers EF_SCH_CORE buffer-size percent 40
user@mx-agg-device#set schedulers EF_SCH_CORE priority medium-low
user@mx-agg-device#set schedulers NC_SCH_CORE transmit-rate percent 10
user@mx-agg-device#set schedulers NC_SCH_CORE buffer-size percent 10
user@mx-agg-device#set schedulers NC_SCH_CORE priority high
```

2. Create a scheduler map.

```
[edit class-of-service]
user@mx-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class BE scheduler BE_SCH_CORE
user@mx-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class EF scheduler EF_SCH_CORE
user@mx-agg-device#set scheduler-maps CORE_SCHED_MAP forwarding-class AF scheduler AF_SCH_CORE
user@mx-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@mx-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@mx-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@mx-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@mx-agg-device# run show class-of-service scheduler-hierarchy interface xe-0/0/1 | | | | | | |
| Interface/ | Shaping | Guaranteed | 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 on an MX Series Aggregation Device in Junos Fusion Provider Edge | 152](#)

2

PART

Configuration Statements and Operational Commands

- [Junos CLI Reference Overview | 172](#)
-

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Read this guide to learn about the syntax and options that make up the statements and commands. Also 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](#)