Solution Guide

Enterprise Data Center: Junos Fusion Data Center Architecture
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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Enterprise Data Center</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>About This Solution Guide</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Understanding the Enterprise Data Center Solution</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Data Center Networking Architectures</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Enterprise Data Center Networking Overview</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Junos Fusion Data Center</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Enterprise Data Center Network Requirements</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Automation and Orchestration Tools</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Analytics</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Network Traffic Segmentation</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Class of Service</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Example: Configuring the Enterprise Data Center Solution</td>
<td>11</td>
</tr>
<tr>
<td>Appendix</td>
<td>Appendix: Enterprise Data Center Solution Complete Configuration</td>
<td>87</td>
</tr>
<tr>
<td></td>
<td>MX480 Router (mx480-core-router):</td>
<td>87</td>
</tr>
<tr>
<td></td>
<td>Aggregation Device 1 (ad1-qfx10002):</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>Aggregation Device 2 (ad2-qfx10002):</td>
<td>99</td>
</tr>
</tbody>
</table>
CHAPTER 1

Enterprise Data Center

- About This Solution Guide on page 5
- Understanding the Enterprise Data Center Solution on page 5
- Example: Configuring the Enterprise Data Center Solution on page 11
- Appendix: Enterprise Data Center Solution Complete Configuration on page 87

About This Solution Guide

The Enterprise Data Center solution provides a state of the art Ethernet fabric data center architecture built using Junos Fusion Data Center technology. This Ethernet fabric architecture is intended for installation in privately-owned Enterprise Data Center networks that are seeking a simplified architecture that can support the rapidly-evolving networking requirements of the modern data center.

The intent of this solution guide is to provide an overview of the Enterprise Data Center solution, and to provide a detailed step-by-step reference architecture that explains design considerations while also illustrating how the architecture was implemented by the Juniper Networks solutions team. We know that every private Enterprise data center has its own requirements; our hope is that you can apply the information in this guide to make better network design decisions and to implement the features in a manner that best meets the requirements of your Enterprise data center network.

The intended audience for this guide is system integrators, infrastructure vendors, and any Enterprise networking customers that are currently using or considering upgrading to a modern Ethernet fabric data center architecture.

Understanding the Enterprise Data Center Solution

- Data Center Networking Architectures on page 6
- Enterprise Data Center Networking Overview on page 6
- Junos Fusion Data Center on page 7
- Enterprise Data Center Network Requirements on page 8
- Implementation on page 10
Data Center Networking Architectures

Data Center network architectures have evolved rapidly in recent years, from hierarchical architectures running spanning tree protocol (STP) to spine and leaf topologies utilizing Multichassis link aggregation (MC-LAG) to modern data center fabric architectures.

Fabrics are the preferred architecture for modern data center networks, for the following reasons:

- **Topology**—Fabrics leverage the non-blocking Clos designs already used extensively in wide area networks to create flatter, faster, and simpler data center network topologies.

- **Control Plane**—Fabrics use a control plane that is logically separate from the rest of the network to distribute addressing information and suppress loops, thereby avoiding broadcast and other network traffic that can overwhelm a layer 2 network. The separate control plane simplifies network operation and maximizes bandwidth utilization.

- **Central point of management**—The better designed fabric networks are managed as a single coherent system that automates and abstracts the provisioning and management of all devices in the data center network. Networking devices are managed individually in traditional data center networks, which significantly increases network management overhead and costs.

The two primary types of data center fabrics are Ethernet fabrics and IP fabrics. Ethernet fabrics provide typical layer 2 and layer 3 service to applications while also providing support services such as multicast and lossless data center bridging. IP fabrics provide Layer 3 service and must use overlay technologies to provide Layer 2 services over the network. Ethernet fabrics are typically simpler to install and operate. IP fabrics are typically more open and scalable than Ethernet fabrics.

The Enterprise Data Center solution documented in this guide provides a state of the art Ethernet fabric data center architecture built using Junos Fusion Data Center technology. This Enterprise Data Center solution is intended for installation in privately-owned data center networks.

Enterprise Data Center Networking Overview

Enterprise data center networks—private data center networks that are owned and operated by an Enterprise—need to move to network topologies that leverage the agility, efficiency, and simplicity provided by recent technical innovations in data center networking to best support their business requirements.

Legacy Enterprise data center networks are often hindered by a siloed approach to data center applications that evolved due to limitations with older underlying networking infrastructures. The application silos are often tightly coupled to the networking infrastructure, and the approach often leads to a topology that inefficiently provides applications over the network. A heavily-siloed data center often contains a proliferation of devices that are expensive to purchase, difficult to maintain, and difficult or impossible to upgrade due to the structured nature of the silos.
The Juniper Networks Enterprise Data Center Solution provides an agile, flexible, easy-to-manage topology that allows you to leverage modern data center networking technologies for a private Enterprise data center network.

The advantages of the Enterprise Data Center Solution include:

- **Agility**—the Enterprise Data Center Solution is a topology that has the agility to support any device using any application anywhere within the Enterprise data center network. This agility extends to data center application support in environments where an application must be made available over a private and a public data center network, since many businesses simultaneously support their own private Enterprise data center network for some functions while using a public data center network provided by a service provider for other functions.

- **Adaptability**—modern Enterprise data center networking equipment is often reconfigured by network operators to support the constantly evolving needs of the business. The Enterprise Data Center Solution topology has the flexibility to adapt to network changes and evolutions quickly.

- **Management**—the Enterprise Data Center Solution topology is built using Junos Fusion Data Center, a technology that simplifies management for a network operator by allowing over 3,000 user-facing interfaces on 64 switches to be managed from a single device running Junos OS. The simplified management provided by Junos Fusion Data Center reduces overall cost of ownership.

### Junos Fusion Data Center

The Enterprise Data Center solution is built on a Junos Fusion Data Center topology.

Junos Fusion Data Center brings Juniper Networks Junos Fusion technology to the data center. A Junos Fusion Data Center simplifies network management by allowing one or two aggregation devices running Junos OS to act as the management point or points for a topology that can include up to sixty-four satellite devices.

In the Junos Fusion Data Center topology, satellite devices provide access interfaces for endpoint devices, much like leaf devices in a traditional spine and leaf architecture. Aggregation devices, meanwhile, transfer traffic between access switches, move traffic from access switches to the Layer 3 gateway, and move traffic received from the Layer 3 gateway toward the access switches. Aggregation devices, therefore, perform many functions that are performed by spine devices in a traditional spine and leaf architecture.

Figure 1 on page 8 illustrates the Junos Fusion Data Center topology used in the Enterprise Data Center solution.
In the Enterprise Data Center Solution topology, two QFX10002 switches act as aggregation devices and sixty-four total EX4300 and QFX5100 switches act as satellite devices, providing a networking topology that provides over three thousand networking-facing interfaces managed entirely from the aggregation devices.

For additional information on Junos Fusion Data Center, see Junos Fusion Data Center Feature Guide.

Enterprise Data Center Network Requirements

The requirements for an Enterprise data center network are vast and have evolved substantially in recent years.

This section reviews common Enterprise data center network requirements, and how the Enterprise Data Center Solution addresses these requirements.

Automation and Orchestration Tools

Automation technology is technology that uses software to perform tasks that would otherwise be performed manually. Automation technology often reduces the amount of work required to configure or troubleshoot a network, for instance, although automation technology refers broadly to any tool that automates a previously manual task.

Orchestration technology takes automation to another level by utilizing automation technology to provide services in the network.

The Enterprise Data Center solution provides a powerful topology that supports a broad range of automation and orchestration tools. Juniper Networks products such as Junos Space Management and Contrail Networking can be implemented in the Enterprise Data Center solution to provide automation and orchestration. Other Juniper tools that allow Enterprise data centers to build and run applications—such as the Juniper Extension Toolkit (JET) and Junos PyEZ—are also available to enhance the Enterprise Data Center solution.

The solution’s open platform also allows the network to leverage third-party automation and orchestration tools to enhance network performance and capabilities. Third party automation frameworks such as Chef, Puppet, Ansible, and NETCONF are supported by the solution. The solution also provides options for programmable network platforms, OpenConfig support, and vendor-independent orchestration with software defined networking (SDN) and Network Functions Virtualization (NFV).
Analytics

Network analytics provide visibility into the performance and behavior of the data center infrastructure. Network analytics tools collect data from the device, analyze the data using sophisticated algorithms, and capture the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

The Enterprise Data Center solution supports a range of analytical tools available for Juniper Networks data center products, including support for obtaining fine-grained network analytics data in various formats that include Google Protocol Buffer (GBP), Javascript Object Notation (JSON), Comma-separated Values (CSV), or Tab-separated Values (TSV).

See Network Analytics Overview for additional information on data center network analytics collection.

Network Traffic Segmentation

Network traffic segmentation—the ability to isolate traffic on different paths—is required in most data center networks for a variety of reasons, including isolation of tenant traffic in a shared data center or isolation of traffic that has different handling requirements in a shared or non-shared private data center. Network traffic segmentation is provided in the Enterprise Data Center solution topology through the use of virtual LANs (VLANs), integrated routing and bridging (IRB) interfaces, and virtual routing and forwarding (VRF) instances.

VLANs are used in the Enterprise Data Center solution to segment traffic at Layer 2 and VRF instances are used to segment traffic at Layer 3. IRB interfaces are used on the aggregation devices to forward traffic between different VLANs in the data center topology.

Management

The Enterprise Data Center solution provides a centralized, easy-to-manage topology using Junos Fusion Data Center.

A Junos Fusion Data Center can manage over 3,000 access interfaces from the aggregation devices running Junos OS, allowing an Enterprise to manage a medium-sized data center from as little as two management IP addresses. This central point of management avoids the overhead of managing each device in the topology individually, which is a common requirement in traditional data center networks.

Class of Service

Junos OS class of service (CoS) enables you to divide traffic into classes and set various levels of throughput and packet loss when congestion occurs. CoS provides greater control over packet loss because you can configure rules tailored to the needs of your network.

The Enterprise Data Center solution supports a wide range of CoS options for traffic in your data center network.
For additional information on CoS in a Junos Fusion Data Center, see Understanding CoS in Junos Fusion Data Center.

Implementation

The following hardware equipment and software features were used to create the Enterprise Data Center Solution provided in this document.

Core Layer

Router:

- 1 MX480 3D Universal Edge Router
- Two 6x40GE + 24x10GEMPC5EQ MPCs

NOTE: Other devices can be used at the core layer in this topology.

The device to use in the core layer depends largely on the bandwidth requirements and feature support for each individual data center. See MX960, MX480, MX240, MX104 and MX80 3D Universal Edge Routers Data Sheet or QFX10000 Modular Ethernet Switches Data Sheet for information on other devices that are commonly deployed at the core layer in Enterprise data center networks.

Junos Fusion Data Center Switching Topology

Aggregation Devices:

- 2 QFX10002-72Q switches

NOTE: A QFX10002-72Q switch has 72 40-Gbps QSFP+ interfaces.

An Enterprise Data Center network that requires fewer 40-Gbps QSFP+ interfaces could configure this reference architecture using two QFX10002-36Q switches, which support up to 36 40-Gbps QSFP+ interfaces, in place of the QFX10002-72Q switches. The QFX10002-36Q switches can also be deployed in environments that support a large number of 10-Gbps SFP+ interfaces, since one 40-Gbps interface on a QFX10002 switch can be converted into four 10-Gbps SFP+ interfaces using a breakout cable.

Satellite Devices:

- 24 EX4300 switches
- 40 QFX5100 switches
NOTE: A Junos Fusion Data Center support up to 64 satellite devices. The satellite devices can be any mix of EX4300 and QFX5100 switches. For a list of supported satellite devices in a Junos Fusion Data Center, see Understanding Junos Fusion Data Center Software and Hardware Requirements.

Now that we have completed our overview of the Enterprise Data Center solution, it is time to view the configuration and verification sections of the solution.

Related Documentation

- Example: Configuring the Enterprise Data Center Solution on page 11

### Example: Configuring the Enterprise Data Center Solution

This example describes how to build the Enterprise Data Center solution.

This example is intended as a reference architecture that has been validated by Juniper Networks. The example contains one method of configuring each feature, with explanatory text and pointers to additional information sources to provide greater detail when your Enterprise data center network has different requirements than the reference architecture provided in this example.

**Requirements**

Table 1 on page 11 lists the hardware and software components used in this example.

### Table 1: Solution Hardware and Software Requirements

<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Router</td>
<td>MX480 routers*</td>
<td>Junos OS Release 13.2R1 or later</td>
</tr>
<tr>
<td>Aggregation devices</td>
<td>QFX10002-72Q switches**</td>
<td>Junos OS Release 17.2R1 or later</td>
</tr>
<tr>
<td>Satellite devices</td>
<td>QFX5100 switches***</td>
<td>Satellite software version 3.0R1</td>
</tr>
<tr>
<td></td>
<td>EX4300 switches***</td>
<td>Satellite devices must be running Junos OS Release 14.1X53-D43 or later before conversion into a satellite device.</td>
</tr>
</tbody>
</table>

* An MX480 router is used in this solution because of its ability to scale in an Enterprise data center. The device to use in the core layer depends largely on the bandwidth requirements and feature support needs of each individual data center. See [MX960, MX480, MX240, MX104 and MX80 3D Universal Edge Routers Data Sheet](https://www.juniper.net) or [QFX10000 Modular Ethernet Switches Data Sheet](https://www.juniper.net) for information on other devices that are commonly deployed at the core layer in Enterprise data center networks.

** QFX10002-72Q switches are needed to implement the solution in this reference architecture because the switch has 72 40-Gbps QSFP+ interfaces and can therefore support the large number of 40-Gbps QSFP+ interfaces utilized in this topology.
QFX10002-36Q switches have 36 40-Gbps QSFP+ interfaces and can be used as aggregation devices to implement this solution in smaller environments that require fewer satellite devices or network-facing interfaces, or in environments that conserve 40-Gbps QSFP+ interfaces by using breakout cables to create multiple 10-Gbps SFP+ cascade port interfaces.

*** All EX4300 and QFX5100 switches that can be converted into satellite devices for a Junos Fusion Data Center when the aggregation device is running Junos OS Release 17.2R1 or later can be used as satellite devices in this topology. The following switches can be converted into satellite devices: QFX5100-24Q-2P, QFX5100-4BS-6Q, QFX5100-48T-6Q, QFX5100-96S-8Q, EX4300-24T, EX4300-32F, EX4300-48T, and EX4300-48T-BF. Any combination of these switches can be used as satellite devices, with the requirement that Junos Fusion Data Center supports up to 64 total satellite devices.

See Understanding Junos Fusion Data Center Software and Hardware Requirements for information on supported satellite devices in a Junos Fusion Data Center.

Overview and Topology

The topology used in this example consists of one MX480 3D Universal Edge Router, two QFX10002-72Q switches acting as aggregation devices, and sixty-four QFX5100 and EX4300 switches acting as satellite devices. The topology is shown in Figure 2 on page 12.

Figure 2: Enterprise Data Center Solution Topology

Core Layer: MX480 Universal Edge 3D Router Interfaces Summary

The MX480 Universal Edge 3D Router connects to each QFX10002-72Q switch using an aggregated Ethernet interface—a100 to connect to aggregation device 1 and ae101 to connect to aggregation device 2—that contains six 40-Gbps QSFP member interfaces.

Table 2 on page 13 summarizes the aggregated Ethernet interfaces on the MX480 router.
### Table 2: MX480 Router Interfaces Summary

<table>
<thead>
<tr>
<th>Aggregated Ethernet Interface</th>
<th>Member Interfaces</th>
<th>IP Address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae100</td>
<td>et-3/2/0, et-3/2/1, et-3/2/2, et-4/2/0, et-4/2/1, et-4/2/2</td>
<td>10.0.1.1/24</td>
<td>Connects the MX480 router to the QFX10002-72Q switch acting as aggregation device 1.</td>
</tr>
</tbody>
</table>

### Aggregation Layer: QFX10002-72Q Switches Interfaces Summary

A QFX10002-72Q switch has seventy-two 40-Gbps interfaces. A 40-Gbps interface on a QFX10002-72Q switch can be converted into four 10-Gbps interfaces using a breakout cable.

Both QFX10002-72Q switches in the Enterprise Data Center solution are cabled identically, with the first sixty-four 40-Gbps interfaces—et-0/0/0 through et-0/0/63—connected as cascade ports to the EX4300 and QFX5100 switches acting as satellite devices. Cascade ports are ports on aggregation devices that connect to satellite devices in a Junos Fusion topology.

The next two 40-Gbps interfaces on the front panel of the QFX10002-72Q switches—et-0/0/64 and et-0/0/65—are configured into an aggregated Ethernet interface that functions as the ICL between aggregation devices. A Junos Fusion Data Center with dual aggregation devices is built using an MC-LAG topology, and therefore must have an interchassis link (ICL) to pass data traffic between peers while also supporting the Inter-Chassis Control Protocol (ICCP) to send and receive control traffic. The ICL carries data traffic between aggregation devices in this topology, ICCP control traffic, which is used to send control information between devices in an MC-LAG topology, has its own link in some MC-LAG topologies but is sent over the ICL in the Enterprise Data Center topology, thereby preserving a 40-Gbps interface for other networking purposes.

The remaining interfaces on each aggregation device—et-0/0/66, et-0/0/67, et-0/0/68, et-0/0/69, et-0/0/70, and et-0/0/71—are aggregated into a single aggregated Ethernet interface and are used as uplink interfaces to connect the QFX10002-72Q switches to the MX480 router at the core layer.

*Figure 3 on page 14 summarizes the role of each interface on the QFX10002-72Q switches in this solution topology.*
Table 3 on page 14 summarizes the purpose of each interface on the QFX10002-72Q switch in this solution topology.

Table 3: QFX10002-72Q Switches Interfaces Summary

<table>
<thead>
<tr>
<th>Interface Numbers</th>
<th>Interface Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>et-0/0/0 through</td>
<td>Cascade port</td>
<td>Connects the QFX10002-72Q aggregation device switches to QFX5100 or EX4300 satellite device switches.</td>
</tr>
<tr>
<td>et-0/0/63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>et-0/0/64 and et-0/0/65</td>
<td>Interchassis link (ICL)</td>
<td>Connects the QFX10002-72Q aggregation device switches together and passes data traffic between them.</td>
</tr>
<tr>
<td>ae999</td>
<td></td>
<td>et-0/0/64 and et-0/0/65 are the member interfaces in aggregated Ethernet interface ae999.</td>
</tr>
<tr>
<td>et-0/0/66 through</td>
<td>Network port</td>
<td>Connects the QFX10002-72Q aggregation device switches to the MX480 router</td>
</tr>
<tr>
<td>et-0/0/71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae100</td>
<td></td>
<td>et-0/0/66, et-0/0/67, et-0/0/68, et-0/0/69, et-0/0/70, and et-0/0/71 are the member interfaces in aggregated Ethernet interface ae100.</td>
</tr>
</tbody>
</table>

Access Layer: FPC ID Numbering and Cascade Port Summary

The access layer in this topology is the QFX5100 and EX4300 switches configured into satellite devices. The access layer devices are responsible for providing the access interfaces that connect endpoint devices to the network.

Each satellite device in a Junos Fusion Data Center is assigned an FPC ID number. FPC ID numbers are used to identify satellite devices within a Junos Fusion.

A cascade port in a Junos Fusion is a port on the aggregation device—in the Enterprise Data Center solution, the aggregation devices are the QFX10002-72Q switches—that connects to a satellite device. Cascade ports forward and receive traffic to and from the satellite devices.

See the “Assigning Cascade Ports to FPC ID Numbers and Creating Satellite Device Aliases” on page 30 section for additional information on FPC ID numbers and cascade ports.
Table 4 on page 15 provides a summary of each satellite device’s hardware model, FPC ID number, alias name, and associated cascade port.

**Table 4: Satellite Device and Cascade Port Summary**

<table>
<thead>
<tr>
<th>FPC ID Number</th>
<th>Hardware Model</th>
<th>Alias Names</th>
<th>Cascade Port Interface (on QFX10002-72Q Switch Aggregation Devices)****</th>
</tr>
</thead>
<tbody>
<tr>
<td>100-139</td>
<td>QFX5100</td>
<td>qfx5100-sd100 through qfx5100-sd139</td>
<td>et-0/0/0 through et-0/0/39 One 40-Gbps cascade port interface is connected to each QFX5100 switch operating as a satellite device.</td>
</tr>
<tr>
<td>140-156</td>
<td>EX4300</td>
<td>ex4300-sd140 through ex4300-sd156</td>
<td>et-0/0/40 through et-0/0/56 One 40-Gbps cascade port interface is connected to each EX4300 switch operating as a satellite device.</td>
</tr>
<tr>
<td>157-160</td>
<td>EX4300</td>
<td>ex4300-sd157 through ex4300-sd160</td>
<td>et-0/0/57:0 through et-0/0/57:3 et-0/0/57 is converted from one 40-Gbps interface into four 10-Gbps channelized interfaces using a breakout cable. One 10-Gbps cascade port interface is connected to each EX4300 switch operating as a satellite device.</td>
</tr>
<tr>
<td>161-163</td>
<td>EX4300</td>
<td>ex4300-sd161 through ex4300-sd163</td>
<td>et-0/0/58 through et-0/0/63 Two 40-Gbps cascade port interfaces are connected to each EX4300 switch operating as a satellite device.</td>
</tr>
</tbody>
</table>

**** The two QFX10002-72Q switches in this topology have identical cascade port interface configurations. The port numbers are, therefore, applied identically on each QFX10002-72Q switch.

**Access Devices: Link Aggregation Groups Overview**

The access ports on the satellite devices in the Enterprise Data Center solution topology can be used to connect any endpoint devices to the data center. Access ports on satellite devices in a Junos Fusion are also called extended ports.

Endpoint devices can be single-homed to a single extended port or multi-homed to multiple extended ports.

To maximize fault tolerance and increase high availability, it is often advisable to multi-home an endpoint device to two or more extended ports on different satellite devices to ensure traffic flow continues when a single satellite device fails. The multi-homed links can be configured into an aggregated Ethernet interface to better manage traffic flows and simplify network manageability.

Figure 4 on page 16 illustrates six servers using multi-homed links to extended ports on different satellite devices in this topology. Each server is multi-homed to two satellite devices using member links that are part of the same aggregated Ethernet interface.
Figure 4: Aggregated Ethernet Interfaces

Table 5: Aggregated Ethernet Access Interface Summary

<table>
<thead>
<tr>
<th>Aggregated Ethernet Interface Name</th>
<th>Member Interfaces</th>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae1</td>
<td>ge-101/0/22</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>ge-102/0/22</td>
<td></td>
</tr>
<tr>
<td>ae2</td>
<td>ge-101/0/23</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>ge-102/0/23</td>
<td></td>
</tr>
<tr>
<td>ae3</td>
<td>ge-101/0/24</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>ge-102/0/24</td>
<td></td>
</tr>
<tr>
<td>ae4</td>
<td>ge-103/0/22</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>ge-104/0/22</td>
<td></td>
</tr>
<tr>
<td>ae5</td>
<td>ge-103/0/23</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>ge-104/0/23</td>
<td></td>
</tr>
<tr>
<td>ae6</td>
<td>ge-103/0/24</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>ge-104/0/24</td>
<td></td>
</tr>
</tbody>
</table>

A typical data center deployment often utilizes numerous aggregated Ethernet interfaces to connect endpoint devices to the network. The topology in this solutions guide minimizes the total number of aggregated Ethernet interfaces in the topology to six to better focus the configuration procedure.

See the "Enabling an Aggregated Ethernet Interface For Access Interfaces" on page 53 section of this Solutions Guide to configure aggregated Ethernet interfaces for endpoint devices in this topology.

**IP Addressing Summary**

Table 6 on page 17 summarizes the IP addresses used in this topology.
### Table 6: IP Addressing Summary

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MX480 Core Router</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae100</td>
<td>10.0.1.1/24</td>
<td>Aggregated Ethernet interface to AD1</td>
</tr>
<tr>
<td>ae101</td>
<td>10.0.2.1/24</td>
<td>Aggregated Ethernet interface to AD2</td>
</tr>
<tr>
<td>lo0.10</td>
<td>192.168.100.5</td>
<td>Loopback interface used in OSPF and PIM configuration</td>
</tr>
<tr>
<td><strong>QFX10002-72Q Switch (Aggregation Device 1)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae100</td>
<td>10.0.1.100/24</td>
<td>Aggregated Ethernet interface to R1</td>
</tr>
<tr>
<td>em1</td>
<td>192.168.255.40</td>
<td>Management port also used to ping between aggregation devices.</td>
</tr>
<tr>
<td>irb.100</td>
<td>10.1.1/24</td>
<td>IRB interface associated with VLAN 100</td>
</tr>
<tr>
<td>irb.200</td>
<td>10.2.2/1/24</td>
<td>IRB interface associated with VLAN 200</td>
</tr>
<tr>
<td>ae999.32769</td>
<td>10.0.0.1/30</td>
<td>IP address created by automatic ICCP provisioning and used by ICCP and BFD over the ICL.</td>
</tr>
<tr>
<td>lo0.10</td>
<td>192.168.100.1</td>
<td>Loopback interface used in OSPF and PIM configuration</td>
</tr>
<tr>
<td><strong>QFX10002-72Q Switch (Aggregation Device 2)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae100</td>
<td>10.0.2.100/24</td>
<td>Aggregated Ethernet interface to R1</td>
</tr>
<tr>
<td>em1</td>
<td>192.168.255.41</td>
<td>Management port also used to ping between aggregation devices.</td>
</tr>
<tr>
<td>irb.100</td>
<td>10.1.1/24</td>
<td>IRB interface associated with VLAN 100</td>
</tr>
<tr>
<td>irb.200</td>
<td>10.2.2/1/24</td>
<td>IRB interface associated with VLAN 200</td>
</tr>
<tr>
<td>ae999.32769</td>
<td>10.0.0.2/30</td>
<td>IP address created by automatic ICCP provisioning and used by ICCP and BFD over the ICL.</td>
</tr>
<tr>
<td>lo0.10</td>
<td>192.168.100.2</td>
<td>Loopback interface used in OSPF and PIM configuration</td>
</tr>
</tbody>
</table>

### Virtual Routing Instances Summary

The Enterprise Data Center solution topology uses virtual routing instances to enable EGBP, OSPF, DHCP Relay, and PIM. Virtual routing instances allow the devices in a topology to support multiple routing tables on each device in a topology. The separate routing tables allow the topology to completely isolate traffic into separate “virtual” networks with their own routing tables, protocols, and other requirements. This traffic
isolation can serve many purposes in a data center network, including isolation between customer networks in a multi-tenant data center or isolation between traffic handling when different users or traffic needs to be isolated in a non-shared Enterprise data center network.

Multiple routing instances are configured in this topology to separate EBGP and OSPF configurations. EBGP and OSPF configurations are not typically configured simultaneously in an Enterprise Data Center topology due to the overhead of maintaining two routing protocols in a data center, although the configuration is possible. The two virtual routing instances are enabled on the same interfaces—a100 and a101 on the MX480 router and a100 on both QFX10002-72Q switches—in this topology. A single device interface, however, can only support one virtual routing instance per interface so you could not implement both routing instances in your network. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGP, DHCP Relay, and PIM-SM that is appropriate for your network.

Table 7 on page 18 summarizes the virtual routing instances in the Enterprise Data Center solution topology.

NOTE: Table 7 on page 18 is provided to show which features are included in the virtual routing instances in this reference architecture only. You can configure OSPF, EBGP, DHCP Relay, and PIM-SM in any routing instance that requires the functionality. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGP, DHCP Relay, and PIM-SM that is appropriate for your network.

Table 7: Virtual Routing Instances Summary

<table>
<thead>
<tr>
<th>Virtual Routing Instance Name</th>
<th>Participating Devices</th>
<th>OSPF</th>
<th>EBGP</th>
<th>DHCP Relay</th>
<th>PIM Sparse Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>vr-10</td>
<td>MX480</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>QFX10002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AD1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QFX10002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AD2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vr-20</td>
<td>MX480</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>QFX10002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AD1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QFX10002</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AD2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuration

This section provides the configuration steps needed to implement this solution.
It contains the following sections:

- Configuring Commit Synchronization Between Aggregation Devices on page 20
- Configuring the Aggregated Ethernet Interfaces Connecting the MX480 Router to the QFX10002-72Q Switches on page 24
- Assigning Cascade Ports to FPC ID Numbers and Creating Satellite Device Aliases on page 30
- Converting Interfaces into Cascade Ports on page 34
- Configuring the Aggregated Ethernet Interfaces for the Interchassis Link (ICL) on page 36
- Configuring Dual Aggregation Device Support on page 38
- Configuring Bidirectional Forwarding Detection (BFD) over the ICL on page 40
- Enabling Automatic Satellite Device Conversion on page 42
- Installing and Managing the Satellite Software on page 43
- Preparing the Satellite Devices on page 45
- Verifying that the Junos Fusion Data Center is Operational on page 47
- Configuring Uplink Port Pinning on page 48
- Enabling Uplink Failure Detection on page 51
- Enabling an Aggregated Ethernet Interface For Access Interfaces on page 53
- Configuring IRB Interfaces and VLANs on page 59
- Configuring OSPF on page 63
- Configuring BGP on page 67
- Configuring Class of Service on page 71
- Configuring DHCP Relay on page 74
- Configuring Layer 3 Multicast on page 77
- Configuring IGMP Snooping to Manage Multicast Flooding on VLANs on page 79
- Configuring VLAN Autosense on page 80
- Configuring Layer 2 Loop Detection and Prevention for Extended Ports in a Junos Fusion on page 81
- Configuring LLDP on page 82
- Configuring a Firewall Filter on page 83
- Configuring SNMP on page 85
Configuring Commit Synchronization Between Aggregation Devices

Step-by-Step Procedure

Commit synchronization is used in the Enterprise Data Center solution to simplify administration tasks between aggregation devices.

The Enterprise Data Center solution uses a Junos Fusion Data Center topology that often requires matching configurations on both aggregation devices to support a feature.

Configuration synchronization simplifies administration of the Junos Fusion Data Center in this solution by allowing users to enter commands once in a configuration group and apply the configuration group to both aggregation devices rather than repeating a configuration procedure manually on each aggregation device. Configuration groups are used extensively in the Enterprise Data Center solution for this management simplicity.

The Junos Fusion Data Center setup in this solution is a multichassis link aggregation (MC-LAG) topology. For additional information on commit synchronization in an MC-LAG, see Understanding MC-LAG Configuration Synchronization.

NOTE: This document assumes that basic network configuration has been done for all devices in the topology, including hostname configuration, DNS setup, and basic IP configuration setup.

See Junos OS Basics Feature Guide for QFX10000 Switches if you need to setup basic network connectivity on your QFX10002-72Q switches before starting this procedure.
1. Ensure the aggregation devices are reachable from one another:

   **Aggregation device 1:**

   ```
   user@ad1-qfx10002> ping ad2-qfx10002 rapid
   PING ad2-qfx10002.host.example.net (192.168.255.41): 56 data bytes
   !!!!!
   --- ad2-qfx10002.example.net ping statistics ---
   5 packets transmitted, 5 packets received, 0% packet loss
   round-trip min/avg/max/stddev = 0.317/0.331/0.378/0.024 ms
   ```

   **Aggregation device 2:**

   ```
   user@ad2-qfx10002> ping ad1-qfx10002 rapid
   PING ad1-qfx10002.host.example.net (192.168.255.40): 56 data bytes
   !!!!!
   --- ad1-qfx10002.example.net ping statistics ---
   5 packets transmitted, 5 packets received, 0% packet loss
   round-trip min/avg/max/stddev = 0.317/0.331/0.378/0.024 ms
   ```

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

   **Aggregation device 1:**

   ```
   user@ad1-qfx10002# set system static-host-mapping ad2-qfx10002 inet 192.168.255.41
   user@ad1-qfx10002# commit
   user@ad1-qfx10002# run ping ad2-qfx10002 rapid
   ```

   **Aggregation device 2:**

   ```
   user@ad2-qfx10002# set system static-host-mapping ad1-qfx10002 inet 192.168.255.40
   user@ad2-qfx10002# commit
   user@ad2-qfx10002# run ping ad1-qfx10002 rapid
   ```

   If the devices cannot ping one another after the IP addresses are statically mapped, see [Configuring a QFX10000](#) or the [Junos OS Basics Feature Guide for QFX10000 Switches](#).

2. Enable commit synchronization:

   **Aggregation device 1:**

   ```
   set system commit peers-synchronize
   ```

   **Aggregation device 2:**

   ```
   set system commit peers-synchronize
   ```

3. Configure each aggregation device so that the other aggregation device is identified as a commit peer. Enter the authentication credentials of each peer aggregation device to ensure group configurations on one aggregation device are committed to the other aggregation device.
WARNING: The password `password` is used in this configuration step for illustrative purposes only. Use a more secure password in your device configuration.

NOTE: This step assumes a user with an authentication password has already been created on each QFX10002 switch acting as an aggregation device. For instructions on configuring username and password combinations, see Configuring a QFX10000.

Aggregation device 1:

```
set system commit peers ad2-qfx10002 user root authentication password
```

Aggregation device 2:

```
set system commit peers ad1-qfx10002 user root authentication password
```

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

   **Aggregation device 1:**

   ```
   set system services netconf ssh
   ```

   **Aggregation device 2:**

   ```
   set system services netconf ssh
   ```

5. Commit the configuration:

   **Aggregation device 1:**

   ```
   commit
   ```

   **Aggregation device 2:**

   ```
   commit
   ```

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

   **Aggregation Device 1:**

   ```
   set groups TEST when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups TEST
   ```

   **Aggregation Device 2:**
set apply-groups TEST

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

Aggregation device 1:

set groups TEST interfaces ge-0/0/1 description testing123
commit

Aggregation device 2:

user@ad2-qfx10002# show groups TEST
when {
    peers [ ad1-qfx10002 ad2-qfx10002 ];
}
interfaces {
    ge-0/0/1 {
        description testing123;
    }
}
user@ad2-qfx10002# run show interfaces ge-0/0/1
Physical interface: ge-0/0/1, Enabled, Physical link is Down
    Interface index: 235, SNMP ifIndex: 743
    Description: testing123
    (additional output removed for brevity)

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

Delete the test configuration group on each aggregation device.

Aggregation device 1:

delete groups test

Aggregation device 2:

delete groups test

NOTE: All subsequent procedures in this Solutions Guide assume that commit synchronization is enabled on both QFX10002-72Q switches acting as aggregation devices, and that the aggregation devices are configured as peers in each configuration group.
Configuring the Aggregated Ethernet Interfaces Connecting the MX480 Router to the QFX10002-72Q Switches

Step-by-Step Procedure
The bandwidth requirements for the links connecting the QFX10002-72Q switch to the MX480 router can vary widely between Enterprise data center networks, and is largely dependent on the bandwidth needs of a specific Enterprise data network. The available hardware interfaces—in particular, the hardware interfaces available in the modular interface slots of the MX480 router—can also impact which interfaces are used to connect the QFX10002-72Q switches to the MX480 router.

The remainder of this reference architecture assumes that two 6x40GE + 24x10GE MPC5EQ MPCs are installed in the MX480 router in slots 3 and 4.

The MX480 core router in the Enterprise Data Center solution uses two six member link aggregated Ethernet interfaces—one that connects to the QFX10002-72Q switch acting as aggregation device 1 and another that connects to the QFX10002-72Q switch acting as aggregation device 2—to provide a path for Layer 3 traffic in the topology. Each individual aggregated Ethernet interface contains six 40-Gbps QSFP+ member links, providing 240-Gbps total throughput.

Another usable option for this uplink connection would be to configure interfaces et-0/0/67 and et-0/0/71 as 100-Gbps interfaces to provide 200-Gbps total throughput between the MX480 router and each QFX10002-72Q switch, using two 100-Gbps cables instead of six 40-Gbps cables. This option would require you to disable the other 40-Gbps interfaces—et-0/0/66, et-0/0/68, et-0/0/69, and et-0/0/70—on the QFX10002-72Q switches, however, and provides slightly less bandwidth than using all six 40-Gbps QSFP+ interfaces. For information on using 100-Gbps interfaces for a QFX10002-72Q switch, see QFX10002-72Q Port Panel.

Link Aggregation Control Protocol (LACP) is used in each aggregated Ethernet interface to provide additional functionality for LAGs, including the ability to help prevent communication failures by detecting misconfigurations within a LAG.

Figure 5 on page 25 illustrates the MX480 router links to the QFX10002-72Q switches in the Enterprise Data Center solution.

Figure 5: MX480 Router to QFX10002-72Q Switch Connections

For additional information on aggregated Ethernet interfaces and LACP, see Understanding Aggregated Ethernet Interfaces and LACP and Configuring Link Aggregation.

To configure the aggregated Ethernet interfaces connecting the MX480 router to the QFX10002-72 switches in the Enterprise Data Center topology:
1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   Aggregation Device 1:
   set groups AE-ROUTER-ADSWITCHES when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups AE-ROUTER-ADSWITCHES

   Aggregation Device 2:
   set apply-groups AE-ROUTER-ADSWITCHES

   This procedure assumes commitment synchronization is configured. See “Configuring
Commit Synchronization Between Aggregation Devices” on page 20.

2. Set the maximum number of aggregated Ethernet interfaces permitted on the switch and router.

   The aggregated Ethernet device count value is set at 1000 on the MX router and both aggregation devices to avoid any potential complications with aggregated Ethernet interface configurations in this topology. This approach can create multiple empty, unused aggregated Ethernet interfaces with globally unique MAC addresses on the aggregation device. You can simplify network administration by setting the device count to the number of aggregated Ethernet devices that you are using on your aggregation device, if desired.

   MX480 Router:
   set chassis aggregated-devices ethernet device-count 1000

   QFX10002 Switch (Aggregation Device 1 or 2)
   set groups AE-ROUTER-ADSWITCHES chassis aggregated-devices ethernet device-count 1000

   NOTE: A device count must be set whenever an aggregated Ethernet interface is configured. Aggregated Ethernet interfaces are configured in other procedures in this document, and the aggregated Ethernet device count is set as part of those procedures. You can skip this step if the aggregated Ethernet device count has already been set.

   NOTE: The defaults for minimum links and link speed are maintained for the aggregated Ethernet interfaces configured in this solution. There is no need to change the default link speed setting or the default minimum links setting. The default minimum links setting, which can be changed by entering the set interfaces aeX aggregated-ether-options minimum-links number-of-minimum-links, is 1.
3. Create and name the aggregated Ethernet interfaces, and optionally assign a description to them:

**MX480 Router**

set interfaces ae100 description "ae to AD1-QFX10002"
set interfaces ae101 description "ae to AD2-QFX10002"

**QFX10002 Switch (Aggregation Device 1 or 2)**

set groups AE-ROUTER-ADSWITCHES interfaces ae100 description "ae to CORE-ROUTER-MX480"

---

**NOTE:** The QFX10002-72Q switches use the same aggregated Ethernet interfaces and names throughout this procedure, and can therefore be configured using shared groups.

The MX480 router is not synchronizing its configuration with other devices, and is therefore configured outside of shared configuration groups.

---

4. Assign interfaces to each aggregated Ethernet interface:

**MX480 Router:**

set interfaces et-3/2/0 ether-options 802.3ad ae100
set interfaces et-3/2/1 ether-options 802.3ad ae100
set interfaces et-3/2/2 ether-options 802.3ad ae100
set interfaces et-4/2/0 ether-options 802.3ad ae100
set interfaces et-4/2/1 ether-options 802.3ad ae100
set interfaces et-4/2/2 ether-options 802.3ad ae100
set interfaces et-3/3/0 ether-options 802.3ad ae101
set interfaces et-3/3/1 ether-options 802.3ad ae101
set interfaces et-3/3/2 ether-options 802.3ad ae101
set interfaces et-4/3/0 ether-options 802.3ad ae101
set interfaces et-4/3/1 ether-options 802.3ad ae101
set interfaces et-4/3/2 ether-options 802.3ad ae101

**QFX10002 Switch (Aggregation Device 1 or 2):**

set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/66 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/67 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/68 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/69 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/70 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/71 ether-options 802.3ad ae100
5. Assign an IP address for each aggregated Ethernet interface.
   Because IP addresses are local values, assign the IP address outside of the group configuration.

   **MX480 Router**

   set interfaces ae100 unit 0 family inet address 10.0.1.1/24
   set interfaces ae101 unit 0 family inet address 10.0.2.1/24

   **Aggregation Device 1**

   set interfaces ae100 unit 0 family inet address 10.0.1.100/24

   **Aggregation Device 2**

   set interfaces ae100 unit 0 family inet address 10.0.2.100/24

6. Enable LACP for the aggregated Ethernet interfaces and set them into active mode:

   **MX480 Router**

   set interfaces ae100 aggregated-ether-options lacp active
   set interfaces ae101 aggregated-ether-options lacp active

   **QFX10002 Switch (Aggregation Device 1 or 2)**

   set groups AE-ROUTER-ADSWITCHES interfaces ae100 aggregated-ether-options lacp active

7. Set the interval at which the interfaces send LACP packets.
   The Enterprise Data Center solution sets the LACP periodic interval as fast, which sends an LACP packet every second.

   **MX480 Router**

   set interfaces ae100 aggregated-ether-options lacp periodic fast
   set interfaces ae101 aggregated-ether-options lacp periodic fast

   **QFX10002 Switch (Aggregation Device 1 or 2)**

   set groups AE-ROUTER-ADSWITCHES interfaces ae100 aggregated-ether-options lacp periodic fast

8. After the aggregated Ethernet configuration is committed, confirm that the aggregated Ethernet interface is enabled, that the physical link is up, and that packets are being transmitted if traffic has been sent:

   **MX480 Router**

   user@mx480-core-router> show interfaces ae100
   Physical interface: ae100, Enabled, Physical link is Up
   Interface index: 640, SNMP ifIndex: 501
   Description: ae to AD1-QFX10002
   Link-level type: Ethernet, MTU: 1514, Speed: 240Gbps, BPDU Error: None, MAC-REWRITE Error: None,
   Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled,
Minimum links needed: 1,
Minimum bandwidth needed: 1bps
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Current address: 0c:86:10:d5:a9:be, Hardware address: 0c:86:10:d5:a9:be
Last flapped : 2017-03-14 00:29:32 PST (20:26:02 ago)
Input rate : 1928 bps (2 pps)
Output rate : 946264 bps (924 pps)

Logical interface ae100.0 (Index 2627) (SNMP ifIndex 1663)
Flags: Up SNMP-Traps Internal: 0x4000
Encapsulation: Ethernet-Bridge

Statistics Packets pps Bytes bps
Bundle:
Input : 136 0 18496 0
Output: 0 0 0 0

QFX10002 Switch (Aggregation Device 1 or 2):

user@ad1-qfx10002> show interfaces ae100
Physical interface: ae100, Enabled, Physical link is Up
Interface index: 640, SNMP ifIndex: 501
Description: ae to CORE-ROUTER-MX480
Link-level type: Ethernet, MTU: 1514, Speed: 240Gbps, BPDU Error: None,
MAC-REWRITE Error: None,
Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled,
Minimum links needed: 1,
Minimum bandwidth needed: 1bps
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Current address: 0c:86:10:d5:a9:be, Hardware address: 0c:86:10:d5:a9:be
Last flapped : 2017-03-14 00:29:33 PST (20:26:01 ago)
Input rate : 3915 bps (4 pps)
Output rate : 846261 bps (824 pps)

Logical interface ae100.0 (Index 2627) (SNMP ifIndex 1663)
Flags: Up SNMP-Traps Internal: 0x4000
Encapsulation: Ethernet-Bridge

Statistics Packets pps Bytes bps
Bundle:
Input : 136 0 18496 0
Output: 0 0 0 0

9. After committing the configuration, confirm the LACP status is Active and that the receive state is Current for each link.

The output below provides the status for interface et-3/2/0.

user@ad1-qfx10002> show lacp interfaces et-3/2/0
Aggregated interface: ae1
LACP state: Role Exp Def Dist Col Syn Aggr Timeout
Activity et-3/2/0 Actor No No Yes Yes Yes Yes Fast
Active et-3/2/0 Partner No No Yes Yes Yes Yes Fast
Active LACP protocol: Receive State Transmit State Mux State
et-3/2/0 Current Fast periodic Collecting distributing

Repeat this step for each link in the aggregated Ethernet bundle.
Assigning Cascade Ports to FPC ID Numbers and Creating Satellite Device Aliases

Step-by-Step Procedure
This procedure provides the instructions to map cascade port interfaces to the FPC ID numbers of connected satellite devices.

In a Junos Fusion Data Center, the port on the aggregation device that connects to a satellite device is called a cascade port. All network and control traffic sent between an aggregation device and a satellite device traverses a cascade port.

Figure 6 on page 31 illustrates the location of cascade ports in a Junos Fusion.

Figure 6: Cascade Ports in a Junos Fusion

The Enterprise Data Center reference topology uses the native 40-Gbps QSFP+ interfaces as well 10-Gbps interfaces channelized from the native 40-Gbps QSFP+ interfaces as cascade ports. An aggregation device can use one or more cascade ports to connect to a satellite device.

An FPC ID number is an identification number assigned to each satellite device in a Junos Fusion topology. Every satellite device in a Junos Fusion topology is assigned an FPC ID number.

Each satellite device in this topology is also assigned an alias. Aliases are optional but recommended attributes that assist with satellite device identification and network management.

Figure 7 on page 31 illustrates the cascade port to satellite device connections for some links in the satellite devices in the Enterprise Data Center solution topology. The figure does not include all cascade port to satellite device links for the topology for readability reasons.

Figure 7: Cascade Port to Satellite Device Connections
To assign cascade ports, FPC IDs, and satellite device aliases to the Enterprise Data Center solution topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**
   
   set groups FUSION-FPC-CASCADE-ALIAS when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups FUSION-FPC-CASCADE-ALIAS

   **Aggregation Device 2:**
   
   set apply-groups FUSION-FPC-CASCADE-ALIAS

   This procedure assumes commitment synchronization is configured. See "Configuring Commit Synchronization Between Aggregation Devices" on page 20.

2. Configure the interfaces on the QFX10002 switch acting in the aggregation device role into cascade ports. As part of this process, assign an FPC ID number and alias to each satellite device.

   **CAUTION:** This procedure uses group configurations to simplify FPC ID and cascade port configurations because the cascade port and FPC ID configurations are identical on both aggregation devices. Use manual configuration to configure FPC IDs and cascade ports on each aggregation device if your aggregation devices have different cascade port and FPC ID configurations.

   - To configure 40-Gbps QSFP+ interfaces et-0/0/0 through et-0/0/56 as cascade ports to FPC IDs 100 through 156:

     **Aggregation device 1 or 2:**
     
     set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 100 cascade-ports et-0/0/0
     set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 100 alias qfxs100-sd100
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 101
cascade-ports et-0/0/1
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 101
alias qfx5100-sd101
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 102
cascade-ports et-0/0/2
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 102
alias qfx5100-sd102
... ...
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 156
cascade-ports et-0/0/56
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 156
alias ex4300-sd156

- To configure each of the 4 10-Gbps channelized interfaces from
  et-0/0/57—et-0/0/57:0, et-0/0/57:1, et-0/0/57:2, and et-0/0/57:3—as cascade
  ports to FPC IDs 157 through 160:

  **Aggregation device 1 or 2:**

  set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 157
cascade-ports et-0/0/57:0
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 157
alias ex4300-sd157
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 158
cascade-ports et-0/0/57:1
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 158
alias ex4300-sd158
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 159
cascade-ports et-0/0/57:2
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 159
alias ex4300-sd159
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 160
cascade-ports et-0/0/57:3
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 160
alias ex4300-sd160

- To configure two cascade ports each from interfaces et-0/0/58 through
  et-0/0/63 to FPC IDs 161, 162, and 163:

  **Aggregation device 1 or 2:**

  set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161
cascade-ports et-0/0/58
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161
cascade-ports et-0/0/59
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161
alias ex4300-sd161
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162
cascade-ports et-0/0/60
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162
cascade-ports et-0/0/61
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162
alias ex4300-sd162
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163
cascade-ports et-0/0/62
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163
cascade-ports et-0/0/63
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163 alias ex4300-sd163

3. Commit the configuration.

commit

Because commit synchronization is enabled and this configuration is done in configuration groups, the configuration in the group is committed to aggregation device 2 as well as on aggregation device 1.

Converting Interfaces into Cascade Ports

FPC ID numbers were assigned to cascade ports in the prior procedure. However, an interface on an aggregation device must also be explicitly configured into a cascade port before it can function as a cascade port.

Follow the instructions in this section to configure interfaces into cascade ports.

For a comprehensive configuration example of this procedure that includes configuration of every cascade port configuration in the solution, see Appendix: Enterprise Data Center Solution Complete Configuration.

To configure interfaces on the aggregation device into cascade ports:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   Aggregation Device 1:

   set groups FUSION-FPC-CASCADE-ALIAS when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups FUSION-FPC-CASCADE-ALIAS

   Aggregation Device 2:

   set apply-groups FUSION-FPC-CASCADE-ALIAS

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Configure each cascade port interface into a cascade port:

   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/0 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/1 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/2 cascade-port
   ...
   ...
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:0 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:1 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:2 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:3 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/58 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/59 cascade-port
   set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/60 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/61 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/62 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/63 cascade-port

3. Commit the configuration.

   commit

Because commit synchronization is enabled and this configuration is done in configuration groups, the configuration in the group is committed to aggregation device 2 as well as on aggregation device 1.
Configuring the Aggregated Ethernet Interfaces for the Interchassis Link (ICL)

The aggregation devices in a Junos Fusion Data Center topology are MC-LAG peers. MC-LAG peers use an interchassis link (ICL), also known as the interchassis link-protection link (ICL-PL), to provide a redundant path across the MC-LAG topology when a link failure (for example, an MC-LAG trunk failure) occurs on an active link.

MC-LAG peers use the Inter-Chassis Control Protocol (ICCP) to exchange control information and coordinate with one another to ensure that data traffic is forwarded properly. ICCP traffic is also sent over the ICL in this solution topology, although some MC-LAG implementations use a separate link for ICCP traffic. Junos Fusion Data Center supports automatic ICCP provisioning, a feature that automatically provisions ICCP traffic to be sent across the ICL without user configuration. Automatic ICCP provisioning is enabled by default, so no user configuration is required to enable ICCP in this solution topology.

See Multichassis Link Aggregation Features, Terms, and Best Practices for additional information on ICLs and ICCP.

In the Enterprise Data Center topology, an aggregated Ethernet interface—ae999—with two member interfaces—et-0/0/64 and et-0/0/65—provides the ICL on each aggregation device.

Figure 8 on page 36 illustrates the ICL for the Enterprise Data Center solution:

Figure 8: ICL in the Enterprise Data Center Solution Topology

To configure the ICL:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**

   ```
   set groups ICL-CONFIG when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups ICL-CONFIG
   ```

   **Aggregation Device 2:**

   ```
   set apply-groups ICL-CONFIG
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. On aggregation device 1, create a group for the ICL link configuration and set the aggregated Ethernet device count for the aggregation devices:
Aggregation Device 1:

set groups ICL-CONFIG chassis aggregated-devices ethernet device-count 1000

---

**NOTE:** A device count must be set whenever an aggregated Ethernet interface is configured. Aggregated Ethernet interfaces are configured in other procedures in this document, and the aggregated Ethernet device count is set as part of those procedures. You can skip this step if the aggregated Ethernet device count has already been set.

---

**NOTE:** This approach can create multiple empty, unused aggregated Ethernet interfaces with globally unique MAC addresses on the aggregation device. You can simplify network administration by setting the device count to the number of aggregated Ethernet devices that you are using on your aggregation device.

---

3. Create the aggregated Ethernet interface that will function as the ICL, and optionally add a description to the interface:

**Aggregation Device 1:**

set groups ICL-CONFIG interfaces ae999 description icl-link

4. Add the member links to the aggregated Ethernet interface:

**Aggregation Device 1:**

set groups ICL-CONFIG interfaces et-0/0/64 ether-options 802.3ad ae999
set groups ICL-CONFIG interfaces et-0/0/65 ether-options 802.3ad ae999

5. Enable LACP for the aggregated Ethernet interface and configure the LACP packet interval:

**Aggregation Device 1:**

set groups ICL-CONFIG interfaces ae999 aggregated-ether-options lacp active
set groups ICL-CONFIG interfaces ae999 aggregated-ether-options lacp periodic fast

6. Configure the ICL aggregated Ethernet interface as a trunk interface, and configure it as a member of all VLANs:

**Aggregation Device 1:**

set groups ICL-CONFIG interfaces ae999 unit 0 family ethernet-switching interface-mode trunk
set groups ICL-CONFIG interfaces ae999 unit 0 family ethernet-switching vlan members all
The ICL aggregated Ethernet interface is now configured. The aggregated Ethernet interface is converted into an ICL in the next section, as part of the procedure to configure dual aggregation device support.

**Configuring Dual Aggregation Device Support**

**Step-by-Step Procedure**

The Enterprise Data Center topology is a Junos Fusion Data Center architecture with dual aggregation devices.

A Junos Fusion Data Center architecture with dual aggregation devices is enabled by configuring all devices in the Junos Fusion Data Center topology into a redundancy group. The ICL is defined as part of the redundancy group configuration.

This procedure shows how to configure dual aggregation device support for the Enterprise Data Center solution topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   *Aggregation Device 1:*
   
   set groups DUAL-AD-CONFIG when peers [ad1-qfx10002 ad2-qfx10002]
   
   set apply-groups DUAL-AD-CONFIG
   
   *Aggregation Device 2:*
   
   set apply-groups DUAL-AD-CONFIG

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. (Optional unless single-home was previously configured on the aggregation device)
Delete single home configuration mode on each QFX10002 switch to ensure single-home configuration is disabled:

   *Aggregation device 1:*
   
   delete chassis satellite-management single-home

   *Aggregation device 2:*
   
   delete chassis satellite-management single-home

3. Create the satellite management redundancy group.

   In a Junos Fusion Data Center topology, both aggregation devices and all satellite devices must be part of the same redundancy group.

   *Aggregation device 1:*
   
   set groups DUAL-AD-CONFIG chassis satellite-management redundancy-groups rg1 redundancy-group-id 1
4. Add all satellite devices to the redundancy groups.
   
   ```
   set groups DUAL-AD-CONFIG chassis satellite-management redundancy-groups rg1 satellite all
   ```

5. Define the chassis ID number of each aggregation device. The chassis ID is a local parameter for each aggregation device, and should therefore be configured outside of a configuration group.

   **Aggregation device 1:**
   
   ```
   set chassis satellite-management redundancy-groups chassis-id 1
   ```

   **Aggregation device 2:**
   
   ```
   set chassis satellite-management redundancy-groups chassis-id 2
   ```

6. Define the peer chassis ID number—the chassis ID number of the other aggregation device—and interface to use for the ICL on each aggregation device.

   The peer chassis ID number is a local parameter for each aggregation device, and should therefore be configured outside of a configuration group.

   **Aggregation device 1:**
   
   ```
   set chassis satellite-management redundancy-groups rg1 peer-chassis-id 2 inter-chassis-link ae999
   ```

   **Aggregation device 2:**
   
   ```
   set chassis satellite-management redundancy-groups rg1 peer-chassis-id 1 inter-chassis-link ae999
   ```

7. Commit the configuration individually on each aggregation device.

   **Aggregation device 1:**
   
   ```
   commit
   ```

   **Aggregation device 2:**
   
   ```
   commit
   ```

   The portions of this configuration that were configured in groups are committed to aggregation device 1 and 2, since commit synchronization is enabled.

8. Confirm that ICCP is operational between the peers:

   This step assumes that the redundancy groups and the aggregated Ethernet interface for the ICCP link have been configured and committed.

   ICCP is automatically provisioned in this topology, since the automatic ICCP provisioning feature is automatically enabled in dual aggregation device topologies by default and is not altered in this configuration procedure.

   **Aggregation device 1:**
   
   ```
   ```
Configuring Bidirectional Forwarding Detection (BFD) over the ICL

Step-by-Step Procedure

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that can quickly detect a link failure in a network. BFD hello packets are sent at a specified, regular interval. A neighbor failure is detected when a device doesn’t receive a reply to a BFD hello message within a specified interval.

In the Enterprise Data Center topology, BFD is used to provide link failure detection for the ICL. BFD sends hello packets between the aggregation devices over the ICL connecting the aggregation devices.

To configure BFD over the ICL for the Enterprise Data Center solution:

1. Configure the BFD liveness detection parameters on each aggregation device.

   We recommend configuring minimum intervals of 2000 to ensure stability in the MC-LAG configuration.

   **Aggregation device 1:**

   ```
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 2 liveness-detection minimum-interval 2000
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 2 liveness-detection multiplier 3
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 2 liveness-detection transmit-interval minimum-interval 2000
   ```

   **Aggregation device 2:**

   ```
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 1 liveness-detection minimum-interval 2000
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 1 liveness-detection multiplier 3
   set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1 peer-chassis-id 1 liveness-detection transmit-interval minimum-interval 2000
   ```
2. After committing the configuration, verify that BFD state to the peer aggregation device is operational:

*Aggregation device 1:*

```bash
user@ad1-qfx10002> show bfd session
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>Up</td>
<td></td>
<td>6.000</td>
<td>2.000</td>
</tr>
</tbody>
</table>

1 sessions, 1 clients
Cumulative transmit rate 0.5 pps, cumulative receive rate 0.5 pps

*Aggregation device 2:*

```bash
user@ad2-qfx10002> show bfd session
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>Up</td>
<td></td>
<td>6.000</td>
<td>2.000</td>
</tr>
</tbody>
</table>

1 sessions, 1 clients
Cumulative transmit rate 0.5 pps, cumulative receive rate 0.5 pps
Enabling Automatic Satellite Device Conversion

Automatic satellite device conversion automatically converts a switch running Junos OS into a satellite device upon cabling, assuming all other configuration prerequisites—the satellite device is a model of switch that can be converted into a satellite device and is running a version of Junos OS that supports conversion, cascade ports and FPC ID numbering is configured and enabled, and satellite software upgrade groups are created so the satellite device can retrieve satellite software—are met. The steps for creating satellite software upgrade groups are provided in the next section of this guide; all of the other pre-requisite steps were done in earlier sections of this guide.

Although other methods of converting a switch into a satellite device exist, this solution uses automatic satellite conversion exclusively to convert switches running Junos OS into satellite devices.

To enable automatic satellite device conversion for all satellite devices connected to a cascade port on an aggregation device:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**

   ```
   set groups AUTO-SAT-CONV when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups AUTO-SAT-CONV
   ```

   **Aggregation Device 2:**

   ```
   set apply-groups AUTO-SAT-CONV
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Enable automatic satellite conversion:

   ```
   set groups AUTO-SAT-CONV chassis satellite-management auto-satellite-conversion satellite all
   ```

   Automatic satellite conversion is recommended for this solution but other satellite software upgrade methods exist. See Configuring or Expanding a Junos Fusion Data Center.
Installing and Managing the Satellite Software

Satellite devices in a Junos Fusion Data Center run satellite software. Satellite software upgrade groups must be created on the aggregation devices to manage satellite software installations. The topology in this solution uses two satellite software upgrade groups. One satellite software upgrade group is used to install satellite software onto all EX4300 switches acting as satellite devices; the other is used to install software onto all QFX5100 switches acting as satellite devices.

The same version of satellite software—satellite software version 3.0R1—runs on EX4300 and QFX5100 switches acting as satellite devices in this topology. Both satellite software upgrade groups use the same software package to upgrade satellite software.

For a comprehensive configuration example of this procedure that includes all satellite software upgrade group configuration commands, see Appendix: Enterprise Data Center Solution Complete Configuration.

To install and manage the satellite software:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:
   
   **Aggregation Device 1:**
   
   ```
   set groups SAT-SW-UPGRADE when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups SAT-SW-UPGRADE
   ```
   
   **Aggregation Device 2:**
   
   ```
   set apply-groups SAT-SW-UPGRADE
   ```
   
   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Copy the satellite software 3.0R1 image onto each QFX10002 switch acting as an aggregation device.
   
   File copying options are beyond the scope of this solutions guide. See Upgrading Software.
   
   These instructions assume a satellite software image has been installed to the var/tmp directory on each aggregation device.

3. Create the satellite software upgrade groups and associate the FPC IDs with the groups:
   
   **Aggregation Device 1:**
   
   ```
   set groups SAT-SW-UPGRADE chassis satellite-management upgrade-groups qfx5100-sd satellite 100-139
   set groups SAT-SW-UPGRADE chassis satellite-management upgrade-groups ex4300-sd satellite 140-163
   ```

   Copyright © 2017, Juniper Networks, Inc.
4. Commit the configuration:

commit

5. On each aggregation device, associate a satellite software image with each satellite software upgrade group:

Aggregation Device 1:

user@ad1-qfx10002> request system software add /var/tmp/satellite-3.0R1.6-signed.tgz
upgrade-group qfx5100-sd
user@ad1-qfx10002> request system software add /var/tmp/satellite-3.0R1.6-signed.tgz
upgrade-group ex4300-sd

Aggregation Device 2:

user@ad2-qfx10002> request system software add /var/tmp/satellite-3.0R1.6-signed.tgz
upgrade-group qfx5100-sd
user@ad2-qfx10002> request system software add /var/tmp/satellite-3.0R1.6-signed.tgz
upgrade-group ex4300-sd

The satellite software upgrade starts at this point of the procedure. The satellite software upgrade can take several minutes per satellite device and is throttled, so satellite devices restart operations at different intervals.

The satellite software upgrade group configurations can be verified later in this process, once the satellite devices are operational.
Preparing the Satellite Devices

Step-by-Step Procedure

To prepare the switches to become satellite devices, perform the following steps:

1. Log into each switch’s console port, and zeroize it.

   ```
   user@sd101-con> request system zeroize
   user@sd102-con> request system zeroize
   user@sd103-con> request system zeroize
   ...
   user@sd163-con> request system zeroize
   ```

   **NOTE:** Perform this procedure from the console port connection. A management connection will be lost when the switch is rebooted to complete the zeroizing procedure.

2. (EX4300 switches only) After the switches reboot, convert the built-in 40-Gbps interfaces with QSFP+ transceivers from Virtual Chassis ports (VCPs) into network ports:

   The following sample output shows how to perform this procedure on each EX4300 switch acting as a satellite device.

   ```
   user@sd140-con> request virtual-chassis vc-port delete pic-slot 1 port 0
   user@sd140-con> request virtual-chassis vc-port delete pic-slot 1 port 1
   user@sd140-con> request virtual-chassis vc-port delete pic-slot 1 port 2
   user@sd140-con> request virtual-chassis vc-port delete pic-slot 1 port 3
   ...
   (some redundant procedures removed for brevity)
   user@sd163-con> request virtual-chassis vc-port delete pic-slot 1 port 0
   user@sd163-con> request virtual-chassis vc-port delete pic-slot 1 port 1
   user@sd163-con> request virtual-chassis vc-port delete pic-slot 1 port 2
   user@sd163-con> request virtual-chassis vc-port delete pic-slot 1 port 3
   ```

   This step has to be performed on EX4300 switches only, since built-in 40-Gbps interfaces on EX4300 switches are set as Virtual Chassis ports (VCPs) by default. A Virtual Chassis port (VCP) cannot be converted into an uplink port on a satellite device in a Junos Fusion.

**NOTE:** These instructions assume each switch is already running Junos OS Release 14.1X53-D43 or later. See Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure) for instructions on upgrading Junos OS software.
This step is skipped for QFX5100 switches because the built-in 40-Gbps interfaces on QFX5100 switches are not configured into VCPs by default.

3. Cable each switch into the Junos Fusion, if you haven’t already done so.

Because automatic satellite conversion is enabled and the satellite software upgrade groups have been configured, the satellite software installation process starts for each satellite device when it is cabled to the aggregation device.

NOTE: If the satellite software installation does not begin, log onto the aggregation devices and ensure the configurations added in previous steps have been committed.

The installation can take several minutes.

4. Verify that the satellite software installation was successful:

NOTE: The show chassis satellite software command generates output only after the satellite software upgrades are complete. If you enter the show chassis satellite software command and no output is generated, consider re-entering the command in a few minutes.

Aggregation device 1:

```
user@ad1-qfx10002> show chassis satellite software
Version           Platforms          Group
3.0R1.6            i386 ppc          ex4300-sd
                   qfx5100-sd
```

Aggregation device 2:

```
user@ad2-qfx10002> show chassis satellite software
Version           Platforms          Group
3.0R1.6            i386 ppc          ex4300-sd
                   qfx5100-sd
```

5. Confirm the satellite software upgrade groups configurations:

```
user@ad1-qfx10002> show chassis satellite upgrade-group
Group           Sw-Version State       Slot  State
__ungrouped__   3.0R1       in-sync     140 version-in-sync
                  141 version-in-sync
                  142 version-in-sync
                  ...(some redundant output removed for brevity)
qfx5100-sd       3.0R1       in-sync     163 version-in-sync
                   100 version-in-sync
                   101 version-in-sync
```
Verifying that the Junos Fusion Data Center is Operational

**Purpose**
Verify that the aggregation device recognizes all satellite devices, and that all satellite devices and cascade ports are online.

**Action**
Enter the `show chassis satellite` command:

```
user@ad1-qfx10002> show chassis satellite
Device          Cascade      Port       Extended Ports
Alias            Slot   State           Ports        State      Total/Up
qfx5100-sd100    100    Online          et-0/0/0     online     52/52
ae999*       backup
qfx5100-sd101    101    Online          et-0/0/1     online     52/52
ae999*       backup
qfx5100-sd102    102    Online          et-0/0/2     online     52/52
ae999*       backup
...  
ex4300-sd156     156    Online          et-0/0/56    online     52/52
ae999*       backup
ex4300-sd157     157    Online          et-0/0/57:0  online     52/52
ae999*       backup
ex4300-sd158     158    Online          et-0/0/57:1  online     52/52
ae999*       backup
ex4300-sd159     159    Online          et-0/0/57:2  online     52/52
ae999*       backup
ex4300-sd160     160    Online          et-0/0/57:3  online     52/52
ae999*       backup
ex4300-sd161     161    Online          et-0/0/58    online     52/52
et-0/0/59    online
ae999*       backup
ex4300-sd162     162    Online          et-0/0/60    online     52/52
et-0/0/61    online
ae999*       backup
ex4300-sd163     163    Online          et-0/0/62    online     52/52
et-0/0/63    online
ae999*       backup
...  
```

The **Alias** and **Slot** outputs list all satellite devices and the **Device State** output confirms that each satellite device is online. These outputs confirm the satellite devices are recognized and operational.

The **Cascade Ports** output confirms the cascade port configuration on the aggregation device, and the **Port State** output confirms that the cascade ports are online. It includes the ICL interface as a backup port, since cascade port traffic may flow over the ICL if a cascade port link to a single aggregation device fails.
Configuring Uplink Port Pinning

Step-by-Step Procedure
Uplink port pinning is used to ensure all upstream traffic from a specified extended port on a satellite device is transported to the aggregation device over a specified uplink port.

When uplink port pinning is not configured on an extended port in a Junos Fusion, all traffic from the extended port is load balanced across all uplink interfaces when it is transported to the aggregation devices.

Uplink port pinning is useful in cases where you want to better manage upstream traffic to the aggregation devices. For instance, uplink port pinning can help in scenarios where the default load balancing of upstream traffic under-utilizes one of the upstream links by letting you direct all traffic from an extended port or ports to the under-utilized link. Uplink port pinning is also useful if you want to isolate traffic from an extended port or ports so that the traffic flows always receive identical treatment to the aggregation device.

In the Enterprise Data Center solution, uplink port pinning is enabled for extended port interfaces ge-162/0/47 and ge-163/0/47—port 47 on FPC ID 162 and FPC ID 163—to ensure all traffic received on these extended ports is transported to the aggregation device over uplink port 1/0 on their satellite devices.

Figure 9 on page 49 illustrates traffic flow in the Enterprise Data Center solution before and after uplink port pinning is enabled.

Figure 9: Uplink Port Pinning

See Configuring Uplink Port Pinning for Satellite Devices on a Junos Fusion Data Center for additional information on uplink port pinning.

To configure uplink port pinning:
1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**

   ```
   set groups UPLINK_PIN when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups UPLINK_PIN
   ```

   **Aggregation Device 2:**

   ```
   set apply-groups UPLINK_PIN
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Create a port group alias in a satellite policy to define the extended port on the satellite device whose traffic will be pinned to an uplink port:

   ```
   set groups UPLINK_PIN policy-options satellite-policies port-group-alias extended-port47 pic 0 port 47
   ```

3. Create a port group alias in a satellite policy to define the uplink port on the satellite device that is pinned to the extended port:

   ```
   set groups UPLINK_PIN policy-options satellite-policies port-group-alias uplink-port1 pic 1 port 0
   ```

4. Create a forwarding policy that groups the port group alias definitions into a single policy.

   ```
   set groups UPLINK_PIN policy-options satellite-policies forwarding-policy uplink-port-policy-port47-to-port0 port-group-extended extended-port1 port-group-uplink uplink-port1
   ```

5. Associate the forwarding policy with the FPC ID numbers of the satellite devices.

   ```
   set groups UPLINK_PIN chassis satellite-management fpc 162 forwarding-policy uplink-port-policy-port47-to-port0
   set groups UPLINK_PIN chassis satellite-management fpc 163 forwarding-policy uplink-port-policy-port47-to-port0
   ```

6. After committing the configuration, enter the `show chassis satellite detail fpc-slot fpc-slot-id-number detail` command to verify uplink port pinning operation.

   In the output below, uplink port pinning operation is confirmed for the satellite device using FPC slot 162.

   ```
   user@ad1-qfx10002> show chassis satellite detail fpc-slot 162 detail
   Satellite Alias: ex4300-sd162
   FPC Slot: 162
   Operational State: Online
   Product Model: EX4300-48P
   ... ...
   ```
Enabling Uplink Failure Detection

The uplink failure detection feature (UFD) on a Junos Fusion enables satellite devices to detect link failures on the uplink interfaces used to connect to aggregation devices. When UFD detects that all uplink interfaces on a satellite device are down, all of the satellite 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 UFD 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.

In the Enterprise Data Center solution, UFD is enabled for all satellite device uplink interfaces in the Junos Fusion Data Center topology.

For more information on UFD in a Junos Fusion, see Overview of Uplink Failure Detection on a Junos Fusion.

For information on other methods and options for configuring UFD in a Junos Fusion, see Configuring Uplink Failure Detection on a Junos Fusion.

To configure UFD for all uplink ports in the Junos Fusion Data Center topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   Aggregation Device 1:
   ```
   set groups UFD when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups UFD
   ```

   Aggregation Device 2:
   ```
   set apply-groups UFD
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Enable UFD with the default settings. By default, UFD is applied to all cascade port connections.
set groups UFD chassis satellite-management uplink-failure-detection

The default UFD settings—apply UFD for all uplink ports on all satellite devices—are maintained in this configuration. See Overview of Uplink Failure Detection on a Junos Fusion for additional information on uplink port failure detection default settings. See Configuring Uplink Failure Detection on a Junos Fusion for other UFD configuration options.

3. After committing the configuration, enter the show chassis satellite detail fpc-slot fpc-slot-id-number command to verify UFD operation and settings.

In the output below, UFD operation is confirmed for the satellite device using FPC slot 100.

```
user@ad1-qfx10002>  show chassis satellite detail fpc-slot 100
Satellite Alias: qfx5100-sd100
FPC Slot: 100
Operational State: Online
...
...(Output not related to uplink failure detection removed for brevity)
UFD config state: Enable (persist), Minimum link: 1, Hold down timer (seconds): 6
UFD operational state: Enable
Candidate uplink interfaces (pic/port):
  1/0
  1/1
  1/2
  1/3
  2/0
  2/1
  2/2
  2/3
```

A configuration with UFD must be committed before this output is visible. No UFD information appears in the show chassis satellite detail fpc-slot fpc-slot-id-number command output when UFD is not enabled.
Enabling an Aggregated Ethernet Interface For Access Interfaces

Step-by-Step Procedure
This procedure shows how to create an aggregated Ethernet interface composed of access interfaces. Access interfaces are the network-facing interfaces on the EX4300 and QFXS100 switches acting as satellite devices. Access interfaces on satellite devices in a Junos Fusion Data Center are also called extended ports.

An aggregated Ethernet interface is a collection of multiple links between physical interfaces that are bundled into one logical point-to-point link. An aggregated Ethernet interface is also commonly called a link aggregation group (LAG).

An aggregated Ethernet interface balances traffic across its member links within the aggregated Ethernet bundle and effectively increases the uplink bandwidth. Aggregated Ethernet interfaces also increase high availability, because an aggregated Ethernet interface is composed of multiple member links that can continue to carry traffic when one member link fails.

Link Aggregation Control Protocol (LACP) provides additional functionality for LAGs, including the ability to help prevent communication failures by detecting misconfigurations within a LAG.

In the Enterprise Data Center solution, aggregated Ethernet interfaces are configured using extended port member links to increase uplink bandwidth and high availability. These member links can be on extended port interfaces located on different satellite devices, and often should be to ensure high availability and load balancing for traffic to and from the endpoint device. These aggregated Ethernet interfaces also are configured to use LACP for link control.

Six total aggregated Ethernet interfaces composed of extended ports—each with two member links to interfaces on different satellite devices—are used in this reference topology. These step-by-step instructions show how to configure one aggregated Ethernet interface—ae1—first before providing the instructions for configuring the remaining aggregated Ethernet interfaces.

Figure 10 on page 54 illustrates the aggregated Ethernet 1 interface configuration in this topology.

**Figure 10: Aggregated Ethernet Interface Example (ae1)**

For additional information on aggregated Ethernet interfaces and LACP, see Understanding Aggregated Ethernet Interfaces and LACP and Configuring Link Aggregation.
To configure an aggregated Ethernet interface with extended port member links that uses LACP in the Enterprise Data Center solution topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**
   
   ```
   set groups AE-LACP-VLAN when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups AE-LACP-VLAN
   ```

   **Aggregation Device 2:**
   
   ```
   set apply-groups AE-LACP-VLAN
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Set the maximum number of aggregated Ethernet interfaces permitted on the aggregation device switch.

   ```
   set groups AE-LACP-VLAN chassis aggregated-devices ethernet device-count 1000
   ```

   **NOTE:** A device count must be set whenever an aggregated Ethernet interface is configured. Aggregated Ethernet interfaces are configured in other procedures in this document, and the aggregated Ethernet device count is set as part of those procedures. You can skip this step if the aggregated Ethernet device count has already been set.

   **NOTE:** This approach can create multiple empty, unused aggregated Ethernet interfaces with globally unique MAC addresses on the aggregation device. You can simplify network administration by setting the device count to the number of aggregated Ethernet devices that you are using on your aggregation device.

   **NOTE:** The defaults for minimum links and link speed are maintained for the aggregated Ethernet interfaces configured in this solution. There is no need to change the default link speed setting or the default minimum links setting. The default minimum links setting, which can be changed by entering the `set interfaces aeX aggregated-ether-options minimum-links number-of-minimum-links`, is 1.
3. Create and name the aggregated Ethernet interface, and optionally assign a
description to it:

   set groups AE-LACP-VLAN interfaces ae1 description "ae to server1"

4. Assign interfaces to the aggregated Ethernet interface:

   set groups AE-LACP-VLAN interfaces ge-101/0/22 ether-options 802.3ad ae1
   set groups AE-LACP-VLAN interfaces ge-102/0/22 ether-options 802.3ad ae1

5. Enable LACP for the aggregated Ethernet interface and set LACP into active mode:

   set groups AE-LACP-VLAN interfaces ae1 aggregated-ether-options lacp active

6. Set the interval at which the interfaces send LACP packets.

   The Enterprise Data Center solution sets the LACP periodic interval as fast, which
   sends an LACP packet every second.

   set groups AE-LACP-VLAN interfaces ae1 aggregated-ether-options lacp periodic
   fast

7. After the aggregated Ethernet configuration is committed, confirm that the
aggregated Ethernet interface is enabled and that the physical link is up:

   user@ad1-qfx10002> show interfaces ae1
   Physical interface: ae1, Enabled, Physical link is Up, Extended Port,
multi-homed
   Interface index: 640, SNMP ifIndex: 501
   Description: ae1 to server1
   Link-level type: Ethernet, MTU: 1514, Speed: 2Gbps, BPDU Error: None,
   MAC-REWRITE Error: None,
   Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled,
   Minimum links needed: 1,
   Minimum bandwidth needed: 1bps
   Device flags : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Current address: 0c:86:10:d5:a9:be, Hardware address: 0c:86:10:d5:a9:be
   Last flapped : 2017-02-03 00:29:32 PST (20:26:02 ago)
   Input rate : 1928 bps (2 pps)
   Output rate : 946264 bps (924 pps)
   Logical interface ae1.0 (Index 2627) (SNMP ifIndex 1663)
   Flags: Up SNMP-Traps 0x24024000 Encapsulation: Ethernet-Bridge
   Statistics        Packets        pps         Bytes          bps
   Bundle:             Input: 136          0         18496            0
   Output:             0            0             0            0
   (additional output removed for brevity)

8. After committing the configuration, confirm the LACP status is Active and that the
receive state is Current for each link.

   The output below provides the status for interface ge-101/0/22.

   user@ad1-qfx10002> show lACP interfaces ge-101/0/22
   Aggregated interface: ae1
   LACP state:            Role  Exp  Def  Dist  Col  Syn  Aggr  Timeout

Repeat this step for each link in the aggregated Ethernet bundle.

9. Repeat this procedure to configure each aggregated Ethernet interface in your implementation of the solution.

Figure 11 on page 57 illustrates all of the aggregated Ethernet access interfaces in the solution.

Figure 11: Aggregated Ethernet Interfaces

To configure the remaining five aggregated Ethernet interfaces:

set groups AE-LACP-VLAN interfaces ae2 description "ae to server2"
set groups AE-LACP-VLAN interfaces ge-101/0/23 ether-options 802.3ad ae2
set groups AE-LACP-VLAN interfaces ge-102/0/23 ether-options 802.3ad ae2
set groups AE-LACP-VLAN interfaces ae2 aggregated-ether-options lACP active
set groups AE-LACP-VLAN interfaces ae2 aggregated-ether-options lACP periodic
set groups AE-LACP-VLAN interfaces ae2 aggregated-ether-options lACP fast
set groups AE-LACP-VLAN interfaces ae3 description "ae to server3"
set groups AE-LACP-VLAN interfaces ge-101/0/24 ether-options 802.3ad ae3
set groups AE-LACP-VLAN interfaces ge-102/0/24 ether-options 802.3ad ae3
set groups AE-LACP-VLAN interfaces ae3 aggregated-ether-options lACP active
set groups AE-LACP-VLAN interfaces ae3 aggregated-ether-options lACP periodic
set groups AE-LACP-VLAN interfaces ae3 aggregated-ether-options lACP fast
set groups AE-LACP-VLAN interfaces ae4 description "ae to server4"
set groups AE-LACP-VLAN interfaces ge-103/0/22 ether-options 802.3ad ae4
set groups AE-LACP-VLAN interfaces ge-104/0/22 ether-options 802.3ad ae4
set groups AE-LACP-VLAN interfaces ae4 aggregated-ether-options lACP active
set groups AE-LACP-VLAN interfaces ae4 aggregated-ether-options lACP periodic
set groups AE-LACP-VLAN interfaces ae4 aggregated-ether-options lACP fast
set groups AE-LACP-VLAN interfaces ae5 description "ae to server5"
set groups AE-LACP-VLAN interfaces ge-103/0/23 ether-options 802.3ad ae5
set groups AE-LACP-VLAN interfaces ge-104/0/23 ether-options 802.3ad ae5
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lACP active
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lACP periodic
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lACP fast
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lACP periodic fast
set groups AE-LACP-VLAN interfaces ae6 description "ae to server6"
set groups AE-LACP-VLAN interfaces ge-103/0/24 ether-options 802.3ad ae6
set groups AE-LACP-VLAN interfaces ge-104/0/24 ether-options 802.3ad ae6
set groups AE-LACP-VLAN interfaces ae6 aggregated-ether-options lACP active
set groups AE-LACP-VLAN interfaces ae6 aggregated-ether-options lACP periodic fast
Configuring IRB Interfaces and VLANs

Step-by-Step Procedure
Traffic is isolated and segmented at layer 2 in the Enterprise Data Center solution using VLANs. Traffic is moved between VLANs using IRB interfaces on the aggregation devices.

A VLAN is a collection of LAN nodes grouped together to form an individual broadcast domain. VLANs segment traffic on a LAN into separate broadcast domains to limit the amount of traffic flowing across the entire LAN, reducing collisions and packet retransmissions. For instance, a VLAN can include all employees in a department and the resources that they use often, such as printers, servers, and so on. See Understanding Bridging and VLANs for additional information on VLANs.

IRB interfaces have multiple uses in this data center topology. Traffic that is forwarded from one endpoint device in the Junos Fusion Data Center to another endpoint device in a different VLAN in the same Junos Fusion Data Center uses the IRB interfaces to forward the traffic between the VLANs. IRB interfaces also move upstream traffic originating from an endpoint device to the MX480 core router.

The IRB interfaces are configured on the aggregation devices in this solution topology. An advantage of configuring IRB interfaces on the aggregation devices is that inter-VLAN traffic is processed more efficiently in the Enterprise Data Center because it doesn’t have to be passed to the MX router—a process that adds an upstream and a downstream hop—for processing.

This topology shows how to configure two VLANs, each with three member aggregated Ethernet interfaces that have links connecting to two satellite devices. The aggregated Ethernet interfaces were configured in the previous section. The IRB interfaces in this configuration move inter-VLAN traffic—traffic moving between VLAN 100 and VLAN 200—between the two VLANs.

Figure 12 on page 60 illustrates the VLANs and IRB interface configuration used in this architecture.

Figure 12: IRB Interfaces and VLANs
For additional information on IRB interfaces, see Understanding Integrated Routing and Bridging.

To configure VLANs and IRB interfaces:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   
   **Aggregation Device 1:**
   ```
   set groups IRB-VLANS when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups IRB-VLANS
   
   **Aggregation Device 2:**
   ```
   set apply-groups IRB-VLANS
   
   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Configure the extended port aggregated Ethernet interfaces into VLANs:

   **NOTE:** The aggregated Ethernet interfaces were configured in the previous section.

   ```
   set groups IRB-VLANS interfaces ae1 unit 0 family ethernet-switching vlan members 100
   set groups IRB-VLANS interfaces ae2 unit 0 family ethernet-switching vlan members 100
   set groups IRB-VLANS interfaces ae3 unit 0 family ethernet-switching vlan members 100
   set groups IRB-VLANS interfaces ae4 unit 0 family ethernet-switching vlan members 200
   set groups IRB-VLANS interfaces ae5 unit 0 family ethernet-switching vlan members 200
   set groups IRB-VLANS interfaces ae6 unit 0 family ethernet-switching vlan members 200
   ```

3. Create the VLANs by naming and numbering them:

   ```
   set groups IRB-VLANS vlans vlan100 vlan-id 100
   set groups IRB-VLANS vlans vlan200 vlan-id 200
   ```

4. Create the IRB interfaces and configure. Set an IPv4 and an IPv6 address for each IRB interface:

   **NOTE:** The IP address for an IRB interface must match on both aggregation devices in this topology. Do not assign separate IP addresses for the same IRB interface on different aggregation devices.
set groups IRB-VLANS interfaces irb unit 100 family inet address 10.1.1.1/24
set groups IRB-VLANS interfaces irb unit 100 family inet6 address 2001:db8:1::1/64
set groups IRB-VLANS interfaces irb unit 200 family inet address 10.2.2.1/24
set groups IRB-VLANS interfaces irb unit 200 family inet6 address 2001:db8:2::1/64

**NOTE:** Although typically recommended, the unit number for an IRB interface is arbitrary and does not have to match the VLAN ID number. We have configured the unit number to match the VLAN ID number in this topology to avoid confusion.

5. Bind the IRB interfaces to VLANs, and enable MAC synchronization for each VLAN:

   set groups IRB-VLANS vlans vlan100 l3-interface irb.100
   set groups IRB-VLANS vlans vlan200 l3-interface irb.200
   set groups IRB-VLANS vlans vlan100 mcae-mac-synchronize
   set groups IRB-VLANS vlans vlan200 mcae-mac-synchronize

6. After committing the configuration, confirm the VLANs are created and are associated with the correct interfaces.

   The output below confirms the interfaces that belong to vlan100:

   ```
   user@ad1-qfx10002> show vlans vlan100
   Routing instance  VLAN name      Tag   Interfaces
   default-switch    vlan100        100     ae1.0*
   ae2.0*
   ae3.0*
   ```

7. After committing the configuration, confirm that the IRB interface is processing traffic by checking the Input packets and Output packets counters.

   The output below confirms irb.100:

   ```
   user@ad1-qfx10002> show interfaces irb.100
   Logical interface irb.100 (Index 796) (SNMP ifIndex 940)
   Flags: Up SNMP-Traps 0x4004000 Encapsulation: ENET2
   Bandwidth: 1000mbps
   Routing Instance: default-switch Bridging Domain: vlan100
   Input packets : 28121476
   Output packets: 28437484
   Protocol inet, MTU: 1500
   Max nh cache: 75000, New hold nh limit: 75000, Curr nh cnt: 0, Curr new hold cnt: 0,
   NH drop cnt: 0
   Flags: Sendbcast-pkt-to-re
   Addresses, Flags: Is-Preferred Is-Primary
   Destination: 10.1.1/24, Local: 10.1.1.1, Broadcast: 10.1.1.255
   ```
Configuring OSPF

Step-by-Step Procedure
OSPF is a widely-adopted interior gateway protocol (IGP) that is used to route packets within a single area. OSPF is a mature, industry-standard routing protocol and the range of OSPF options is well beyond the scope of this document. For additional information on OSPF, see OSPF Feature Guide or OSPF Feature Guide for the QFX Series.

OSPF can be adopted as the routing protocol in the Enterprise Data Center solution. It can be used to exchange traffic with devices outside the Layer 2 topology presented in this solution architecture, such as non-data center devices in the Enterprise network, devices in a different data center, or devices that need to be reached over the Internet. Because the Enterprise Data Center solution is designed for private deployments where the Enterprise installing the data center also owns the upstream devices, an IGP using one autonomous system (AS) is often appropriate for the implementation.

OSPF is one routing protocol option for the Enterprise Data Center solution; BGP is another option. In general, OSPF is more appropriate in smaller scale environments with fewer routes and less need for routing policy control. In larger scale environments with more routes and more need for routing policy control, BGP is often the more appropriate routing protocol option. An Enterprise Data Center solution can run OSPF and BGP simultaneously in large scale setups or in scenarios where an IGP and an EGP are required.

In the Enterprise Data Center solution, OSPF is configured in a virtual routing instance (vr-10). Layer 3 multicast is also configured in this virtual routing instance. The MX480 router and the two QFX10002 switches all place interfaces into the OSPF backbone area (area 0).

NOTE: Multiple routing instances are configured in this topology over the same interfaces. Only one virtual routing instance is supported per interface. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGP, DHCP Relay, and PIM-SM that is appropriate for your networking requirements.

Figure 13 on page 64 illustrates the OSPF topology in this solution.

Figure 13: OSPF Topology

This configuration procedure shows how to enable OSPF on the devices in the Enterprise Data Center solution topology only. The purpose of OSPF is to enable connectivity to devices outside the data center, so the devices outside the data center topology must also enable OSPF support. The process for enabling OSPF on those devices is beyond the scope of this guide.
To configure OSPF for the Enterprise Data Center solution:

1. Configure the virtual routing instance on the MX480 router and both QFX10002 switches:
   
   **MX480 Router:**
   
   set routing-instances vr-10 instance-type virtual-router
   
   **QFX10002 Switch (Aggregation Device 1):**
   
   set routing-instances vr-10 instance-type virtual-router
   
   **QFX10002 Switch (Aggregation Device 2):**
   
   set routing-instances vr-10 instance-type virtual-router

2. Configure the IP address of the loopback interface:
   
   **MX480 Router:**
   
   set interfaces lo0 unit 10 family inet address 192.168.100.5
   
   **QFX10002 Switch (Aggregation Device 1):**
   
   set interfaces lo0 unit 10 family inet address 192.168.100.1
   
   **QFX10002 Switch (Aggregation Device 2):**
   
   set interfaces lo0 unit 10 family inet address 192.168.100.2

3. Configure a loopback interface into the routing instance on each device:
   
   **MX480 Router:**
   
   set routing-instances vr-10 interface lo0.10
   
   **QFX10002 Switch (Aggregation Device 1):**
   
   set routing-instances vr-10 interface lo0.10
   
   **QFX10002 Switch (Aggregation Device 2):**
   
   set routing-instances vr-10 interface lo0.10

4. Assign a router ID to each device participating in the OSPF network:
   
   **MX480 Router:**
   
   set routing-instances vr-10 routing-options router-id 192.168.100.5
   
   **QFX10002 Switch (Aggregation Device 1):**
   
   set routing-instances vr-10 routing-options router-id 192.168.100.1
   
   **QFX10002 Switch (Aggregation Device 2):**
**NOTE:** We recommend configuring the router ID as the IP address of the loopback addresses to simplify network management. The router ID can be any value and does not have to match the IP address of the loopback address.

5. Configure interfaces into OSPF.

The loopback interface is configured into OSPF as part of the procedure, and is enabled as a passive interface on each device.

**MX480 Router:***

```plaintext
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae101
```

**QFX10002 Switch (Aggregation Device 1):***

```plaintext
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100
```

**QFX10002 Switch (Aggregation Device 2):***

```plaintext
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100
```

6. After committing the configuration, verify that the OSPF state is full for all neighbor routers:

**MX480 Router:**

```plaintext
user@mx480-core-router> show ospf neighbor instance vr-10
Address          Interface   State   ID             Pri  Dead
10.0.1.100        ae100.0     Full    192.168.100.1   128    37
10.0.2.100        ae101.0     Full    192.168.100.2   128    34
```

Many other verification commands are available for OSPF. See [OSPF Feature Guide](#).

This configuration procedure shows how to enable OSPF on the devices in the Enterprise Data Center solution topology only. The purpose of OSPF is to enable connectivity to devices outside the data center, so the devices outside the data center topology must also configure OSPF support. The OSPF configuration of those devices is beyond the scope of this guide.
Configuring BGP

Step-by-Step Procedure
BGP is a widely-adopted exterior gateway protocol (EGP) that is used to route packets between autonomous systems (ASs). The range of eBGP options and behaviors are well beyond the scope of this document. For additional information on BGP, see the BGP Feature Guide.

The Enterprise Data Center solution can use external BGP (EBGP) to exchange traffic with devices outside the Layer 2 topology presented in this solution architecture, such as non-data center devices in the Enterprise network, devices in a different data center, or devices that need to be reached over the Internet.

EBGP is one routing protocol option for the Enterprise Data Center solution; OSPF is another option. In general, EBGP is often the more appropriate routing protocol option in larger scale environments with more routes and more need for routing policy control. OSPF is often the more appropriate routing protocol option in smaller scale environments with fewer routes and less need for routing policy control. One routing protocol is needed in most topologies, although this Enterprise Data Center solution can run OSPF and BGP simultaneously in large scale setups or in scenarios where both an IGP and an EGP are required.

In the Enterprise Data Center solution, EBGP is configured in a virtual routing instance. The QFX10002 switches in the topology are in AS 64500 and the MX480 router is in AS 64501. The MX480 router is an EBGP peer to each QFX10002 switch.

BGP is configured in virtual routing instance 20 (vr-20) on both QFX10002 switches and the MX480 core router. In addition to BGP, DHCP Relay is also running in the virtual routing instance. DHCP Relay configuration is covered in “Configuring DHCP Relay” on page 74.

NOTE: Multiple routing instances are configured in this topology over the same interfaces. Only one virtual routing instance is supported per interface. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGP, DHCP Relay, and PIM-SM that is appropriate for your networking requirements.

Figure 14 on page 68 illustrates the BGP topology in this solution.

Figure 14: EBGP Topology

This configuration procedure shows how to enable EBGP on the devices in the Enterprise Data Center solution topology only. The purpose of EBGP is to enable connectivity to devices outside the data center, so the devices outside the data center topology must
also enable EBGP support. The procedure to enable EBGP on those devices is beyond the scope of this guide.

To configure this EBGP implementation:

1. Obtain and download a BGP license for each QFX10002-72Q switch in this topology.
   For information about how to purchase software licenses, contact your Juniper Networks sales representative.
   To download a new license, see Adding New Licenses (CLI Procedure).
   A license is required to run BGP on the QFX10002-72Q switches in this topology only. A license is not required to run BGP on the MX480 Router used in this topology. See Software Feature Licenses

2. Configure the virtual routing instance on the MX480 router and both QFX10002 switches:
   **MX480 Router:**
   ```
   set routing-instances vr-20 instance-type virtual-router
   ```
   **QFX10002 Switch (Aggregation Device 1):**
   ```
   set routing-instances vr-20 instance-type virtual-router
   ```
   **QFX10002 Switch (Aggregation Device 2):**
   ```
   set routing-instances vr-20 instance-type virtual-router
   ```

3. Add the interfaces on each device that are participating in the virtual routing instance:
   **MX480 Router**
   ```
   set routing-instances vr-20 interface ae100.0
   set routing-instances vr-20 interface ae101.0
   ```
   **QFX10002 Switch (Aggregation Device 1):**
   ```
   set routing-instances vr-20 interface ae100.0
   ```
   **QFX10002 Switch (Aggregation Device 2):**
   ```
   set routing-instances vr-20 interface ae100.0
   ```

4. Create the EBGP group and specify the type, peer AS, local AS, and neighbor device parameter for all devices:
   **MX480 Router:**
   ```
   set routing-instances vr-20 protocols bgp group ebgp-20 type external
   set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64501
   set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64500
   set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.1.100
   set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.2.100
   ```
QFX10002 Switch (Aggregation Device 1):

```plaintext
set routing-instances vr-20 protocols bgp group ebgp-20 type external
set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64500
set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64501
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.1.1
```

QFX10002 Switch (Aggregation Device 2):

```plaintext
set routing-instances vr-20 protocols bgp group ebgp-20 type external
set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64500
set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64501
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.2.1
```

5. After the configurations are committed on the MX480 router and both QFX10002 switches, confirm the BGP neighbor relationships have formed by entering the `show bgp neighbor instance` command on any device.

The sample below provides this output for the QFX10002 switch acting as aggregation device 1:

```plaintext
user@ad1-qfx10002> show bgp neighbor instance vr-20
Peer: 10.0.1.1 AS 64501 Local: 10.0.1.100 AS 64500
  Group: ebgp-20   Routing-Instance: vr-20
  Forwarding routing-instance: vr-20
  Type: External   State: Established   Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  ...
  ...
  (output removed for brevity)
  Last traffic (seconds): Received 84701 Sent 84493 Checked 84701
  Input messages: Total 2912 Updates 1 Refreshes 0 Octets 55376
  Output messages: Total 2941 Updates 0 Refreshes 0 Octets 55921
  Output Queue[1]: 0 (vr-20.inet.0, inet-unicast)
```

The output confirms the correct BGP group and virtual routing instance, and that BGP traffic is being sent and received on the switch.

6. After the configurations are committed on the MX480 router and both QFX10002 switches, confirm that the BGP state is established and that BGP traffic is being sent and received on the device by entering the `show bgp summary group ebgp-20`

```plaintext
user@ad1-qfx10002> show bgp summary group ebgp-20
Groups: 1 Peers: 1 Down peers: 0
  Peer   AS  InPkt OutPkt OutQ Flaps Last Up/Dwn State #Active/Received/Accepted/Damped
  10.0.1.1 64501 2912 2941 0 0 23:28:17 Establ vr-20.inet.0: 0/0/0/0
```

The output confirms that the BGP state is established and that input and output packets are being sent and received.
Configuring Class of Service

Step-by-Step Procedure
Class of service (CoS) enables you to divide traffic into classes and set various levels of throughput and packet loss when congestion occurs. You have greater control over packet loss because you can configure rules tailored to your needs.

For additional information on CoS in a Junos Fusion Data Center, see Understanding CoS in Junos Fusion Data Center.

In the Enterprise Data Center solution, one classifier with four output queues is created to manage incoming traffic congestion from the servers connected to access interfaces. Each output queue has its own low, medium-high, and high loss priority flows to manage traffic in the event of congestion. The classifier is attached to the aggregated Ethernet interfaces that connect the server to the extended ports—the access interfaces—on the satellite devices.

This configuration procedure shows how to configure the classifier only. The configuration of service levels is not covered.

The CoS classifier used in this Solutions Guide is simple and provides an illustration of how a CoS classifier may be configured in an Enterprise Data Center. Juniper Networks offer many CoS configuration options for its data center products, and covering all of them is beyond the scope of this Solutions Guide. For information on other CoS configuration options, see Configuring CoS in Junos Fusion Data Center.

To configure the CoS classifier for the Enterprise Data Center solution:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:
   
   **Aggregation Device 1:**
   ```
   set groups COS when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups COS
   ```

   **Aggregation Device 2:**
   ```
   set apply-groups COS
   ```
   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Configure all four forwarding classes, setting the loss priorities for each class:
   
   **Aggregation Device 1 or 2:**
   ```
   set groups COS class-of-service classifiers dscp dscp_classifier
   forwarding-class fc0 loss-priority low code-points 000010
   set groups COS class-of-service classifiers dscp dscp_classifier
   forwarding-class fc0 loss-priority medium-high code-points 000110
   set groups COS class-of-service classifiers dscp dscp_classifier
   forwarding-class fc0 loss-priority high code-points 001110

   set groups COS class-of-service classifiers dscp dscp_classifier
   forwarding-class fc1 loss-priority low code-points 000100
   set groups COS class-of-service classifiers dscp dscp_classifier
   forwarding-class fc1 loss-priority medium-high code-points 011100
   ```
set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc1 loss-priority high code-points 011110

set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc2 loss-priority low code-points 011000
set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc2 loss-priority medium-high code-points 100100
set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc2 loss-priority high code-points 101110

set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc3 loss-priority low code-points 110000
set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc3 loss-priority medium-high code-points 110100
set groups COS class-of-service classifiers dscp dscp_classifier
forwarding-class fc3 loss-priority high code-points 110110

3. Assign each forwarding class to a queue number:

   Aggregation Device 1 or 2:

   set groups COS class-of-service forwarding-classes class fc0 queue-num 0
   set groups COS class-of-service forwarding-classes class fc1 queue-num 1
   set groups COS class-of-service forwarding-classes class fc2 queue-num 2
   set groups COS class-of-service forwarding-classes class fc3 queue-num 3

4. Assign the classifiers to the aggregated Ethernet interfaces:

   set groups COS class-of-service interfaces ae1 unit 0 classifiers dscp
dscp_classifier
   set groups COS class-of-service interfaces ae2 unit 0 classifiers dscp
dscp_classifier
   set groups COS class-of-service interfaces ae3 unit 0 classifiers dscp
dscp_classifier
   set groups COS class-of-service interfaces ae4 unit 0 classifiers dscp
dscp_classifier
   set groups COS class-of-service interfaces ae5 unit 0 classifiers dscp
dscp_classifier
   set groups COS class-of-service interfaces ae6 unit 0 classifiers dscp
dscp_classifier

5. This configuration procedure shows how to configure the classifier only. The
   configuration of service levels is not covered.

   For information on other CoS configuration options, see Configuring CoS in Junos Fusion
   Data Center.
Configuring DHCP Relay

Step-by-Step Procedure
You can configure a Junos Fusion Data Center to act as a Dynamic Host Configuration Protocol (DHCP) relay agent. This means that if a Junos Fusion Data Center receives a broadcast DHCP request from a locally attached host (client), it relays the message to the specified DHCP server.

For additional information on DHCP Relay, see DHCP and BOOTP Relay Overview.

In the Enterprise Data Center solution, DHCP Relay is enabled in a virtual routing instance to relay DHCP requests that originate from hosts in the routing instance to the DHCP server or servers in the server group. Both the server and the host in this configuration are attached to extended port interfaces—the access interfaces on the QFX5100 and EX4300 switches acting as satellite devices—so the DHCP request is relayed across the Junos Fusion Data Center topology.

**NOTE:** Multiple routing instances are configured in this topology over the same interfaces. Only one virtual routing instance is supported per interface. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBG, DHCP Relay, and PIM-SM that is appropriate for your networking requirements.

To enable the DHCP Relay configuration for the Enterprise Data Center solution:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**
   ```
   set groups DHCP-RELAY when peers [ad1-qfx10002 ad2-qfx10002] apply-groups DHCP-RELAY
   ```

   **Aggregation Device 2:**
   ```
   set apply-groups DHCP-RELAY
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Configure the routing instance, name the server group, and specify the IP address of the DHCP server by configuring the DHCP Relay server group.

   ```
   set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay server-group sg1 203.0.113.1
   ```

3. Create and name a client group within the active server group. Configure the DHCP Relay server group as the active server group for the client group:

   ```
   set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay group client1 active-server-group sg1
   ```

4. Associate the client group with the virtual routing instance.
5. Associate the client group with an IRB interface.

```
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay
    group client1 forward-only routing-instance vr-20
```

6. After committing the configuration, confirm that DHCP Relay packets are being sent and received:

```
user@ad1-qfx10002> show dhcp relay statistics
Packets dropped:
    Total                      0

Messages received:
    BOOTREQUEST               168
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPREQUEST               168
    DHCPLEASEACTIVE           0
    DHCPLEASEUNASSIGNED       0
    DHCPLEASEUNKNOWN          0
    DHCPLEASEQUERYDONE        0

Messages sent:
    BOOTREPLY                 75
    DHCPOFFER                  0
    DHCPACK                    75
    DHCPNAK                    0
    DHCPFORCERENEW             0
    DHCPLEASEQUERY             0
    DHCPBULKLEASEQUERY         0

Packets forwarded:
    Total                      243
    BOOTREQUEST               168
    BOOTREPLY                 75
```
Configuring Layer 3 Multicast

Multicast traffic is traffic that is sent from one source to many receivers. See Multicast Overview for additional information on multicast.

Layer 3 multicast is enabled in the Enterprise Data Center solution within a virtual routing instance. The virtual routing instance—vr-10—was used earlier in this guide to enable OSPF. This procedure assumes the virtual routing instance and loopback address were created as part of the OSPF configuration procedure. See the “Configuring OSPF” on page 63 for the steps required to configure the virtual routing instance and the loopback address, if needed.

The topology in the solution implements multicast using Protocol Independent Multicast sparse-mode (PIM-SM). The MX480 router acts as the rendezvous point (RP) in the PIM-SM configuration. All interfaces on the MX480 router and both QFX10002 switches are enabled to support PIM-SM.

NOTE: Multiple routing instances are configured in this topology over the same interfaces. Only one virtual routing instance is supported per interface. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGP, DHCP Relay, and PIM-SM that is appropriate for your networking requirements.

See Understanding PIM Sparse Mode for additional information on PIM-SM.

To enable Layer 3 Multicast in a virtual routing instance for the Enterprise Data Center solution:

1. Configure the virtual routing instance on the MX480 router and both QFX10002 switches:

   **MX480 Router:**
   ```
   set routing-instances vr-10 instance-type virtual-router
   ```

   **QFX10002 Switch (Aggregation Device 1):**
   ```
   set routing-instances vr-10 instance-type virtual-router
   ```

   **QFX10002 Switch (Aggregation Device 2):**
   ```
   set routing-instances vr-10 instance-type virtual-router
   ```

2. Configure the MX480 router as the rendezvous point (RP), and enable PIM-SM on all interfaces on the MX480 router in the routing instance:

   **MX480 Router:**
   ```
   set routing-instances vr-10 protocols pim rp local address 192.168.100.5
   set routing-instances vr-10 protocols pim interface all mode sparse
   ```
3. Configure the non-RP devices, which are both QFX10002 switches in this topology:

   **QFX10002 Switch (Aggregation Device 1):**

   ```
   set routing-instances vr-10 protocols pim rp static address 192.168.100.5
   set routing-instances vr-10 protocols pim interface all mode sparse
   ```

   **QFX10002 Switch (Aggregation Device 2):**

   ```
   set routing-instances vr-10 protocols pim rp static address 192.168.100.5
   set routing-instances vr-10 protocols pim interface all mode sparse
   ```

   **NOTE:** This configuration assumes the interfaces for the virtual routing instance and the loopback addresses are already created. See the “Configuring OSPF” on page 63 for the steps required to configure the virtual routing instance and the loopback address.

   All interfaces in the virtual routing instance participate in the PIM-SM topology once this configuration is committed.

4. After committing the configuration, confirm that PIM is operational.

   **QFX10002 Switch (Aggregation Device 1):**

   ```
   user@ad1-qfx10002> show pim neighbors instance vr-10
   B = Bidirectional Capable, G = Generation Identifier
   H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
   P = Hello Option DR Priority, T = Tracking Bit
   Instance: PIM.vr10
   Interface     IP  V Mode Option Option         Uptime Neighbor addr
    ae100         4 2   HPLGT          02:47:26 192.168.100.5
Configuring IGMP Snooping to Manage Multicast Flooding on VLANs

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on a VLAN by monitoring IGMP messages and only forwarding multicast traffic to interested receivers. For more information on IGMP snooping, see Configuring IGMP Snooping (CLI Procedure).

In the Enterprise Data Center Solution, IGMP snooping is enabled to constrain IPv4 multicast traffic flooding in the Layer 2 VLANs when PIM is enabled. The VLANs include the aggregated Ethernet interface on each QFX10002 switch connecting to the MX480 router (the multicast router interface) as well as multiple access interfaces that connect to the topology using the extended ports on the satellite devices.

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**
   ```
   set groups IGMP-SNOOPING when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups IGMP-SNOOPING
   ```

   **Aggregation Device 2:**
   ```
   set apply-groups IGMP-SNOOPING
   ```

   This procedure assumes commitment synchronization is configured. See "Configuring Commit Synchronization Between Aggregation Devices" on page 20.

2. On the aggregation devices, enable IGMP snooping and configure an interface in the VLAN as a static multicast router interface:

   **QFX10002 Switch (Aggregation Device 1 or 2):**
   ```
   set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae100.0 multicast-router-interface
   ```

3. Enable IGMP snooping on access interfaces in the VLAN:

   ```
   set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae1.0
   set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae2.0
   set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae3.0
   ```

4. After committing the configuration, confirm that IGMP snooping is enabled:

   ```
   user@ad1-qfx10002> show igmp snooping membership
   Instance: default-switch
   Vlan: vlan100
   ```
Configuring VLAN Autosense

Step-by-Step Procedure

VLAN autosense gives extended ports in a Junos Fusion Data Center—the access interfaces on the satellite devices—the ability to add themselves to a VLAN in cases when traffic is traversing the interface that belongs to a VLAN that is not currently assigned to the interface. For instance, if extended port ge-101/0/1 was not part of VLAN 102 but received traffic destined for VLAN 102, port ge-101/0/1 would automatically add itself as a member of VLAN 102 if VLAN autosense was enabled.

VLAN autosense is enabled on interface ae1 in the Enterprise Data Center topology.

To enable VLAN autosense for the Enterprise Data Center topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   Aggregation Device 1:

   set groups VLAN-AUTOSENSE when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups VLAN-AUTOSENSE

   Aggregation Device 2:

   set apply-groups VLAN-AUTOSENSE

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Enable VLAN autosense:

   set groups VLAN-AUTOSENSE interfaces ae1 unit 0 family ethernet-switching vlan-auto-sense
Configuring Layer 2 Loop Detection and Prevention for Extended Ports in a Junos Fusion

Loop detection is a lightweight Layer 2 protocol that can be enabled on all extended ports—in this topology, the extended ports are the access ports on the EX4300 and QFX5100 satellite devices—in a Junos Fusion.

When loop detection is enabled on an extended port, the port periodically transmits a Layer 2 multicast packet with a user-defined MAC address. If the packet is received on an extended port interface in the Junos Fusion topology, the ingress interface is logically shut down and a loop detect error is flagged. If a loop is created between two extended ports, both interfaces receive the packets transmitted from the other interface, and both ports are shut down. Manual intervention is required to bring the interfaces back online.

Loop detection is useful for detecting accidental loops caused by faulty wiring or by VLAN configuration errors. Loop detection is useful in this solution for detecting these and other errors in a low overhead manner, since loop detection and prevention only requires the periodic transmission of a small packet for operation and not the full overhead of other loop detection protocols like STP.

See Understanding Loop Detection and Prevention on a Junos Fusion and Configuring Loop Detection in a Junos Fusion for additional overview and configuration information on loop detection and prevention in a Junos Fusion topology.

In the Enterprise Data Center topology, loop detection is enabled on all extended ports and a loop detection packet is transmitted at the default interval of every 30 seconds.

To enable loop detection for the Enterprise Data Center topology:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:
   
   **Aggregation Device 1:**
   
   set groups LOOP-DETECTION when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups LOOP-DETECTION

   **Aggregation Device 2:**
   
   set apply-groups LOOP-DETECTION

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Enable loop detection on all extended ports:
   
   **Aggregation Device 1 or 2:**
   
   set groups LOOP-DETECTION protocols loop-detect interface all-extended-ports

3. Specify the MAC address to use in the loop detection packet:
   
   **Aggregation Device 1 or 2:**
set groups LOOP-DETECTION protocols loop-detect destination-mac 00:00:5E:00:53:AA

4. After committing the configuration, confirm that loop detection is enabled:

   user@ad1-qfx10002> show loop-detect interface
   Interface Parent-Interface  State
   ge-100/0/0 -            UP
   ge-100/0/1 -            UP
   ge-100/0/2 -            UP
   ....(additional output removed for brevity)

### Configuring LLDP

**Step-by-Step Procedure**

Juniper Networks devices use Link Layer Discovery Protocol (LLDP) to learn and distribute device information on network links. The information allows a Juniper Networks device to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

In the Enterprise Data Center solution architecture, LLDP is enabled on all satellite device and aggregation device interfaces.

To configure LLDP for the Enterprise Data Center solution:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:
   
   **Aggregation Device 1:**
   
   set groups LLDP when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups LLDP

   **Aggregation Device 2:**
   
   set apply-groups LLDP

   This procedure assumes commitment synchronization is configured. See "Configuring Commit Synchronization Between Aggregation Devices" on page 20.

2. Enable LLDP on all extended port interfaces:
   
   **Aggregation Device 1 or 2:**
   
   set groups LLDP protocols lldp interface all

3. After committing the configuration, enter the `show lldp` command to confirm that LLDP is enabled:

   user@ad1-qfx10002> show lldp
   LLDP                          : Enabled
   Advertisement interval     : 30 seconds
   Transmit delay             : 2 seconds
   Hold timer                 : 120 seconds
   Notification interval     : 5 Second(s)
Configuring a Firewall Filter

Firewall filters provide rules that define whether to accept or discard packets that are transiting an interface or VLAN, as well as actions to perform on packets that are accepted on the interface or VLAN.

Comprehensive coverage of firewall filter implementation options and behaviors is beyond the scope of this document. For additional information on firewall filters, see Overview of Firewall Filters.

In the Enterprise Data Center solution topology, a simple firewall filter used to count packets from a specific MAC address received in VLAN 100 are counted.

For information on other firewall filter configuration options, see Configuring Firewall Filters.

To configure this basic firewall filter:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   Aggregation Device 1:
   
   set groups FIREWALL-FILTER when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups FIREWALL-FILTER

   Aggregation Device 2:
   
   set apply-groups FIREWALL-FILTER

   This procedure assumes commitment synchronization is configured. See "Configuring Commit Synchronization Between Aggregation Devices" on page 20.

2. Create a firewall filter match condition to identify traffic.

   In this topology, all traffic from source MAC address 00:00:5E:00:53:00 is accepted and counted.

   Aggregation Device 1 or 2:
   
   set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1
   term source-mac-0053000 from source-mac-address 00:00:5E:00:53:00

3. Specify the action to take on matching traffic.

   ————
In this topology, matching traffic is accepted and counted:

**Aggregation Device 1 or 2:**

```plaintext
set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1
   term source-mac-005300 then accept
set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1
   term source-mac-005300 then count source-mac-count
```

4. Apply the filter to a VLAN:

**Aggregation Device 1 or 2:**

```plaintext
set groups FIREWALL-FILTER vlans vlan100 forwarding-options filter input
   filter1
```

5. After committing the configuration, verify that the firewall filter is accepting and counting traffic.

The firewall filter counters in the `show firewall` output only display firewall filter statistics from one of the aggregation devices due to how traffic is load balanced in a Junos Fusion topology. The other aggregation device always displays 0 bytes and 0 packets filtered by the firewall.

In the output below, the firewall filter statistics in the `show firewall` output are visible from aggregation device 2 only.

**Aggregation Device 1:**

```
user@ad1-qfx10002> show firewall
Filter: __default_bpdu_filter__

Filter: filter1
Counters:
  Name           Bytes   Packets
  source-mac-count      0        0
```

**Aggregation Device 2:**

```
user@ad2-qfx10002> show firewall
Filter: __default_bpdu_filter__

Filter: filter1
Counters:
  Name           Bytes   Packets
  source-mac-count  66504     489
```
Configuring SNMP

SNMP enables the monitoring of network devices from a central location using a network management system (NMS). For additional information on SNMP, see Understanding the Implementation of SNMP.

This document shows how to enable SNMP on the aggregation devices in the Enterprise Data Center solution only. The solution supports SNMP version 2 (SNMPv2). A complete SNMP implementation that includes selection and configuration of the NMS is beyond the scope of this document. See Configuring SNMP.

To configure SNMP from the aggregation devices:

1. Create the configuration group and ensure the configuration group is applied on both aggregation devices:

   **Aggregation Device 1:**
   ```
   set groups SNMP when peers [ad1-qfx10002 ad2-qfx10002]
   set apply-groups SNMP
   ```

   **Aggregation Device 2:**
   ```
   set apply-groups SNMP
   ```

   This procedure assumes commitment synchronization is configured. See “Configuring Commit Synchronization Between Aggregation Devices” on page 20.

2. Enable SNMP:

   **Aggregation Device 1 or 2:**
   ```
   set groups SNMP system processes snmp enable
   ```

3. Specify the physical location of the system:

   **Aggregation Device 1 or 2:**
   ```
   set groups SNMP snmp location "Enterprise Data Center 1"
   ```

4. Specify an administrative contact for the SNMP system:

   **Aggregation Device 1 or 2:**
   ```
   set groups SNMP snmp contact "Jane Doe"
   ```

5. Specify an SNMP interface:

   **Aggregation Device 1 or 2:**
   ```
   set groups SNMP snmp interface em1.0
   ```

6. Specify an SNMP community name for the read-only authorization level.

   **Aggregation Device 1 or 2:**
set groups SNMP snmp community public authorization read-only

7. Specify an SNMP community name for the read-write authorization level.
   Aggregation Device 1 or 2:
   set groups SNMP snmp community private authorization read-write

8. Configure a trap group and a target to receive the SNMP traps.
   Aggregation Device 1 or 2:
   set groups SNMP snmp trap-group space targets 203.0.113.251

9. After committing the configuration, confirm SNMP messages are being transmitted and received:

   user@ad1-qfx10002> show snmp statistics
   SNMP statistics:
   Input:
   Packets: 1331899, Bad versions: 0, Bad community names: 0,
   Bad community uses: 0, ASN parse errors: 0,
   Too bigs: 0, No such names: 0, Bad values: 0,
   Read onlys: 0, General errors: 0,
   Total request varbinds: 6512218, Total set varbinds: 0,
   Get requests: 4, Get nexts: 183360, Set requests: 0,
   Get responses: 0, Traps: 0,
   Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
   Throttle drops: 0, Duplicate request drops: 0
   (some output removed for brevity)

   Output:
   Packets: 1351583, Too bigs: 0, No such names: 0,
   Bad values: 0, General errors: 0,
   Get requests: 0, Get nexts: 0, Set requests: 0,
   Get responses: 1331899, Traps: 19684

   Performance:
   Average response time(ms): 1.21
   Number of requests dispatched to subagents in last:
   1 minute:0, 5 minutes:7266, 15 minutes:59250
   Number of responses dispatched to NMS in last:
   1 minute:0, 5 minutes:7266, 15 minutes:59250

Related Documentation
- Understanding the Enterprise Data Center Solution on page 5
Appendix: Enterprise Data Center Solution Complete Configuration

This appendix provides the complete configuration of the Enterprise Data Center topology provided in this guide.

The optional procedures in the step-by-step procedures as well as the steps to commit the configuration are not included in this appendix. Procedures that can be performed on either aggregation device and synchronized to the other aggregation device are always done on aggregation device 1.

To quickly configure a device using the CLI configuration in this appendix: copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

The appendix is annotated for readability. The annotated text is ignored by the CLI if entered into a device so it can safely be copied and pasted into a CLI session.

**NOTE:** Multiple routing instances are configured in this appendix over the same interfaces. Only one virtual routing instance can be configured on an interface. In your deployment, create one virtual routing instance that includes the combination of OSPF, EBGp, DHCP Relay, and PIM-SM that is appropriate for your networking requirements.

**MX480 Router (mx480-core-router):**

```text
### Aggregated Ethernet Interfaces to QFX10002-72Q AD1 & QFX10002-72Q AD2 ###
set chassis aggregated-devices ethernet device-count 1000
set interfaces ae100 description "ae to AD1-QFX10002"
set interfaces ae101 description "ae to AD2-QFX10002"
set interfaces et-3/2/0 ether-options 802.3ad ae100
set interfaces et-3/2/1 ether-options 802.3ad ae100
set interfaces et-3/2/2 ether-options 802.3ad ae100
set interfaces et-4/2/0 ether-options 802.3ad ae100
set interfaces et-4/2/1 ether-options 802.3ad ae100
set interfaces et-4/2/2 ether-options 802.3ad ae100
set interfaces et-3/3/0 ether-options 802.3ad ae101
set interfaces et-3/3/1 ether-options 802.3ad ae101
set interfaces et-3/3/2 ether-options 802.3ad ae101
set interfaces et-4/3/0 ether-options 802.3ad ae101
set interfaces et-4/3/1 ether-options 802.3ad ae101
set interfaces et-4/3/2 ether-options 802.3ad ae101
set interfaces ae100 unit 0 family inet address 10.0.1.1/24
set interfaces ae101 unit 0 family inet address 10.0.2.1/24
set interfaces ae100 aggregated-ether-options lacp active
set interfaces ae101 aggregated-ether-options lacp active
set interfaces ae100 aggregated-ether-options lacp periodic fast
set interfaces ae101 aggregated-ether-options lacp periodic fast

### OSPF ###
set routing-instances vr-10 instance-type virtual-router
```
set interfaces lo0 unit 10 family inet address 192.168.100.5
set routing-instances vr-10 interface lo0.10
set routing-instances vr-10 routing-options router-id 192.168.100.5
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae101

### BGP ###
set routing-instances vr-20 instance-type virtual-router
set routing-instances vr-20 interface ae100.0
set routing-instances vr-20 interface ae101.0
set routing-instances vr-20 protocols bgp group ebgp-20 type external
set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64501
set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64500
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.1.100
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.2.100

### Layer 3 Multicast ###
set routing-instances vr-10 instance-type virtual-router
set routing-instances vr-10 protocols pim rp local address 192.168.100.5
set routing-instances vr-10 protocols pim interface all mode sparse

Aggregation Device 1 (ad1-qfx10002):

---

WARNING: The password password is used in the commit synchronization configuration procedure for illustrative purposes only. Use a more secure password in your device configuration.

---

### Commit Synchronization ###
set system commit peers-synchronize
set system commit peers ad2-qfx10002 user root authentication password
set system services netconf ssh

### Aggregated Ethernet Interface to MX480 Core Layer Router ###
set groups AE-ROUTER-ADSWITCHES when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups AE-ROUTER-ADSWITCHES
set groups AE-ROUTER-ADSWITCHES chassis aggregated-devices ethernet device-count 1000
set groups AE-ROUTER-ADSWITCHES interfaces ae100 description "ae to CORE-ROUTER-MX480"
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/66 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/67 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/68 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/69 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/70 ether-options 802.3ad ae100
set groups AE-ROUTER-ADSWITCHES interfaces et-0/0/71 ether-options 802.3ad ae100
set interfaces ae100 unit 0 family inet address 10.0.1.100/24
set groups AE-ROUTER-ADSWITCHES interfaces ae100 aggregated-ether-options lacp active
set groups AE-ROUTER-ADSWITCHES interfaces ae100 aggregated-ether-options lacp periodic fast

### FPC ID and Satellite Device Alias Assignment ###
set groups FUSION-FPC-CASCADE-ALIAS when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups FUSION-FPC-CASCADE-ALIAS
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 100 cascade-ports et-0/0/0
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 100 alias qfx5100-sd100
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 101 cascade-ports et-0/0/1
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 101 alias qfx5100-sd101
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 102 cascade-ports et-0/0/2
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 102 alias qfx5100-sd102
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 103 cascade-ports et-0/0/3
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 103 alias qfx5100-sd103
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 104 cascade-ports et-0/0/4
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 104 alias qfx5100-sd104
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 105 cascade-ports et-0/0/5
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 105 alias qfx5100-sd105
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 106 cascade-ports et-0/0/6
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 106 alias qfx5100-sd106
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 107 cascade-ports et-0/0/7
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 107 alias qfx5100-sd107
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 108 cascade-ports et-0/0/8
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 108 alias qfx5100-sd108
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 109 cascade-ports et-0/0/9
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 109 alias qfx5100-sd109
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 110 cascade-ports et-0/0/10
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 110 alias qfx5100-sd110
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 111 cascade-ports et-0/0/11
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 111 alias qfx5100-sd111
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 112 cascade-ports et-0/0/12
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 112 alias qfx5100-sd112
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 113 cascade-ports et-0/0/13
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 113 alias qfx5100-sd113
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 114 cascade-ports et-0/0/14
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 114 alias qfx5100-sd114
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 115
cascade-ports et-0/0/15
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 115 alias
qfx5100-sd115
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 116
cascade-ports et-0/0/16
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 116 alias
qfx5100-sd116
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 117
cascade-ports et-0/0/17
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 117 alias
qfx5100-sd117
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 118
cascade-ports et-0/0/18
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 118 alias
qfx5100-sd118
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 119
cascade-ports et-0/0/19
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 119 alias
qfx5100-sd119
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 120
cascade-ports et-0/0/20
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 120 alias
qfx5100-sd120
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 121
cascade-ports et-0/0/21
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 121 alias
qfx5100-sd121
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 122
cascade-ports et-0/0/22
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 122 alias
qfx5100-sd122
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 123
cascade-ports et-0/0/23
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 123 alias
qfx5100-sd123
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 124
cascade-ports et-0/0/24
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 124 alias
qfx5100-sd124
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 125
cascade-ports et-0/0/25
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 125 alias
qfx5100-sd125
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 126
cascade-ports et-0/0/26
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 126 alias
qfx5100-sd126
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 127
cascade-ports et-0/0/27
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 127 alias
qfx5100-sd127
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 128
cascade-ports et-0/0/28
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 128 alias
qfx5100-sd128
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 129
cascade-ports et-0/0/29
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 129 alias
qfx5100-sd129
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 130
cascade-ports et-0/0/30
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 130 alias qfx5100-sd130
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 131 alias qfx5100-sd131
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 131 alias qfx5100-sd131
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 132 alias qfx5100-sd132
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 132 alias qfx5100-sd132
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 133 alias qfx5100-sd133
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 133 alias qfx5100-sd133
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 134 alias qfx5100-sd134
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 134 alias qfx5100-sd134
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 135 alias qfx5100-sd135
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 135 alias qfx5100-sd135
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 136 alias qfx5100-sd136
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 136 alias qfx5100-sd136
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 137 alias qfx5100-sd137
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 137 alias qfx5100-sd137
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 138 alias qfx5100-sd138
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 138 alias qfx5100-sd138
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 139 alias qfx5100-sd139
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 139 alias qfx5100-sd139
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 140 alias ex4300-sd140
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 140 alias ex4300-sd140
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 141 alias ex4300-sd141
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 141 alias ex4300-sd141
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 142 alias ex4300-sd142
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 142 alias ex4300-sd142
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 143 alias ex4300-sd143
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 143 alias ex4300-sd143
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 144 alias ex4300-sd144
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 144 alias ex4300-sd144
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 145 alias ex4300-sd145
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 145 alias ex4300-sd145
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 145 alias ex4300-sd145
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 146 cascade-ports et-0/0/46
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 146 alias ex4300-sd146
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 147 cascade-ports et-0/0/47
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 147 alias ex4300-sd147
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 148 cascade-ports et-0/0/48
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 148 alias ex4300-sd148
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 149 cascade-ports et-0/0/49
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 149 alias ex4300-sd149
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 150 cascade-ports et-0/0/50
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 150 alias ex4300-sd150
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 151 cascade-ports et-0/0/51
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 151 alias ex4300-sd151
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 152 cascade-ports et-0/0/52
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 152 alias ex4300-sd152
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 153 cascade-ports et-0/0/53
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 153 alias ex4300-sd153
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 154 cascade-ports et-0/0/54
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 154 alias ex4300-sd154
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 155 cascade-ports et-0/0/55
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 155 alias ex4300-sd155
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 156 cascade-ports et-0/0/56
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 156 alias ex4300-sd156
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 157 cascade-ports et-0/0/57:0
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 157 alias ex4300-sd157
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 158 cascade-ports et-0/0/57:1
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 158 alias ex4300-sd158
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 159 cascade-ports et-0/0/57:2
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 159 alias ex4300-sd159
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 160 cascade-ports et-0/0/57:3
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 160 alias ex4300-sd160
ex4300-sd160
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161
cascade-ports et-0/0/58
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161
cascade-ports et-0/0/59
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 161 alias
ex4300-sd161
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162
cascade-ports et-0/0/60
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162
cascade-ports et-0/0/61
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 162 alias
ex4300-sd162
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163
cascade-ports et-0/0/62
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163
cascade-ports et-0/0/63
set groups FUSION-FPC-CASCADE-ALIAS chassis satellite-management fpc 163 alias
ex4300-sd163

### Cascade Port Conversion ###
set groups FUSION-FPC-CASCADE-ALIAS when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups FUSION-FPC-CASCADE-ALIAS
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/0 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/1 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/2 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/3 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/4 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/5 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/6 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/7 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/8 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/9 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/10 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/11 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/12 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/13 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/14 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/15 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/16 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/17 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/18 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/19 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/20 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/21 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/22 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/23 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/24 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/25 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/26 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/27 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/28 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/29 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/30 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/31 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/32 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/33 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/34 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/35 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/36 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/37 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/38 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/39 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/40 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/41 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/42 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/43 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/44 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/45 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/46 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/47 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/48 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/49 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/50 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/51 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/52 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/53 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/54 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/55 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/56 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:0 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:1 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:2 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/57:3 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/58 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/59 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/60 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/61 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/62 cascade-port
set groups FUSION-FPC-CASCADE-ALIAS interfaces et-0/0/63 cascade-port

### ICL Aggregated Ethernet Interfaces ###
set groups ICL-CONFIG when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups ICL-CONFIG
set groups ICL-CONFIG chassis aggregated-devices ethernet device-count 1000
set groups ICL-CONFIG interfaces ae999 description icl-link
set groups ICL-CONFIG interfaces et-0/0/64 ether-options 802.3ad ae999
set groups ICL-CONFIG interfaces et-0/0/65 ether-options 802.3ad ae999
set groups ICL-CONFIG interfaces ae999 aggregated-ether-options lacp active
set groups ICL-CONFIG interfaces ae999 aggregated-ether-options lacp periodic fast
set groups ICL-CONFIG interfaces ae999 unit 0 family ethernet-switching
interface-mode trunk
set groups ICL-CONFIG interfaces ae999 unit 0 family ethernet-switching vlan
members all

### Dual Aggregation Devices ###
set groups DUAL-AD-CONFIG when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups DUAL-AD-CONFIG
delete chassis satellite-management single-home
set groups DUAL-AD-CONFIG chassis satellite-management redundancy-groups rgl
redundancy-group-id 1
set groups DUAL-AD-CONFIG chassis satellite-management redundancy-groups rgl
satellite all
set chassis satellite-management redundancy-groups chassis-id 1
set chassis satellite-management redundancy-groups rgl peer-chassis-id 2
inter-chassis-link ae999

### BFD over ICL ###
set chassis satellite-management redundancy-groups rgl redundancy-group-id 1
peer-chassis-id 2 liveness-detection minimum-interval 2000
set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1
peer-chassis-id 2 liveness-detection multiplier 3
set chassis satellite-management redundancy-groups rg1 redundancy-group-id 1
peer-chassis-id 2 liveness-detection transmit-interval minimum-interval 2000

### Automatic Satellite Device Conversion ###
set groups AUTO-SAT-CONV when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups AUTO-SAT-CONV
set groups AUTO-SAT-CONV chassis satellite-management auto-satellite-conversion satellite all

### Satellite Software Upgrade Groups ###
set groups SAT-SW-UPGRADE when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups SAT-SW-UPGRADE
set groups SAT-SW-UPGRADE chassis satellite-management upgrade-groups qfx5100-sd satellite 100-139
set groups SAT-SW-UPGRADE chassis satellite-management upgrade-groups ex4300-sd satellite 140-163

### Uplink Port Pinning ###
set groups UPLINK_PIN when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups UPLINK_PIN
set groups UPLINK_PIN policy-options satellite-policies port-group-alias extended-port47 pic 0 port 47
set groups UPLINK_PIN policy-options satellite-policies port-group-alias uplink-port1 pic 1 port 0
set groups UPLINK_PIN policy-options satellite-policies forwarding-policy uplink-port-policy-port47-to-port0 port-group-extended extended-port1 port-group-uplink uplink-port1
set groups UPLINK_PIN chassis satellite-management fpc 162 forwarding-policy uplink-port-policy-port47-to-port0
set groups UPLINK_PIN chassis satellite-management fpc 163 forwarding-policy uplink-port-policy-port47-to-port0

### Uplink Failure Detection ###
set groups UFD when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups UFD
set groups UFD chassis satellite-management uplink-failure-detection

### Access Interface Aggregated Ethernet Interfaces ###
set groups AE-LACP-VLAN when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups AE-LACP-VLAN
set groups AE-LACP-VLAN chassis aggregated-devices ethernet device-count 1000
set groups AE-LACP-VLAN interfaces ae1 description "ae to server1"
set groups AE-LACP-VLAN interfaces ge-101/0/22 ether-options 802.3ad ae1
set groups AE-LACP-VLAN interfaces ge-102/0/22 ether-options 802.3ad ae1
set groups AE-LACP-VLAN interfaces ae1 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae1 aggregated-ether-options lacp periodic fast
set groups AE-LACP-VLAN interfaces ae2 description "ae to server2"
set groups AE-LACP-VLAN interfaces ge-101/0/23 ether-options 802.3ad ae2
set groups AE-LACP-VLAN interfaces ge-102/0/23 ether-options 802.3ad ae2
set groups AE-LACP-VLAN interfaces ae2 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae2 aggregated-ether-options lacp periodic fast
set groups AE-LACP-VLAN interfaces ae3 description "ae to server3"
set groups AE-LACP-VLAN interfaces ge-101/0/24 ether-options 802.3ad ae3
set groups AE-LACP-VLAN interfaces ge-102/0/24 ether-options 802.3ad ae3
set groups AE-LACP-VLAN interfaces ae3 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae3 aggregated-ether-options lacp periodic fast
set groups AE-LACP-VLAN interfaces ae4 description "ae to server4"
set groups AE-LACP-VLAN interfaces ge-103/0/22 ether-options 802.3ad ae4
set groups AE-LACP-VLAN interfaces ge-104/0/22 ether-options 802.3ad ae4
set groups AE-LACP-VLAN interfaces ae4 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae4 aggregated-ether-options lacp periodic fast
set groups AE-LACP-VLAN interfaces ae5 description "ae to server5"
set groups AE-LACP-VLAN interfaces ge-103/0/23 ether-options 802.3ad ae5
set groups AE-LACP-VLAN interfaces ge-104/0/23 ether-options 802.3ad ae5
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae5 aggregated-ether-options lacp periodic fast
set groups AE-LACP-VLAN interfaces ae6 description "ae to server6"
set groups AE-LACP-VLAN interfaces ge-103/0/24 ether-options 802.3ad ae6
set groups AE-LACP-VLAN interfaces ge-104/0/24 ether-options 802.3ad ae6
set groups AE-LACP-VLAN interfaces ae6 aggregated-ether-options lacp active
set groups AE-LACP-VLAN interfaces ae6 aggregated-ether-options lacp periodic fast

### VLANs and IRB Interfaces ###
set groups IRB-VLANS when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups IRB-VLANS
set groups IRB-VLANS interfaces ae1 unit 0 family ethernet-switching vlan members 100
set groups IRB-VLANS interfaces ae2 unit 0 family ethernet-switching vlan members 100
set groups IRB-VLANS interfaces ae3 unit 0 family ethernet-switching vlan members 100
set groups IRB-VLANS interfaces ae4 unit 0 family ethernet-switching vlan members 200
set groups IRB-VLANS interfaces ae5 unit 0 family ethernet-switching vlan members 200
set groups IRB-VLANS interfaces ae6 unit 0 family ethernet-switching vlan members 200
set groups IRB-VLANS vlans vlan100 vlan-id 100
set groups IRB-VLANS vlans vlan200 vlan-id 200
set groups IRB-VLANS interfaces irb unit 100 family inet address 10.1.1.1/24
set groups IRB-VLANS interfaces irb unit 200 family inet address 10.2.2.1/24
set groups IRB-VLANS interfaces irb unit 200 family inet6 address 2001:db8:2::1/64
set groups IRB-VLANS vlans vlan100 mcae-mac-synchronize
set groups IRB-VLANS vlans vlan200 mcae-mac-synchronize

### OSPF ###
set routing-instances vr-10 instance-type virtual-router
set interfaces lo0 unit 10 family inet address 192.168.100.1
set routing-instances vr-10 interface lo0.10
set routing-instances vr-10 routing-options router-id 192.168.100.1
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100

### BGP ###
set routing-instances vr-20 instance-type virtual-router
set routing-instances vr-20 interface ae100.0
set routing-instances vr-20 protocols bgp group ebgp-20 type external
set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64500
set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64501
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.1.1

### Class of Service ###
set apply-groups COS
set apply-groups COS when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups COS
set groups COS when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups COS
dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service classifiers dscp dscp_classifier forwarding-class
set groups COS class-of-service forwarding-instances class fc0 queue-num 0
set groups COS class-of-service forwarding-instances class fc1 queue-num 1
set groups COS class-of-service forwarding-instances class fc2 queue-num 2
set groups COS class-of-service forwarding-instances class fc3 queue-num 3
set groups COS class-of-service interfaces ae1 unit 0 classifiers dscp dscp_classifier
set groups COS class-of-service interfaces ae2 unit 0 classifiers dscp dscp_classifier
set groups COS class-of-service interfaces ae3 unit 0 classifiers dscp dscp_classifier
set groups COS class-of-service interfaces ae4 unit 0 classifiers dscp dscp_classifier
set groups COS class-of-service interfaces ae5 unit 0 classifiers dscp dscp_classifier
set groups COS class-of-service interfaces ae6 unit 0 classifiers dscp dscp_classifier

### DHCP Relay ###
set apply-groups DHCP-RELAY
set apply-groups DHCP-RELAY when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups DHCP-RELAY
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay server-group sg1 203.0.113.1
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay group client1 active-server-group sg1
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay group client1 forward-only routing-instance vr-20
set groups DHCP-RELAY routing-instances vr-20 forwarding-options dhcp-relay group
client1 interface irb.20

### Layer 3 Multicast ###
set routing-instances vr-10 instance-type virtual-router
set routing-instances vr-10 protocols pim rp static static-address 192.168.100.5
set routing-instances vr-10 protocols pim interface all mode sparse

### IGMP Snooping ###
set groups IGMP-SNOOPING when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups IGMP-SNOOPING
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae100.0
multicast-router-interface
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan200 interface ae100.0
multicast-router-interface
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae1.0
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae2.0
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan100 interface ae3.0
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan200 interface ae4.0
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan200 interface ae5.0
set groups IGMP-SNOOPING protocols igmp-snooping vlan vlan200 interface ae6.0

### VLAN Autosense ###
set groups VLAN-AUTOSENSE when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups VLAN-AUTOSENSE
set groups VLAN-AUTOSENSE interfaces ae1 unit 0 family ethernet-switching
vlan-auto-sense

### Layer 2 Loop Detection ###
set groups LOOP-DETECTION when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups LOOP-DETECTION
set groups LOOP-DETECTION protocols loop-detect interface all-extended-ports
set groups LOOP-DETECTION protocols loop-detect destination-mac 00:00:5E:00:53:AA

### LLDP ###
set groups LLDP when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups LLDP
set groups LLDP protocols lldp interface all

### Firewall Filter ###
set groups FIREWALL-FILTER when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups FIREWALL-FILTER
set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1 term
source-mac-005300 from source-mac-address 00:00:5E:00:53:00
set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1 term
source-mac-005300 then accept
set groups FIREWALL-FILTER firewall family ethernet-switching filter filter1 term
source-mac-005300 then count source-mac-count
set groups FIREWALL-FILTER vlans vlan100 forwarding-options filter input filter1

### SNMP ###
set groups SNMP when peers [ad1-qfx10002 ad2-qfx10002]
set apply-groups SNMP
set groups SNMP system processes snmp enable
set groups SNMP snmp location "Enterprise Data Center 1"
set groups SNMP snmp contact "Jane Doe"
set groups SNMP snmp interface em1.0
set groups SNMP snmp community public authorization read-only
set groups SNMP snmp community private authorization read-write
set groups SNMP snmp trap-group space targets 203.0.113.251

Aggregation Device 2 (ad2-qfx10002):

WARNING: The password password is used in the commit synchronization configuration procedure for illustrative purposes only. Use a more secure password in your device configuration.

### Commit Synchronization ###
set system commit peers-synchronize
set system commit peers ad1-qfx10002 user root authentication password
set system services netconf ssh

### Aggregated Ethernet Interface to MX480 Core Layer Router ###
set apply-groups AE-ROUTER-ADSWITCHES
set interfaces ae100 unit 0 family inet address 10.0.2.100/24

### FPC ID and Satellite Device Alias Assignment ###
set apply-groups FUSION-FPC-CASCADE-ALIAS

### Cascade Port Conversion ###
set apply-groups FUSION-FPC-CASCADE-ALIAS

### ICL Aggregated Ethernet Interface ###
set apply-groups ICL-CONFIG

### Dual Aggregation Devices ###
delete chassis satellite-management single-home
set chassis satellite-management redundancy-groups chassis-id 2
set chassis satellite-management redundancy-groups rgl peer-chassis-id 1
inter-chassis-link ae999

### BFD over ICL ###
set chassis satellite-management redundancy-groups rgl redundancy-group-id 1 peer-chassis-id 1 liveness-detection minimum-interval 2000
set chassis satellite-management redundancy-groups rgl redundancy-group-id 1 peer-chassis-id 1 liveness-detection multiplier 3
set chassis satellite-management redundancy-groups rgl redundancy-group-id 1 peer-chassis-id 1 liveness-detection transmit-interval minimum-interval 2000

### Automatic Satellite Device Conversion ###
set apply-groups AUTO-SAT-CONV

### Satellite Software Upgrade Groups ###
set apply-groups SAT-SW-UPGRADE
### Uplink Port Pinning ###
set apply-groups UPLINK_PIN

### Uplink Failure Detection ###
set apply-groups UFD

### Access Interface Aggregated Ethernet Interfaces ###
set apply-groups AE-LACP-VLAN

### VLANs and IRB Interfaces ###
set apply-groups IRB-VLANS

### OSPF ###
set routing-instances vr-10 instance-type virtual-router
set interfaces lo0 unit 10 family inet address 192.168.100.2
set routing-instances vr-10 interface lo0.10
set routing-instances vr-10 routing-options router-id 192.168.100.2
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface lo0.10 passive
set routing-instances vr-10 protocols ospf area 0.0.0.0 interface ae100

### BGP ###
set routing-instances vr-20 instance-type virtual-router
set routing-instances vr-20 interface ae100.0
set routing-instances vr-20 protocols bgp group ebgp-20 type external
set routing-instances vr-20 protocols bgp group ebgp-20 local-as 64500
set routing-instances vr-20 protocols bgp group ebgp-20 peer-as 64501
set routing-instances vr-20 protocols bgp group ebgp-20 neighbor 10.0.2.1

### Class of Service ###
set apply-groups COS

### DHCP Relay ###
set apply-groups DHCP-RELAY

### Layer 3 Multicast ###
set routing-instances vr-10 instance-type virtual-router
set routing-instances vr-10 protocols pim rp static address 192.168.100.5
set routing-instances vr-10 protocols pim interface all mode sparse

### IGMP Snooping ###
set apply-groups IGMP-SNOOPING

### VLAN Autosense ###
set apply-groups VLAN-AUTOSENSE

### Layer 2 Loop Detection ###
set apply-groups LOOP-DETECTION

### LLDP ###
set apply-groups LLDP
### Firewall Filter ###
set apply-groups FIREWALL-FILTER

### SNMP ###
set apply-groups SNMP