Network Configuration Example

Midsize Enterprise Campus Solution

Modified: 2016-08-01

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

Network Configuration Example Midsize Enterprise Campus Solution

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at 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

CHAPTER 1

Midsize Enterprise Campus Solution

About This Network Configuration Example

This network configuration example describes the reference architecture for the wired infrastructure of a midsize enterprise campus, discusses considerations and recommendations for designing a midsize campus network, and provides configuration examples for configuring a highly available, secure network that delivers a high quality of services to end users and applications.

This network configuration example is a validated solution within the enterprise campus domain. Juniper Networks validated solutions are complete domain architectures that are expert designed, lab tested at scale, and documented to provide guidance in the deployment of complex solutions. Juniper Networks solution validation labs put all solutions through extensive testing using both simulation and live network elements to ensure comprehensive validation of all published solutions. Customer use cases, common domain examples, and field experience are combined to generate prescriptive configurations and architectures to guide customer and partner implementations of Juniper Networks solutions. This approach enables partners and customers to reduce time to certify and verify new designs by providing tested, prescriptive configurations to use as a baseline.

The Juniper Networks midsize enterprise campus solution addresses the end-to-end validated architecture required to deliver a design and implementation strategy for today's campus environments, built upon a reliable and secure Juniper foundation. Validation comes through testing that encompasses not only the basic connectivity required to

provide service for the campus, but also tests the scale and policy on the entire design, resulting in an architecture that the customers can trust.

Understanding the Benefits of the Midsize Enterprise Campus Solution

Campus networks are evolving and growing at a rapid rate. No longer merely comprised of homogenous desktops and printers—a campus network now includes an array of IP devices, such as phones, wireless access points, tablets, and more. Enterprise knowledge workers require constant connectivity to mission-critical applications and can work from anywhere, as their access permits. Providing a consistent quality experience for all applications deployed across the network can increase the overall productivity of an enterprise. Enterprises must build a network that can provide flexibility, scalability, and high quality of service, while protecting critical data from unauthorized access.

This solution provides an architecture for wired network in the midsize campus that meets the challenges faced by today's enterprises. The solution was scale and performance tested using a variety of end user devices–laptops, VoIP phones, wireless mobile devices—using both real and simulated traffic.

Related Documentation

- Understanding the Design of the Midsize Enterprise Campus Solution on page 6

Understanding the Design of the Midsize Enterprise Campus Solution

The design of the midsize enterprise campus solution is guided by several high-level goals aimed primarily at solving the business problems presented by the proliferation of IP devices and applications in the enterprise. The solution design goals are to:

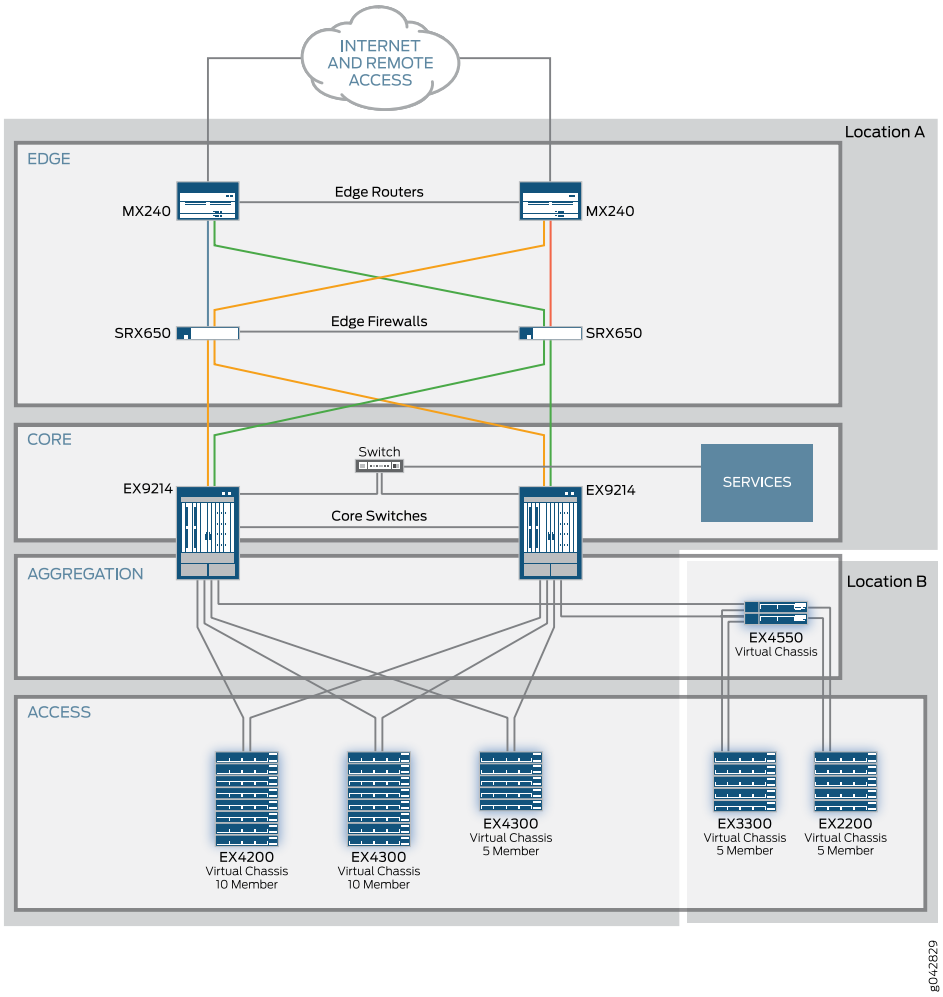
- Support up to 10,000 users and devices
- Ensure uninterrupted voice and video sessions by providing sub-second recovery from network failures
- Provide secure, flexible access to the network while protecting critical data from unauthorized access
- Provide a consistent and high quality of experience for applications, such as voice, video, and mission-critical data applications, through the use of a robust quality-of-service (QoS) feature set and policy

This section describes the overall solution design, the design considerations, and how the components of the design function together to meet the solution goals. It describes:

Basic Functional Design

Figure 1 on page 7 shows the basic topology used in the midsize enterprise campus solution. This topology was chosen to provide a general and flexible example that can be modified to apply to different Enterprise vertical markets and physical facilities. The physical topology is typically based on several factors including availability of cable plant and layout of the building or campus.

Figure 1: Midsize Enterprise Campus Solution Basic Topology



Two physical locations are defined:

- Location A—High-density location that serves as the campus network core: the core switches, edge devices, and services are located here.
- Location B—Low- to medium-density location that is geographically separate from location A.

The topology follows the hierarchical design commonly used in today's campus networks in which the campus LAN is divided into layers: access, aggregation, core, and edge. This type of design allows the components in each layer to assume a distinct role in the network. This in turn facilitates optimizing each component for its role and troubleshooting the network because it is easier to isolate problems. It also permits a modular approach, in which operational changes can be constrained to a subset of the network and in which design elements can be replicated for easy scaling as the network grows.

In addition, the solution design takes advantage of Juniper Networks® Virtual Chassis technology and the high port density of the EX9214 switches to simplify and flatten the network. The use of Virtual Chassis greatly reduces the number of devices to be managed, and the high port density of the EX9214 switches permits the core and aggregation layers to be collapsed in location A. The resulting network design also eliminates the need for the Spanning Tree Protocol (STP).

Access Layer

The access layer provides network connectivity to end-user devices, such as personal computers, VoIP phones, and printers, and connects wireless LAN (WLAN) access points to the network. Access switches typically reside in the wiring closets of each floor in a campus facility.

The access layer should provide end users with a consistent access experience regardless of their location or device. As the first layer of the network to provide user access control, the access layer plays a critical role in protecting the network from malicious attacks.

A well-designed access layer should provide:

- High port density and high-bandwidth uplink ports—Access layer devices must provide high port density for client devices and high-bandwidth uplink ports to reduce the client-to-uplink subscription ratio.
- Reliable connections with high quality of service—Access layer devices must support high availability through redundant hardware. They should also provide traffic management features. They must be able to classify, mark, and prioritize traffic in support of end-to-end quality of service (QoS). With the increasing use of multicast applications, support of multicast snooping is important to limit multicast packet flooding.
- Secure access—Access layer devices must provide access control services, such as 802.1x, and integrate with security infrastructure services. They must support segmentation of traffic through VLANs. In addition, they must provide security from malicious attacks by supporting techniques such as DHCP snooping, dynamic ARP inspection, and IP source guard.
- Simplified deployment and management—Because of the large number of devices deployed in the access layer, simplified management of the devices is a must. To simplify the deployment of IP phones, CCTV, and access points and to reduce capital expenditures, Power over Ethernet (PoE) is a must. When deploying PoE and PoE+,

pay careful attention the PoE power requirements of the powered devices and the overall PoE power budget of the access switch.

- Scalability—The access layer must be able to scale flexibly to reduce capital and operating expenses as users and devices grow.

For the access layer, the solution design uses EX Series Ethernet Switches. EX Series switches have the necessary port density, port types, and features to meet the access layer requirements. The access layer design also takes advantage of Juniper Networks Virtual Chassis technology, which allows interconnected switches to behave, operate, and be managed as a single device with high port density. The use of Virtual Chassis in the access layer:

- Simplifies network management by reducing the number of managed devices by a factor of 4 to 10, depending on the models of switch being used
- Enables the network to grow port count without increasing operational overhead
- Provides control plane redundancy—one switch acts as the master Routing Engine and another as the backup
- Preserves bandwidth—inter-switch traffic is routed over the Virtual Chassis backplane at line rates for all packet sizes

Aggregation Layer

The aggregation layer acts as a multiplexing point between the access layer and the campus network core. The aggregation layer combines a large number of smaller interfaces from the access switches into high-bandwidth trunk ports that can be more easily consumed by the core switch. The aggregation layer also provides Layer 3 routing services to the access layer.

Because all traffic to and from the access layer flows through the aggregation layer, the aggregation layer needs to provide high availability and resiliency, including hardware redundancy and the ability to upgrade the software while the devices are in service. It also must have high throughput, providing wire-rate forwarding and a nonblocking architecture.

Scalability is also a key consideration for the aggregation layer. Scale requirements increase linearly for every port added to the access layer. For example, if an access switch supports 10,000 MAC addresses and an aggregation switch consolidates 100 access switches, the MAC scale requirements for the aggregation switch is 1,000,000 MAC addresses (10,000 x 100).

For location A, the solution design uses EX9214 switches to aggregate the traffic from the access switches in location A . These switches have the feature set, high port density, and scalability that enable them to function simultaneously as aggregation switches and core switches. This allows the core and aggregation layers to be collapsed into a single set of devices in location A. Collapsing the core and aggregation layers has these advantages:

- Decreased number of devices

- Decreased latency
- Decreased complexity and management overhead

The EX9214 switches are in a multichassis link aggregation (MC-LAG) configuration, which provides high availability and a nonblocking architecture for the aggregation layer by eliminating the need for STP. "High Availability Design" on page 12 describes MC-LAG in more detail.

For location B, two EX4550 switches serve as aggregation switches. The EX9214 switches in location A could aggregate the traffic from location B; however, this option would increase cabling costs. EX4550 switches deliver highly available, simple, and scalable 10 GbE connectivity in a compact and power-efficient platform. The switches are in a Virtual Chassis configuration to provide the required redundancy and nonblocking architecture.

Core Layer

The core layer is at the heart of the campus network—every network element ultimately converges at the core. The core is usually configured as a Layer 3 device that provides high-speed packet switching between multiple sets of aggregation and/or access devices and that connects them to the perimeter or WAN edge network. Essential design features of the core layer include:

- High port speed (1 GB, 10 GB, 40 GB) and the expected ability to support higher speeds in the future
- High port density and the ability to scale to support future network expansion
- High throughput, providing wire-rate forwarding and a nonblocking architecture
- High availability
- Robust Layer 2 and Layer 3 feature set

The EX9214 switches used in the solution design support:

- Any combination of 1 GB, 10 GB, and 40 GB line cards, with support of expected future 100 GB line cards
- Up to 240 10 GB ports at line-rate speeds
- MC-LAG for high availability
- Redundant power supplies, fan modules, control modules, and switching fabrics
- Up to 1,000,000 unicast routes
- Up to 256K firewall filters (ACLs)
- Up to 1,000,000 MAC addresses

Edge Layer

The edge layer is the gateway for remote access to the campus network. It handles all Internet traffic into and out of the campus network. As a result, the edge can be a choke

point for Internet traffic, making high availability and redundancy a vital aspect of edge design.

In addition, the edge is the first line of defense against attacks coming from the Internet and must provide robust security.

The midsize enterprise campus solution uses the following devices to fulfill the requirements of the edge network:

- Edge Firewall on page 11
- Edge Routers on page 11

Edge Firewall

The edge firewall provides perimeter security services such as traffic inspection, security policies, NAT, and IPsec. Given the edge firewall's important role in protecting the campus network from attacks, the campus network must be designed so that all Internet traffic entering and exiting the campus network must pass through the firewall.

The solution design uses two SRX650 Services Gateways that are clustered for node redundancy. An SRX650 Services Gateway supports up to 7.0 Gbps firewall, 1.5 Gbps IPsec VPN, and 900 Mbps IPS, making it suitable for a medium to large campus. The SRX650 gateways are physically connected to the core switch and edge routers, ensuring that edge traffic must pass through them.

Edge Routers

The edge router connects the campus network to the Internet service provider. To support any edge interconnect offered, the edge router must support the IPv4, IPv6, ISO, and MPLS protocols. It must also support widely deployed routing protocols in campus networks, such as static routes, OSPF, OSPF-TE, OSPFv3, IS-IS, and BGP.

Because it is directly connected to the Internet, the edge router must provide the following security and tunneling features:

- The ability to limit what type of traffic accesses the control plane and enforce packets per second (pps) limitations
- The ability to police traffic, penalizing or discarding traffic that exceeds a set bandwidth
- Support for granular access control lists that can match on Layer 2 through Layer 4 fields
- Support for the following unicast reverse path forwarding modes: loose, strict, and VRF
- Support for Secure Shell (SSH)
- Support for IPsec, GRE, and IP tunneling

To resolve IP address conflicts and bridge IPv6 islands, the edge router must support a wide variety of NAT techniques such as:

- NAT44 (static translation of source IPv4 without port mapping)
- NAT 64 (translation of IPv6 addresses to IPv4 addresses and vice versa)

- NAPT44 and NAPT66 (static translation of source IPv4 and IPv6 addresses with port mapping)
- Twice NAT44 (static translation of both source and destination IPv4 addresses)
- NAPT-PT (bind addresses in an IPv6 network with addresses in an IPv4 network and vice versa)

Finally, because the edge router is the ingress and egress point of the campus, edge routers must support account data collection, such as average traffic flows and statistics or the number of bytes or packets received and transmitted per application.

The midsize enterprise campus solution uses two MX240 3D Universal Edge Routers in a redundant MC-LAG configuration to meet the edge routing requirements. Because the MX240 router offers dual Routing Engines and unified in-service software upgrade (ISSU) at a reasonable price point, it is the preferred option over the smaller MX80 router.

High Availability Design

The midsize enterprise campus solution is designed to provide users with uninterrupted network access during hardware or software failures. Voice and video users have particularly demanding requirements—for a user to perceive no loss of service, the network must recover from failures in less than 1 second. In addition, users expect 24x7 access to the network—downtime because of planned maintenance must be minimal. This section discusses how the solution design meets these requirements.

- Control Plane Redundancy on page 12
- High Availability Software on page 13
- Node Redundancy on page 13

Control Plane Redundancy

The midsize enterprise campus solution is designed so that all devices in the wired network have redundant control planes. The techniques to achieve redundancy vary according to the type of device:

- Dual Routing Engines in a single physical device—Each EX9214 switch and MX240 router has two Routing Engines. One Routing Engine acts as the primary Routing Engine for the switch, while the other acts as the backup Routing Engine. If the primary Routing Engine fails, the backup Routing Engine takes over.
- Virtual Chassis—All access switches and the paired aggregation switches in location B are in Virtual Chassis configurations. In a Virtual Chassis, one member acts as the primary Routing Engine for the Virtual Chassis, while another member acts as the backup Routing Engine. The remaining members take a line card role. If the Virtual Chassis primary member fails, the backup takes over.
- Chassis cluster—The SRX650 Services Gateways achieve control plane redundancy by being in a chassis cluster configuration. In a chassis cluster configuration, one of the gateways acts as the primary Routing Engine. If the Routing Engine in the primary gateway fails, the Routing Engine in the standby gateway takes over.

High Availability Software

The following high availability software features are enabled on the switches and routers:

- Graceful Routing Engine switchover (GRES)—When GRES is enabled on switches and routers, the backup Routing Engine automatically synchronizes with the primary Routing Engine to preserve kernel state information and forwarding state. This synchronization enables the backup Routing Engine to continue to forward traffic, if the primary Routing Engine fails, without having to relearn routes or port states.
- Nonstop active routing (NSR) and nonstop bridging (NSB)—NSR and NSB prevent service interruptions during the brief period when the backup Routing Engine takes over from a failed primary switch or router. Normally, the absence of the primary device would cause routing and switching protocols to begin the process of reconverging network paths to route around what they determine to be a failed device. NSR and NSB prevent such a reconvergence from occurring, thus maintaining service continuity.

Although you can use GRES with graceful protocol restart instead of NSR, this solution uses NSR because it can result in faster convergence after a control plane failure, supports unified in-service software upgrades, and does not rely on helper routers to assist in restoring routing protocol information.

On the SRX Series gateways, which do not support NSR, graceful protocol restart is enabled.

Node Redundancy

All traffic traveling in and out of the campus flows through the core and edge layers. It is therefore essential that these layers do not have a single point of failure. The solution design uses redundant devices at each of these layers so that, if one device fails, the other device can continue to forward traffic. The following techniques are used to achieve node redundancy at the core and edge:

- Multichassis link aggregation (MC-LAG) configuration for edge routers and core switches
- Chassis cluster for edge firewalls

Multichassis Link Aggregation Design

MC-LAG is configured on the core switches and edge routers to provide node redundancy at the core level. MC-LAG supports link aggregation groups (LAGs) that are spread across more than one device. Thus, if one of the switches fails, the other switch continues to forward the traffic on its MC-LAG link.

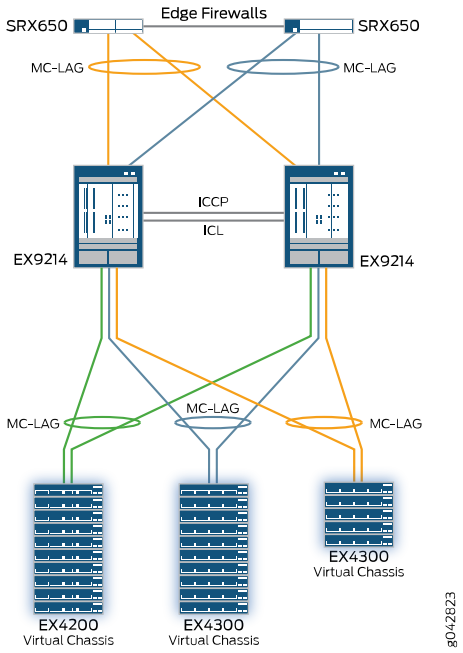
The client device—the device on the other end of the MC-LAG—does not need to be aware of MC-LAG. From its perspective, it is connecting to a single device through a LAG.

To support LAGs across two devices, both devices in an MC-LAG configuration must be able to synchronize their Link Aggregation Control Protocol (LACP) configurations, learned MAC addresses, and Address Resolution Protocol (ARP) entries. MC-LAG uses the following mechanisms to do so:

- Inter-chassis Control Protocol (ICCP)—Control plane protocol that synchronizes configurations and operational states between two MC-LAG peers. It uses TCP as a transport protocol and requires Bidirectional Forwarding Detection (BFD) for fast convergence.
- Interchassis link (ICL) link—Layer 2 link that is used to replicate forwarding information across peers.

Figure 2 on page 14 illustrates the MC-LAG configuration that is used by the core switches.

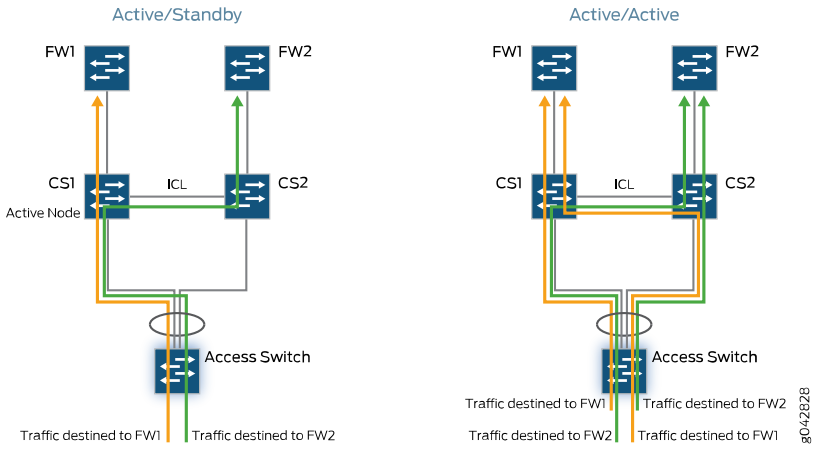
Figure 2: MC-LAG Configuration in the Core Switches



MC-LAG Design Considerations

MC-LAG can be configured in active/standby mode, in which only one device actively forwards traffic, or in active/active mode, in which both devices actively forward traffic. Figure 3 on page 15 illustrates the difference between active/standby and active/active.

Figure 3: MC-LAG Active/Standby Versus Active/Active



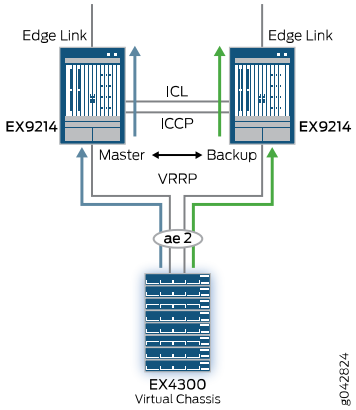
This solution uses active/active as the preferred mode for the following reasons:

- Traffic is load-balanced in active/active mode, resulting in link-level efficiency of 100 percent.
- Convergence is faster in active/active mode than in active/standby mode. In active/active mode, information is exchanged between devices during operations. After a failure, the operational switch or router does not need to relearn any routes and continues to forward traffic.
- It enables you to configure Layer 3 protocols on integrated routing and bridging (IRB) interfaces, providing a hybrid Layer 2 and Layer 3 environment on the core switch.

MC-LAG is used in conjunction with the Virtual Router Redundancy Protocol (VRRP) both on the core switches and on the edge routers. VRRP permits redundant routers to appear as a single virtual router to the other devices. In a VRRP implementation, each VRRP peer shares a common virtual IP address and virtual MAC address in addition to its unique physical IP address and MAC address. Thus, each IRB configured on the core switches must have a virtual IP address.

Typically, VRRP implementations are active/passive implementations, in which only one peer forwards traffic while the other peer is in standby. However, in the Junos® operating system (Junos OS), the VRRP forwarding logic has been modified when both VRRP and active/active MC-LAG are configured. In this case, both VRRP peers forward traffic and load-balance the traffic between them. As shown in Figure 4 on page 16, data packets received by the backup peer on the MC-LAG member link are forwarded by the backup peer rather than being sent to the master peer for forwarding.

Figure 4: VRRP Forwarding in MC-LAG Configuration



Firewall Chassis Cluster Design

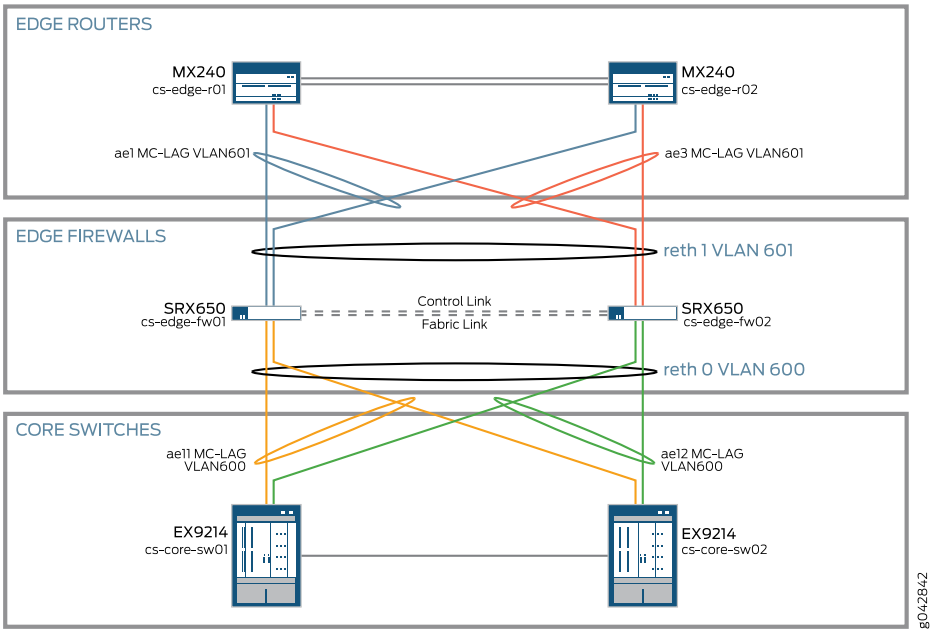
SRX Series Services Gateways achieve node redundancy through chassis clustering. In the solution design, two SRX650 gateways are clustered to provide stateful failover of processes, services, and traffic flow.

Creating a chassis cluster requires configuring the following interfaces on the SRX650 Services Gateways:

- Control link—Link between the cluster nodes that transmits session state, configuration, and aliveness signals.
- Fabric link—Link between the cluster nodes that transmits network traffic between the nodes and synchronizes the data plane software's dynamic runtime state.
- Redundant Ethernet interface—Virtual interface that is active on one node at a time and can fail over to the other node. Each redundant Ethernet (reth) interface consists of at least one interface from each cluster node. The redundant Ethernet interface has its own MAC address, which is different from the physical interface MAC addresses of its members. When a redundant Ethernet interface fails over, the connecting devices are updated with the MAC address of the new physical interface in use. Because the redundant Ethernet interface continues to use the same virtual MAC address and IP address, Layer 3 operations continue to work with no need for user intervention.

Figure 5 on page 17 illustrates the chassis cluster topology.

Figure 5: SRX650 Gateway Chassis Cluster



In this topology, two redundant Ethernet interfaces are configured:

- reth0, which connects to the core switches
- reth1, which connects to the edge routers

To increase redundancy and bandwidth, the redundant Ethernet interfaces are configured as redundant Ethernet LAGs, with two physical interfaces bundled into each LAG on each cluster node. These physical interfaces permit each cluster node to have a physical connection to each core switch and edge router.

Firewall Chassis Cluster Design Considerations

SRX Series chassis clusters support both active/active and active/backup clustering modes. Because the additional scale provided by active/active mode is not required by this solution, the design uses the simpler and more commonly implemented active/backup mode. In active/backup mode, only the LAG member links on the active cluster node are active and forward data traffic.

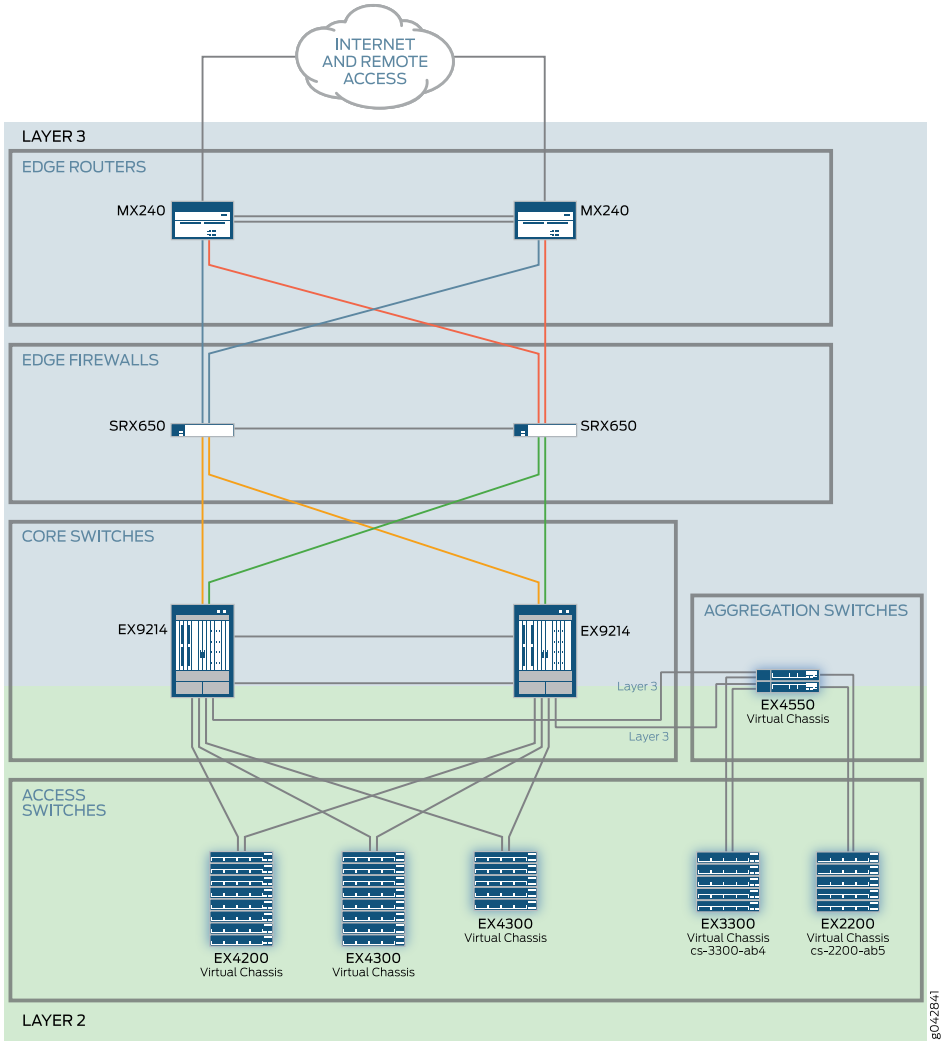
The active node uses gratuitous ARP to advertise to the connecting devices that it is the next-hop gateway. If a failover occurs, the backup node uses gratuitous ARP to announce that it is now the next-hop gateway. As a result, for failover to work, the redundant Ethernet interface members and their connecting interfaces on the other devices must belong to the same bridge domain, as shown in Figure 5 on page 17. These bridge domains result in an OSPF broadcast network.

The core switches and edge routers must be configured with an OSPF priority of 255 and 254 to ensure that they will always be the designated router and backup designated router for their bridge domain.

Switching and Routing Design

In the switching and routing design, the aggregation layer forms the boundary between Layer 2 and Layer 3, as illustrated in Figure 6 on page 18.

Figure 6: Layer 2 and Layer 3 Boundary



The following summarizes the basic switching and routing design:

- The devices in the access layer are configured as Layer 2 switches that forward user traffic on high-speed trunk ports to the aggregation layer.
- The switches in the aggregation layer provide the boundary between Layer 2 and Layer 3. They are configured to provide Layer 2 switching on their downstream trunk ports to the access switches and Layer 3 routing on their upstream ports to the core. They act as the default gateways for the access devices.

- The devices in the core and edge layers are primarily Layer 3 devices, routing traffic between the aggregation layer devices and between the internal campus network and the external Enterprise WAN and Internet.

This section covers:

Switching Design

Important considerations for the design of the switching network are:

Separation of Layer 2 Traffic

The access layer of the campus network provides network access to a wide variety of devices and users. The traffic generated by these devices and users often has different management or security requirements and thus needs to be separated. For example, voice traffic generated by VoIP phones requires different quality-of-service parameters than data traffic generated by laptops. Or users from the finance department might need to be granted access to a server that no other users can access.

Typically in campus networks, this traffic separation is achieved through the use of virtual LANs (VLANs) in the access and aggregation layers. Each organization will have its own requirements for separating user traffic using VLANs. In testing, this solution deployed a VLAN design that is optimized for management simplicity and that can be easily adapted to other organization environments. In the solution design, user traffic is separated into VLANs based on:

- Traffic type—Voice and data traffic are carried on separate VLANs.
- Department—Each functional group, or department, has its own VLAN. For example, there are different VLANs for Engineering, Marketing, Sales, Finance, and Executive personnel.
- Access method—Wired traffic and wireless traffic are separated into different VLANs.

Wired data traffic is dynamically assigned to a port data VLAN as a result of the user authentication process.

For wired voice traffic, this solution takes advantage of the voice VLAN feature supported on EX Series switches. This feature enables otherwise standard access ports to accept both untagged (data) and tagged (voice) traffic and separate these traffic streams into separate VLANs. This in turn allows a VoIP phone and an end-host machine to share a single port while enabling the application of different quality-of-service parameters to the voice traffic.

In this solution, then, each user access port is associated with two VLANs—a data VLAN, which is dynamically assigned as a result of the authentication process, and a voice VLAN,

which is statically configured on the port. A single voice VLAN can be used for all wired voice traffic because voice traffic typically has the same security requirements regardless of user role.

Layer 2 Loop Prevention

In campus architectures, each access switch is typically connected to two aggregation switches for reliability and high availability. The aggregation switches in turn have a Layer 2 connection to each other. This topology can create a Layer 2 loop.

Traditionally, a Spanning Tree Protocol (STP) is used to prevent Layer 2 loops. SPT exchanges information with other switches to prune specific redundant links, creating a loop-free topology with a single active Layer 2 data path between any two switches.

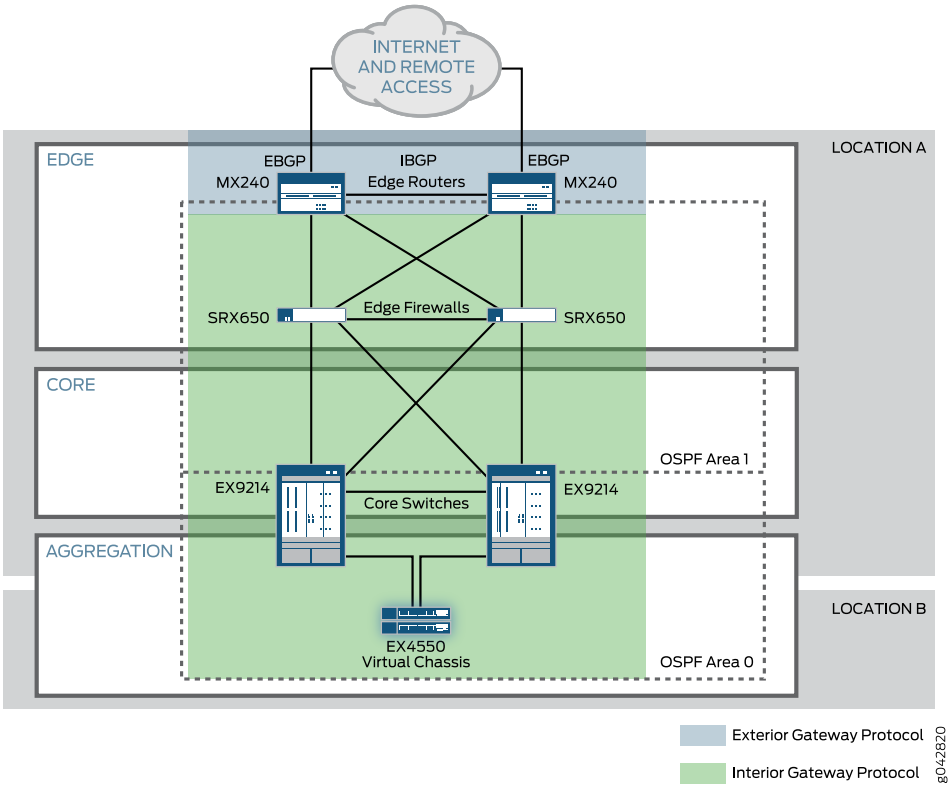
However, STP adds latency to the network. Although more recent versions of STP have reduced convergence after a failure to a few seconds, STP still has not achieved the sub-second convergence that Layer 3 protocols have achieved. Real-time applications, such as voice or video, experience disruptions when STP is used in campus networks. In addition, STP results in inefficient use of network resources because it blocks all but one of the redundant paths.

To prevent the creation of Layer 2 loops, this solution uses MC-LAG in the aggregation layer of location A and Virtual Chassis in the aggregation layer of location B. Each technology creates a single virtual device from one or more physical devices. From the point-of-view of the connecting access switch, the switch has multiple links to a single device through an aggregated Ethernet interface. STP is unnecessary when these technologies are incorporated into the Layer 2 network. This improves network performance by reducing latency and improves network efficiency by enabling all links to forward traffic.

Routing Design

In this solution, Layer 3 routing starts at the aggregation layer. Figure 7 on page 21 provides more detail on the routing design in the aggregation, core, and edge layers.

Figure 7: Routing Design



Elements of the routing design include:

- Integrated Bridging and Routing on page 21
- Interior Gateway Protocol on page 22
- Network Address Translation on page 22
- Exterior Gateway Protocol on page 23
- Bidirectional Forwarding Detection Protocol on page 23

Integrated Bridging and Routing

To provide Layer 3 routing capabilities for the user VLANs, the core switches in location A and the aggregation switches in location B are configured with integrated routing and bridging (IRB) interfaces on the user VLANs. IRB interfaces are also known as routed VLAN interfaces (RVIs). IRB interfaces:

- Function as the gateway router IP addresses for the hosts on the VLAN subnet
- Provide Layer 3 interfaces for routing traffic between VLANs

The core and aggregation switches advertise the network prefixes to the edge firewalls to allow the edge firewalls to provide services such a Network Address Translation (NAT) and encryption.

Interior Gateway Protocol

For the interior gateway protocol (IGP), we recommend the use of a link-state protocol such as IS-IS or OSPF rather than a distance vector protocol such as RIP. Although distance vector protocols are generally easier to configure and to maintain than link-state protocols, link-state protocols feature improved scaling and quicker convergence times, features that are critical in larger networks. The solution design uses OSPF because it is the most commonly used IGP in campus networks.

As shown in Figure 7 on page 21, OSPF routing occurs between two major sections of the campus network: the perimeter and the core. These sections have differing traffic profiles and flows. Traffic traveling to or from the Internet must always pass through the perimeter, while local campus traffic stays entirely within the core.

To limit link-state advertisement (LSA) flooding to within each section, the solution implements two OSPF areas:

- Area 0, the core section, contains the core switches and the location B aggregation switch.
- Area 1, the perimeter section, contains the edge firewalls and routers.

All IRB and VRRP interfaces are configured as passive OSPF interfaces. This enables them to advertise their addresses into OSPF while preventing end devices from receiving LSAs and creating an adjacency with the core switches.

The edge routers have the responsibility of advertising external reachability to the other OSPF nodes. To provide Internet access to the campus network, the routers in this solution export a dynamic, condition-based, default route to the Internet into OSPF towards the edge firewalls and core switches. The edge routers export this default route only when they receive a route through an external BGP (EBGP) advertisement from the Internet service provider. If an edge router does not receive a route advertisement from its EBGP neighbor, it stops exporting the default route.

The following configuration is implemented on each OSPF node:

- Authentication—MD5 encryption is enabled to prevent unauthorized or accidental adjacencies.
- Reference bandwidth—OSPF uses a reference bandwidth to calculate the cost of using an interface. This reference bandwidth should be the same on all nodes. We recommend using bandwidth large enough to accommodate expected near-future increases in Ethernet interface speeds. This solution uses a reference bandwidth of 1000 Gbps.
- Loop-free alternate (LFA) feature—The LFA feature enables fast OSPF network restoration and convergence after network faults, which minimize disruptions to real-time applications such as VoIP and video. It works by preprogramming the Packet Forwarding Engine with loop-free backup paths for known prefixes.

Network Address Translation

The SRX650 Services Gateways provide Network Address Translation (NAT) services. NAT protects the campus private address space by mapping the private IP addresses to

routable, public IP addresses. For more information about the perimeter security features provided by the SRX650 Services Gateways, see "Security Design" on page 26.

Exterior Gateway Protocol

The solution design uses BGP4 as its exterior gateway protocol for Internet connectivity. The MX240 edge routers use external BGP (EBGP) to peer with the ISPs. In addition, the routers are configured to:

- Use internal BGP (IBGP) to peer with each other and use a next-hop-self export policy.
- Advertise the campus public IP address space to the external peers. To support redundancy, each router uses the same prefix for the campus public IP address to external peers.
- Give ISP-1 a higher local preference because it is the preferred exit to the Internet.

Bidirectional Forwarding Detection Protocol

To enable faster detection of link failures than the failure-detection mechanisms of OSPF and BGP deliver, this solution enables the Bidirectional Forwarding Detection (BFD) protocol on all OSPF and BGP links. The BFD protocol is a simple hello mechanism that works at the link level. A pair of routing devices exchanges BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. Because the BFD failure detection timers have shorter time limits than the OSPF and BGP failure detection mechanisms, BFD provides faster detection of link failures.

Multicast Routing and Snooping Design

An increasing number of applications in enterprise networks use multicast forwarding, such as audio/video conferencing, software distribution, stock quotes, distance learning, and so on. For the midsize enterprise campus solution, support for multicast is based on the most common multicast protocols used in enterprise networks for multicast signaling, multicast group management, and Layer 2 multicast snooping.

Multicast Signaling Protocol

Protocol Independent Multicast (PIM) is used for the multicast routing protocol. It is the predominant multicast protocol used on the Internet.

PIM has several modes of operations, the most common of which are:

- Dense mode (PIM-DM)—Uses a flood-and-prune mechanism to build a source-based distribution tree. A router receives the multicast traffic on the interface closest to the source and floods the traffic to all other interfaces. Routers with no multicast receivers must prune back unnecessary branches.
- Sparse mode (PIM-SM)—Uses reverse path forwarding (RPF) to create a path from a multicast source to the multicast receiver when the receiver issues an explicit join request. A single router called a rendezvous point (RP) is initially selected in each multicast domain to be the connection point between multicast sources and interested receivers. Traffic flows are then rooted at the RP along the rendezvous-point tree. The rendezvous-point tree is later replaced by an optimized shortest-path tree.

- Source-specific multicast (PIM-SSM)—Uses a subset of PIM sparse mode and IGMP version 3 (IGMPv3) to enable a receiver to receive multicast traffic directly from the source. PIM-SM builds a shortest-path tree between the receiver and the source without the help of an RP.

Table 1 on page 24 summarizes the pros and cons of each PIM mode.

Table 1: Comparison of PIM Modes

PIM Mode	Pros	Cons
PIM-DM	• Does not require an RP • Guarantees shortest path from source to receiver	• Considerable overhead • Does not scale well
PIM-SM	• Scales better than PIM-DM	• Requires an RP • Might require special hardware to encapsulate register messages
PIM-SSM	• Does not require an RP • Does not require shared tree behavior • Is more secure—prevents malicious hosts from flooding unwanted traffic to a group • Receiver can select the source	• Requires IGMPv3

The solution design uses PIM-SM. By not requiring IGMPv3, PIM-SM enables better interoperability with vendor equipment that does not support IGMPv3 and simplifies configuration.

In implementing PIM-SM, you should choose your RPs carefully to improve the performance and fault-tolerance of the network. Table 2 on page 24 lists the options for RP selection and compares them.

Table 2: Comparison of RP Selection Options

RP Selection Option	Pros	Cons
Static RP	• Simplicity • Supports PIM version 1 and 2	• Single point of failure • Configuration and management overhead • Not scalable
Auto-RP	• Dynamic selection • Provides redundancy • Failover mechanism • Supports PIM version 1 and 2	• Cisco proprietary • Requires use of dense-mode groups to advertise control traffic • Slower failover than the anycast RP option • Only one RP operates at a time

Table 2: Comparison of RP Selection Options *(continued)*

RP Selection Option	Pros	Cons
Bootstrap Router (BSR)	• Dynamic selection • Provides redundancy • Failover mechanism • Part of the PIM version 2 standard • Does not require dense-mode groups for control traffic • Multiple routers can be candidate BSRs or candidate RPs	• Slower failover than the anycast RP option • Only one RP operates at a time
Anycast RP	• Virtual RP for the entire domain • Multiple routers share knowledge about multicast sources • Fast convergence after failure • Best load balancing and redundancy	• Requires Multicast Source Discovery Protocol (MSDP) (unless you use anycast RP only in a single domain)

Because fault tolerance is a necessity in an enterprise network, we recommend that you use one of the dynamic methods of RP selection. The Bootstrap Router method is an industry standard, preferred by Junos OS. As a result, this solution uses the Bootstrap Router method.

Multicast Group Management Protocol

The Internet Group Management Protocol (IGMP) is used for the multicast group management protocol. IGMP manages multicast receiver groups for IPv4 multicast traffic. IGMP enables a router to detect when a host on a directly attached subnet, typically a LAN, wants to receive traffic from a certain multicast group. Even if more than one host on the LAN wants to receive traffic for that multicast group, the router sends only one copy of each packet for that multicast group out on that interface, because of the inherent broadcast nature of LANs. When IGMP informs the router that there are no interested hosts on the subnet, the packets are withheld and that leaf is pruned from the distribution tree.

There are three versions of IGMP, all of which are supported by Junos OS:

- IGMP version 1 (IGMPv1)—In this, the original protocol, all multicast routers send periodic membership queries to an all-host group address. Hosts reply with explicit join messages, but the protocol uses a timeout to determine when hosts leave a group.
- IGMP version 2 (IGMPv2)—In IGMPv2, an election process results in one router in a network sending membership queries. Group-specific queries are supported, and hosts can send explicit leave-group messages.
- IGMP version 3 (IGMPv3)—In IGMPv3, hosts can specify the source from which they want to receive group multicast content. This means that IGMPv3 can be used with PIM-SSM to create a shortest-path tree between receiver and source.

Table 3 on page 26 lists the pros and cons of each IGMP version.

Table 3: Comparison of IGMP Versions

IGMP Version	Pros	Cons
IGMPv1	—	• High latency because there is no explicit mechanism for a host to leave a group. Multicast traffic continues to be forwarded until the timers expire after the last host leaves the group. • No group-specific queries results in increased bandwidth and flooding.
IGMPv2	• Improved latency compared to IGMPv1	• Does not support PIM-SSM.
IGMPv3	• Improved latency compared to IGMPv1 • Efficiency gain compared to IGMPv2 • Accommodates PIM-SSM • Can support a PIM-SM topology without an RP	• Hosts need to have preexisting knowledge of the specific sources active for a given group.

Junos OS defaults to IGMPv2. Because this solution does not require PIM-SSM, the solution design uses IGMPv2. IGMPv2 can interoperate with devices running IGMPv1.

Multicast Snooping

By default, a switch floods multicast traffic to all interfaces in a Layer 2 broadcast domain or VLAN. This behavior increases bandwidth consumption. By examining (snooping) IGMP messages between hosts and multicast routers, a switch can learn which hosts are interested in receiving traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

In this solution design, IGMP snooping is enabled on the Layer 2 devices in the access layers and aggregation layers, including the collapsed core/aggregation switches. In the MC-LAG configuration of the core switches, IGMP snooping membership information is automatically synchronized between both of the core switches.

Security Design

Networks are subject to attacks from various malicious sources. These attacks can be passive, where an intruder intercepts data traveling through the network, or active, where an intruder initiates commands to disrupt the normal operation of the network (for example, denial-of-service attacks or address spoofing). Security for a campus network involves preventing and monitoring unauthorized access, network misuse, unauthorized network modification, or attacks that result in the denial of network services or network accessible resources.

This section discusses the following elements of the security design of the midsize enterprise campus solution:

Access Control

With the proliferation of user devices on the campus, effective access control should support role-based policy orchestration. Together, access control and policy orchestration must be able to:

- Identify the user and the user's role
- Authenticate the user and authorize the user to access resources on the network
- Identify the type of device, operating system, and ownership (corporate-owned or employee-owned)
- Quarantine a device if necessary
- Detect the location of entry point and traffic encryption requirements

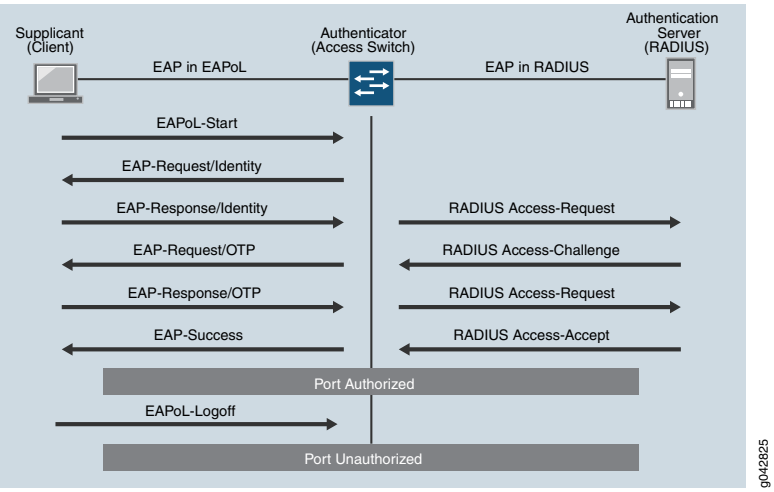
For access control, the solution design uses the 802.1X port-based network access control standard in the access layer, which integrates with and supports role-based policy orchestration.

802.1X Network Access Control Protocol

EX Series switches support endpoint access control through the 802.1X port-based network access control standard. When 802.1X authentication is enabled on a port, the switch (known as the authenticator) blocks all traffic to and from the end device (known as a supplicant) until the supplicant's credentials are presented and matched on an authentication server, typically a RADIUS server. After the supplicant is authenticated, the switch opens the port to the supplicant.

Figure 8 on page 28 illustrates the authentication process. The supplicant and authenticator communicate with each other by using exchanging Extensible Authentication Protocol (EAP) packets carried by the 802.1X protocol. The authenticator and the RADIUS server communicate by exchanging EAP packets carried by the RADIUS protocol.

Figure 8: 802.1X Authentication Process



The 802.1X protocol supports a number of different versions of the EAP protocol. This solution uses EAP-TTLS. EAP-TTLS is an "outer" protocol—it sets up a secure tunnel in which another authentication protocol, the "inner" protocol, handles the communication between the supplicant and the authentication server. The authentication server must present a valid certificate, which EAP-TTLS uses to form the tunnel. Verifying the identity of the authentication server ensures that a user connects to the intended network, and not to an access point that is pretending to be the network. For the inner protocol, the design uses the Password Authentication Protocol (PAP) or, when Junos Pulse is the supplicant, JUAC (a proprietary Juniper Networks protocol).

This solution uses EAP-TTLS because it:

- Provides strong security
- Is supported by the Junos Pulse client
- Does not require client-side certificates, which simplifies the management of client devices
- Is an industry standard

802.1X Supplicants

In a bring-your-own-device environment, 802.1X supplicants can be a wide variety of devices running a variety of supplicant software. The campus design must support these native supplicants, while continuing to provide secure connections to the campus network.

The campus design must also support:

- Devices that do not have an 802.1X supplicant, such as printers, VoIP phones, and security cameras. For these devices, this solution uses MAC authentication, in which the device is authenticated by its MAC address.

- Multiple supplicants on one port. Many organizations connect both a computer and an IP phone to a single port. The solution design supports separate authentication of both devices, using any combination of 802.1X or MAC authentication.

In addition to configuring both MAC authentication and 802.1X authentication on the same port, you can also restrict a port to performing MAC authentication only—for example, if you have a port that connects only to a device without an 802.1X supplicant, such as a video camera.

Authenticators and Policy Enforcement

In this design, the EX switches in the access layer act as 802.1X authenticators. They receive authentication requests from client supplicants, forward the authentication requests to the authentication server, and open or close the ports to traffic depending on the results of the authentication request.

The switches also act as policy enforcement points. Based on the information returned from the authentication server, they dynamically assign user traffic to VLANs and apply firewall filters (ACLs) to the traffic, restricting or allowing access to network resources as required by the user role.

Authentication Server

At minimum, this solution design requires a RADIUS server that acts as an authentication server, providing authentication and returning information such as the VLAN and name of the firewall filter associated with the user. In addition, the authentication server might provide other services such as client compliance checking, device profiling, or mobile device management, either directly or indirectly through integration with other servers.

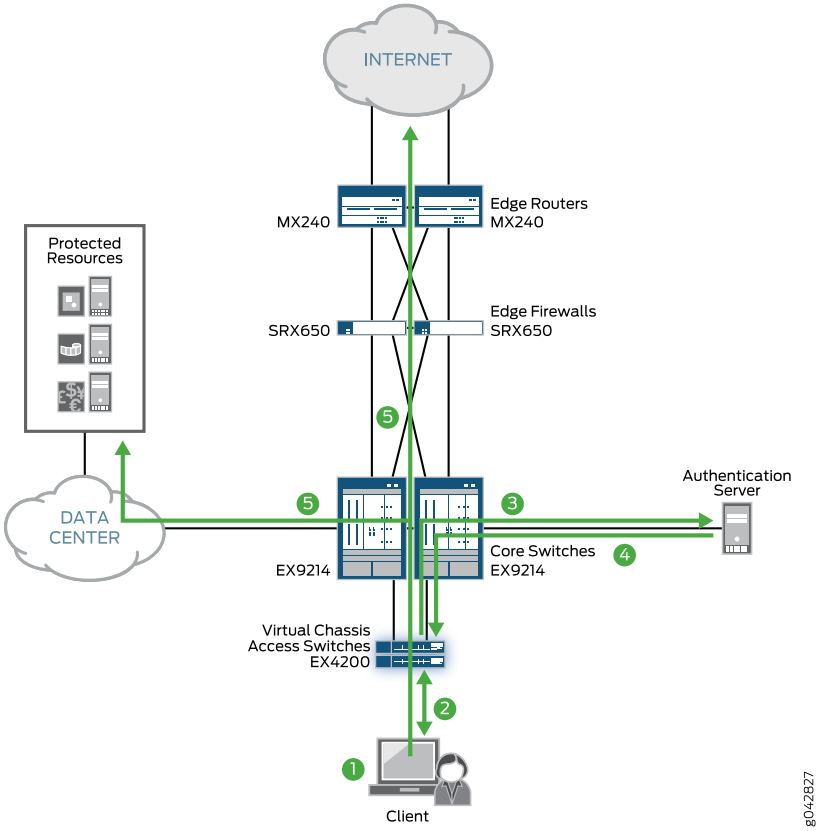
As an example, as part of testing this solution, Juniper Networks used Junos Pulse Access Control Service as the authentication server. This service was integrated with:

- An LDAP server to validate user credentials. The same LDAP server was used to validate the credentials of users connecting remotely.
- Host-checking software on the Junos Pulse client that acted as an 802.1X supplicant on Windows laptops. The host checker determined the status of the antivirus program on the laptop. If the laptop was not running the correct antivirus program or did not have the latest antivirus definitions, the Access Control Service returned to the switch the remediation VLAN ID and associated firewall filter. The filter restricted the user to accessing only the Access Control Service or a remediation server, from which the user could download and install the antivirus program.
- A mobile device management service that acted as an authorization server for mobile devices and pushed profiles to the devices to provision them after the devices were successfully authorized. The purpose of provisioning the devices was to ensure that they would use EAP-TTLS for authentication through the Access Control Service.

Traffic Flows During 802.1X Authentication

Figure 9 on page 30 illustrates the traffic flow during 802.1X authentication.

Figure 9: Traffic Flow During 802.1X Authentication



As illustrated in Figure 9 on page 30, the steps involved in granting an 802.1X supplicant access to the wired network are:

1. The employee connects the device to the access switch. The switch port blocks all traffic other than 802.1X traffic.
2. The switch begins 802.1X communications with the device, requesting the user credentials, while blocking all traffic other than 802.1.X traffic.

   If the 802.1X supplicant is nonresponsive or not enabled on the end device, the switch puts the port in the guest VLAN and assigns the firewall filter associated with the guest VLAN. The guest firewall filter allows access only to the authentication server and the remediation server. In this solution, the guest VLAN purpose is to quarantine the device and does not provide guest user access to the Internet.
3. When the switch receives credentials from the supplicant, it uses the RADIUS protocol to communicate the user credentials to the authentication server.
4. The authentication server validates the user credentials and returns a RADIUS response to the switch containing the VLAN and firewall filter associated with the user.

   If the client device fails host checking—for example, it does not have the correct antivirus program installed—the authentication server returns a RADIUS response containing the remediation VLAN and firewall filter. The remediation filter permits the

user access only to the authentication server and remediation server, quarantining the device.

5. The switch assigns the VLAN to the port and opens the port for user traffic, applying the firewall filter to the traffic. If the user was successfully validated and the user device passed host checking, the user can now access the Internet or the protected resources permitted by the firewall filter.

Headless devices, such as printers, security cameras, and VoIP phones, usually do not have an 802.1X supplicant. For such devices, you can enable MAC authentication on an 802.1X port, allowing connecting devices to be authenticated by their MAC addresses.

Headless devices are granted access to the network as follows:

1. The device is connected to the network.
2. The switch blocks any traffic other than 802.1X traffic on the port and waits for a response from an 802.1X supplicant on the device.
3. When the switch receives no response after a set timeout period, it sends the device's MAC address to the authentication server for authentication.
4. If the MAC address is registered with the authentication server, the server authenticates the device.
5. The authenticator opens the port and allows traffic on it.

It is also possible to configure a port so that only MAC authentication, and not 802.1X authentication, is allowed on the port. In this case, the switch does not wait for a response from an 802.1X supplicant on the connecting device—instead, it sends the MAC address directly to the authentication server for authentication.

Access Port Security

In addition to preventing unauthorized access, security design includes preventing various attacks, such as Layer 2 DoS attacks and address spoofing. DoS attacks can be prevented through ingress firewall filters (ACLs) and rate limiting. For address spoofing, we recommend that you enable the following security measures on access switches:

- DHCP snooping—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (the DHCP snooping database)
- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons
- IP source guard—Mitigates the effects of IP address spoofing attacks. The source IP address in a packet that is sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.

Remote Access Security

Users expect to be able to access the campus network remotely, from anywhere, at any time, using any device. In this solution, an SSL VPN provides remote access security for web-capable devices by intermediating the data that flows between external users and the enterprise's internal resources. During intermediation, the SSL VPN receives secure requests from the external, authenticated users and then makes requests to the internal resources on behalf of those users. The SSL VPN used in testing was the Junos Pulse Secure Access Service, which was integrated with an LDAP server for authenticating users.

Internet Edge Security

The SRX650 Services Gateways provide perimeter security services, stateful policy enforcement, and Network Address Translation (NAT) for Internet traffic that is entering or exiting the campus network.

Security Zones and Security Policies

The SRX Series Services Gateways are zone-based firewalls, enabling you to group interfaces with similar security requirements into security zones. You can then apply security policies to traffic as it traverses from one zone to another zone.

In the solution design, two security zones are defined:

- The trust zone, which contains the interfaces that connect to the core switch
- The untrust zone, which contains the interfaces that connect to the edge router

These zones are configured on the redundant Ethernet interfaces as shown in Figure 10 on page 32.

Figure 10: Security Zones

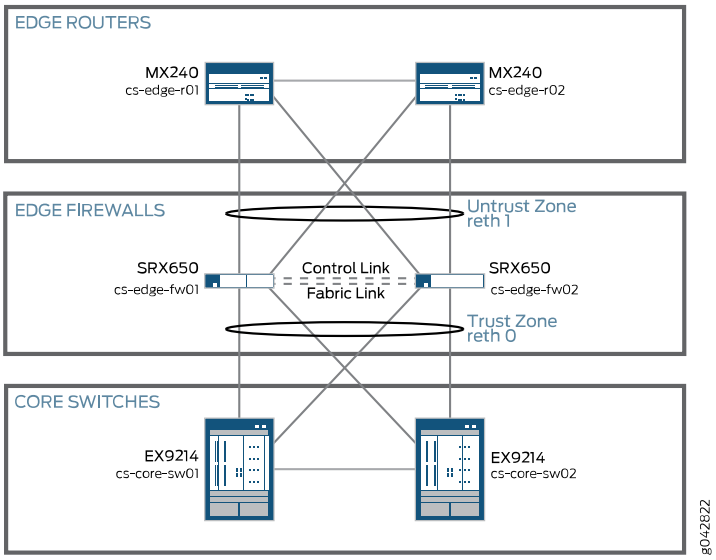


Table 4 on page 33 describes the security policies that govern traffic passing between zones.

Table 4: Zone Policies

From Zone	To Zone	Traffic Description	Policy
untrust	trust	Employee remote access	Permit all public sources addresses to access the SSL VPN service using HTTP and HTTPS only. All other inbound traffic is denied and logged.
trust	untrust	Employee Internet access	Permit all private source addresses within the trust zone to access the Internet with HTTP, HTTPS, DNS, NTP, UDP, and PING. All other outbound traffic is denied and logged.

In some campus environments, additional security policies might be needed. For example, you might require a security policy that allows external access to public domain servers, such as webservers.

Network Address Translation

To protect the internal IP address space, the SRX650 Services Gateways perform Network Address Translation (NAT).

In this solution:

- Outbound traffic uses source NAT. Source NAT translates private IP addresses to public IP addresses selected from a configurable pool. For the public IP addresses, we recommend using a source NAT pool instead of an interface IP pool because it provides more scale.
- Inbound traffic uses destination NAT. Destination NAT translates the public IP address of the Secure Access Service server to its private IP address.

Quality of Service Design

EX Series switches are designed to provide high quality of service (QoS) to end users and applications in the campus. Many EX Series features contribute to delivering high QoS—features such as high-bandwidth links, reduced latency through Virtual Chassis technology, fast route convergence, and so on. Nevertheless, it is still important to implement specific QoS policies. QoS is the manipulation of aggregates of traffic such that each aggregate is forwarded in a fashion that is consistent with the required behaviors of the application generating that traffic. QoS is mandatory for any campus deployment where there is potential for congestion or contention for resources.

- QoS and Service-Level Agreements on page 34
- Overview of QoS in the Campus LAN on page 34
- Deploying CoS in the Campus LAN on page 38

QoS and Service-Level Agreements

QoS policies are typically based on application. Each application has specific service-level agreements (SLAs) that must be considered when determining QoS policies for the campus. Table 5 on page 34 gives some baseline guidance for SLAs.

Table 5: Baseline SLAs for Campus Networks

Application Type	Campus SLA
Voice	Low latency—Less than 150 ms. Low jitter—Less than 20 ms. Low loss—Less than 1%. Bandwidth—Varies according to codec used. Traffic is generally smooth, with small variation in packet size.
Video	Low latency—Less than 150 ms. Low jitter—Less than 20 ms. Low loss—Less than 1%. Bandwidth—Varies according to codec and resolution used, but is significantly higher than voice. Traffic is highly variable and bursty in nature.
Data	Mission-critical data—Should be given higher priority in queuing and policing policies. Other data—Usually treated as best-effort traffic.

The above-mentioned SLAs are generic in nature and might not completely satisfy the requirements of your applications. Use these SLAs as a starting point for determining the SLAs required for your applications.

Overview of QoS in the Campus LAN

Junos OS provides the class-of-service (CoS) feature to allow you to configure an individual node to handle traffic in a way that is consistent with the end-to-end QoS policy. CoS consists of the following components:

- Forwarding Classes on page 34
- Classifiers on page 35
- Queues and Schedulers on page 36
- Policers on page 37
- Rewrite Rules on page 38

Forwarding Classes

A forwarding class is a means of aggregating traffic that has the same characteristics and that requires the same behavior as it flows through a network node. To share a forwarding class, traffic does not have to belong to the same application—it must merely require the same behavior.

A forwarding class is a label used entirely within a network node. A forwarding class does not explicitly appear outside a node. However, forwarding classes are usually implemented consistently across nodes in a campus network.

The forwarding classes used in a campus network depend, of course, on the applications supported and their SLAs. For this configuration example, five forwarding classes are used:

- Network control—For protocol control packets, which generally have a high priority.
- Voice—For voice traffic, which requires low loss, low latency, low jitter, assured bandwidth, and end-to-end service.
- Video—For video traffic. Video traffic is similar to voice traffic in its SLA requirements, but video traffic is bursty and requires more bandwidth to be allocated per stream.
- Mission critical—For data traffic that requires higher QoS than best effort, such as mission-critical applications or transactional applications.
- Best effort—All other traffic.

Some campus environments place video and voice into the same forwarding class; however, the bursty nature of video generally requires a different CoS policy than does voice.

Classifiers

Traffic must be classified before it can be assigned to a forwarding class. Junos OS supports three methods of classifying traffic:

- Interface-based—Traffic is classified by the interface it arrives on. Although interface-based classification is the simplest method, this configuration example does not use it because it means that all traffic arriving on an interface must require the same behavior.
- Behavior Aggregate (BA)—BA classification relies on markings placed in the headers of incoming frames or packets. Ethernet frames and IP packets include a field in their headers that indicates the class of the frame or packet—for example, Ethernet frames use three 802.1p bits while IPv4 packets use the 6-bit DiffServ Code Point (DSCP) field.

  This configuration example uses the DiffServe Code Points shown Table 6 on page 35 to map packets to their forwarding class.

Table 6: DiffServe Code Points Mapped to Forwarding Class

DiffServ Code Point	Forwarding Class
nc1	Network control
ef	Voice
af21	Video
af11	Mission critical

Table 6: DiffServe Code Points Mapped to Forwarding Class *(continued)*

DiffServ Code Point	Forwarding Class
be	Best effort

- Multifield—Multifield classification uses ingress firewall filters to classify traffic based on Layer 2, Layer 3, or Layer 4 information. Multifield classifier filters can be applied to Layer 2 or Layer 3 interfaces or to VLANs or to some combination of these. Because the multifield classifier filters are stored in Ternary Content Addressable Memory (TCAM), the same multifield classifier applied to multiple interfaces can consume TCAM memory. You can reduce TCAM consumption by applying the multifield classifier to VLANs instead. This configuration example uses multifield classification on access switches to classify packets on VLANs for client traffic.

Queues and Schedulers

You can configure each port on a switch to use up to 8 or up to 12 egress queues, depending on the switch model. The forwarding class of a packet determines which queue it is sent to for transmission.

Each queue has one or more schedulers associated with it—different schedulers can be applied to different interfaces. Schedulers determine when packets are placed on the interface from the queue in which they are waiting. When you define a scheduler, you can specify scheduling priority, buffer size, queue shaping, transmit rate, and drop profile, as described here:

- Scheduling priority—Priority can be either strict-high or shaped-deficit weighted round-robin (SDWRR). With strict-high priority scheduling, packets in higher priority queues are always transmitted before packets in lower priority queues. As long as the higher priority queue has packets waiting, the lower priority queues will not be serviced. Queue priority is determined by queue number—higher numbered queues always have a higher priority than lower numbered queues (for example, queue 7 has a higher priority than queue 6). Strict-high priority is used for queues that process traffic that is sensitive to delays, such as voice traffic.

  All other priorities result in the queues being serviced in an SDWRR fashion, with packets being transmitted sequentially, starting with the highest priority queue.

- Buffer size—Buffer size refers to the amount of buffer space allocated to a queue. Consider the following when configuring buffer size:

  - Because strict-high priority queues have a high transmit rate, they require smaller buffers. We recommend reserving a small percentage for strict-high priority queues.
  - SDWRR queues, in contrast, require larger buffers. The buffer size required can vary based on application load and requirements. A common practice is to match buffer size to transmit rate.
  - Voice traffic should not be buffered over a long period, because that increases latency and jitter. Instead, packets should be dropped. To achieve this, you can specify that the buffer size is exact, which prevents any excess voice packets from being buffered in the shared buffer.

- Queue shaping—Shaping limits the rate at which traffic can be transmitted. Traffic that does not conform to the shaper's criteria is held in the queue until it does conform. No explicit constraint is placed on more traffic entering the queue, as long as the queue is not full.

  Because packets in a strict-high priority queue are always transmitted before packets in a lower priority queue, a strict-high priority queue can potentially consume all the bandwidth and starve lower priority queues. We recommend that you use queue shaping on strict-high priority queues to prevent this situation from occurring.

- Transmit rate—Transmit rate specifies the portion of the total interface bandwidth that is allocated to the queue. This rate can be specified as a fixed value, as a percentage of the total bandwidth, or as the rest of the available bandwidth. Transmit rate is not applicable to strict-high priority queues, because these queues are always serviced when there are packets in the queue.

- Drop profile—Tail drop profile is a congestion management mechanism that allows a switch to drop arriving packets when queue buffers become full or begin to overflow. EX Series switches support either weighted tail drop (WTD) or weighted random early detection (WRED). If you do not explicitly configure a drop profile, a default tail drop profile is used.

  We recommend that you do not use WRED on queues that handle UDP traffic. UDP is often used by applications that are intolerant of loss, latency, and jitter. In addition, because UDP has no built-in mechanism for identifying the loss of a packet and modifying its rate of transmission, the packet is either lost (reducing the perceived QoS) without having significant impact on the throughput, or, worse, the application identifies the loss and demands retransmission of the packet, so the packet is then seen twice, potentially increasing the congestion.

  For this solution, the default drop profile is used. Specific drop profiles are not used because each type of traffic within the campus has its own queue and there is no need to differentially drop packets if the queue becomes congested.

Policers

Policing, or rate limiting, lets you control the amount of traffic that enters an interface. You can achieve policing by including policers in firewall filter configurations. A firewall filter configured with a policer permits only traffic within a specified set of rate limits, thereby providing protection from denial-of-service (DoS) attacks. Traffic that exceeds the rate limits specified by the policer is either discarded immediately or is marked as lower priority than traffic that is within the rate limits. The lower priority traffic is discarded when there is traffic congestion.

Hard-drop behavior can have a negative impact, particularly on TCP traffic and when the policer is run consistently at its limit. While it is possible to reclassify packets based on a policer, it is important to avoid reordering packets in applications that are sensitive to the order in which packets are received, such as voice, video, and other real-time traffic.

If traffic rate limiting is required in your implementation, policing should be done at the edge to control the load entering the network. This network configuration example does not implement policers.

Rewrite Rules

A rewrite rule sets the appropriate CoS bits in the outgoing packet, thus allowing the next downstream device to classify the packet into the appropriate service group. Rewriting, or remarking, outbound packets is generally done by edge devices. In this network configuration example, rewriting is done by the switches in the access layer.

Deploying CoS in the Campus LAN

CoS components are implemented on a per-hop basis, with each device being separately configured for CoS. The user, on the other hand, evaluates quality of experience based on the end-to-end traffic flow. Even though CoS is implemented on a per-hop basis, you must consider the end-to-end traffic flow when configuring CoS so that the resulting quality of experience is consistent with the desired end-to-end user experience or application behavior. Bear in mind that a single congested hop can destroy the end-to-end experience, and subsequent nodes can do nothing to recover the end-to-end quality of experience for the user.

This network configuration example implements CoS at the access, aggregation, and core layers. Your organization might want to extend the CoS implementation to include the edge firewalls and routers.

In developing your implementation strategy, it is useful to divide your network into trusted and untrusted domains. Trust and untrust are commonly used terms in a security context, but they can also be used in QoS. An edge device (such as an access switch or a router connecting to the Internet) resides between the trusted and untrusted boundary. These are the first and last entry points into and out of the campus network. The CoS markings on packets coming from the untrusted domain might not conform to the campus QoS policy, but once packets enter the campus LAN, network administrators have complete control and can manipulate packets so that they comply with the established QoS strategy.

For this solution, traffic within the campus LAN is trusted, while traffic arriving at the access layer is untrusted.

Related Documentation

- Example: Configuring High Availability for the Midsize Enterprise Campus on page 39
- Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus on page 85
- Example: Configuring Access Policy and Security for the Midsize Enterprise Campus on page 114
- Example: Configuring Class of Service for the Midsize Enterprise Campus on page 137

Example: Configuring High Availability for the Midsize Enterprise Campus

This example details the steps required on the devices in access, aggregation, core, and edge layers to configure them to meet the high availability goals described in "Understanding the Design of the Midsize Enterprise Campus Solution" on page 6.

Requirements

Table 7 on page 39 shows the hardware and software requirements for this example. Table 8 on page 39 shows the scaling and performance targets used for this example.

Table 7: Hardware and Software Requirements

Hardware	Device Name	Software
MX240	cs-edge-r01, cs-edge-r02	13.2 R2.4
SRX650	cs-edge-fw-01, cs-edge-fw02	12.1 X44-D39.4
EX9214	cs-core-sw01, cs-core-sw02	13.2 R3.7
EX4550	cs-agg-01	12.3 R3.4
EX2200	cs-2200-ab5	12.3 R3.4
EX3300	cs-3300-ab4	12.3 R3.4
EX4200	cs-4200-ab1	12.3 R3.4
EX4300	cs-4300-ab2, cs-4300-ab3	13.2 X51-D21.1

Table 8: Node Features and Performance/Scalability

Node	Features	Performance/Scalability Target Value
Edge (MX240, SRX650)	MC-LAG, OSPF, BGP, IRB	3k IPv4

Table 8: Node Features and Performance/Scalability *(continued)*

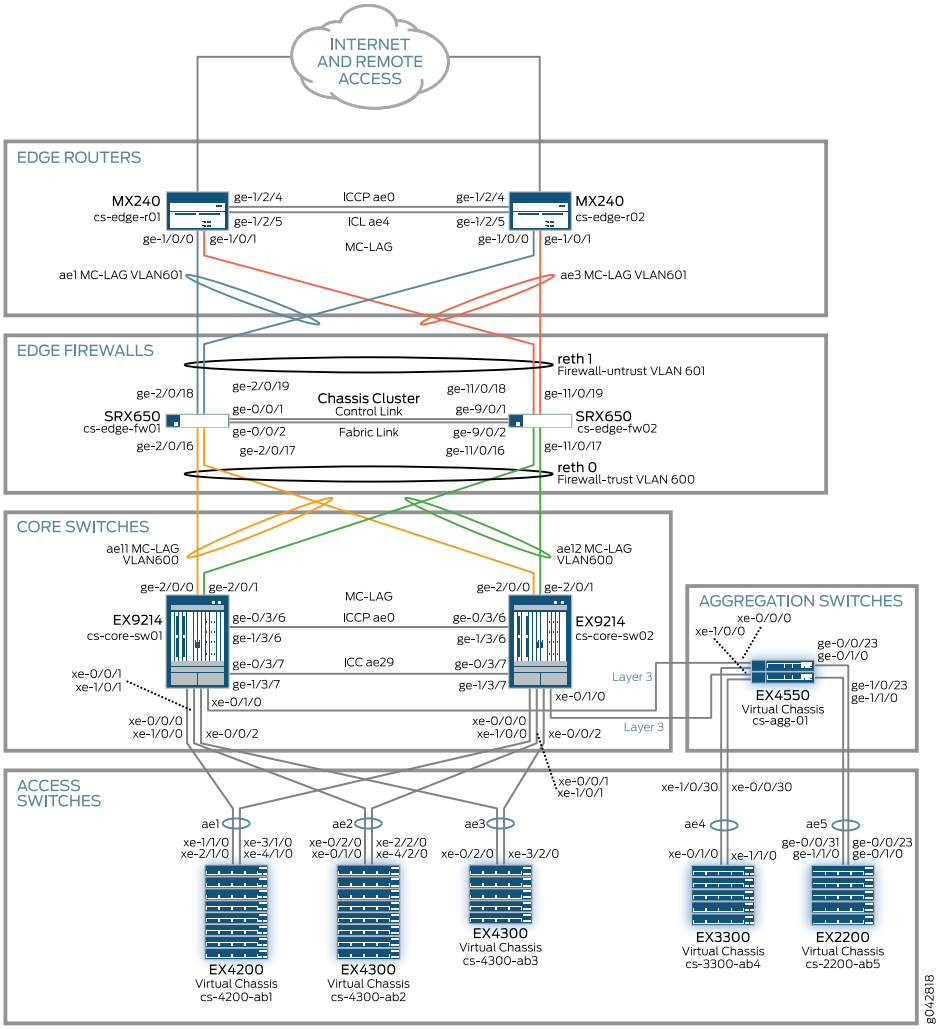
Node	Features	Performance/Scalability Target Value
Core (EX9214)	VLANs, MC-LAG, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, IRB	3k IPv4 routes 128k MAC table entries 16k ARP entries
Aggregation (EX4550)	VLANs, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, RVI	3k IPv4 routes 5 IGMP groups
Access (EX3300, EX4300, EX4200)	VLANs, LAG, 802.1X, IGMP snooping, DHCP snooping, ARP inspection, IP source guard	55k MAC table entries 13k 8021.x users 5 IGMP groups

The configuration procedures that follow assume that all physical cabling has been completed and that the devices have been initially configured.

Overview and Topology

Figure 11 on page 41 shows the topology used for this example.

Figure 11: High Availability Topology



In this topology, all access switches in location A are in a Virtual Chassis configuration. Link aggregation is configured on the uplink ports to the EX9214 switches, giving each Virtual Chassis a physical connection to each EX9214 switch. Similarly, the access switches in location B are in a Virtual Chassis configuration and have link aggregation configured on the uplink ports to the EX4550 Virtual Chassis, giving each access Virtual Chassis a physical link to each member of the EX4550 Virtual Chassis.

For node redundancy in the core and edge layers:

- The EX9214 switches are in an active/active MC-LAG configuration. MC-LAG interfaces ae1, ae2, and ae3 connect to the access switches in location A, and MC-LAG interfaces ae11 and ae12 connect to the SRX650 gateways.
- The SRX650 gateways are in an active/standby chassis cluster configuration, with redundant Ethernet interfaces reth0 and reth1 connecting to the EX9214 core switches and the MX240 edge routers.

- The MX240 routers are in an active/active MC-LAG configuration, with MC-LAG interfaces ae1 and ae3 connecting to the SRX650 gateways.

Configuring the Access Switches for High Availability

This section provides step-by-step procedures for configuring the access switches in the access layer for high availability. It uses configuring the cs-4200-ab1 Virtual Chassis as an example—you can use the same basic procedures to configure the other Virtual Chassis in the access layer.

To configure the access switches for high availability:

- Configure the Virtual Chassis on page 42
- Configure the LAG Interface Towards the Core or Aggregation Layer on page 43
- Configure the High Availability Software on page 44

Configure the Virtual Chassis

Step-by-Step Procedure

To configure the Virtual Chassis:

- Define the members of the Virtual Chassis and their roles.

```
[edit]
user@cs-4200-ab1#  set virtual-chassis preprovisioned
user@cs-4200-ab1#  set virtual-chassis member 0 role line-card
user@cs-4200-ab1# set virtual-chassis member 0 serial-number BP0213230308
user@cs-4200-ab1#  set virtual-chassis member 1 role routing-engine
user@cs-4200-ab1#  set virtual-chassis member 1 serial-number BP0213260624
user@cs-4200-ab1#  set virtual-chassis member 2 role routing-engine
user@cs-4200-ab1# set virtual-chassis member 2 serial-number BP0213260668
user@cs-4200-ab1#  set virtual-chassis member 3 role line-card
user@cs-4200-ab1# set virtual-chassis member 3 serial-number BP0213260540
user@cs-4200-ab1#  set virtual-chassis member 4 role line-card
user@cs-4200-ab1# set virtual-chassis member 4 serial-number BP0213260532
user@cs-4200-ab1#  set virtual-chassis member 5 role line-card
user@cs-4200-ab1# set virtual-chassis member 5 serial-number BP0213230346
user@cs-4200-ab1#  set virtual-chassis member 6 role line-card
user@cs-4200-ab1#  set virtual-chassis member 6 serial-number FP0213313963
user@cs-4200-ab1#  set virtual-chassis member 7 role line-card
user@cs-4200-ab1#  set virtual-chassis member 7 serial-number BP0213310009
user@cs-4200-ab1#  set virtual-chassis member 8 role line-card
user@cs-4200-ab1# set virtual-chassis member 8 serial-number BP0213260607
user@cs-4200-ab1#  set virtual-chassis member 9 role line-card
user@cs-4200-ab1# set virtual-chassis member 9 serial-number BP0213230403
```

Configure the LAG Interface Towards the Core or Aggregation Layer

Step-by-Step Procedure

The following procedure shows how to configure ae1 on cs-4200-ab1. You can use the same procedure for the LAGs on the other switches, substituting the information shown in Table 9 on page 43.

Table 9: LAG Interfaces in the Access Layer

Virtual Chassis	LAG Name	Description String	Member Interfaces
cs-4200-ab1	ae1	"MCLAG towards core-sw1 and core-sw2"	xe-1/1/0, xe-2/1/0, xe-3/1/0, xe-4/1/0
cs-4300-ab2	ae2	"MCLAG towards core-sw1 and core-sw2"	xe-0/2/0, xe-1/2/0, xe-2/2/0, xe-4/2/0
cs-4300-ab3	ae3	"MCLAG towards core-sw1 and core-sw2"	xe-0/2/0, xe-3/2/0
cs-3300-ab4	ae4	"MCLAG towards cs-agg"	xe-0/1/0, xe-1/1/0
cs-2200-ab5	ae5	"MCLAG towards cs-agg"	ge-0/0/23, ge-0/1/0, ge-1/0/23, ge-1/1/0

To configure ae1 on cs-4200-ab1:

1. Specify the number of LAG interfaces on the device.

```
{master:1}[edit]
user@cs-4200-ab1# set chassis aggregated-devices ethernet device-count 3
```

2. Configure the LAG settings for ae1.

```
{master:1}[edit]
user@cs-4200-ab1# set interfaces ae1 description "MCLAG towards core-sw1 and
 core-sw2"
user@cs-4200-ab1# set interfaces ae1 aggregated-ether-options lacp active
user@cs-4200-ab1# set interfaces ae1 aggregated-ether-options lacp periodic
fast
```

3. Specify the members of the LAG.

```
{master:1}[edit]
user@cs-4200-ab1# set interfaces xe-1/1/0 ether-options 802.3ad ae1
user@cs-4200-ab1# set interfaces xe-2/1/0 ether-options 802.3ad ae1
```

```
user@cs-4200-ab1# set interfaces xe-3/1/0 ether-options 802.3ad ae1
user@cs-4200-ab1# set interfaces xe-4/1/0 ether-options 802.3ad ae1
```

4. Configure the LAG interface as a trunk interface with membership in all VLANs.

   The configuration statements used on an EX4300 switch differ from the statements used on the other EX Series switches. Examples of both configurations are shown.

   On EX2200, EX3300, and EX4200 switches, enter:

   ```
   {master:1}[edit]
   user@cs-4200-ab1# set interfaces ae1 unit 0 family ethernet-switching port-mode
    trunk
   user@cs-4200-ab1# set interfaces ae1 unit 0 family ethernet-switching vlan
   members all
   ```

   On EX4300 switches, enter:

   ```
   {master:1}[edit]
   user@cs-4300-ab3# set interfaces ae3 unit 0 family ethernet-switching
   interface-mode trunk
   user@cs-4300-ab3# set interfaces ae3 unit 0 family ethernet-switching vlan
   members all
   ```

Configure the High Availability Software

Step-by-Step Procedure

To enable graceful Routing Engine switchover (GRES), nonstop active routing (NSR), and nonstop bridging (NSB):

- Enter the following configuration statements:

  On EX2200, EX3300, and EX4200 switches, enter:

  ```
  {master:1}[edit]
  user@cs-4200-ab1# set chassis redundancy graceful-switchover
  user@cs-4200-ab1# set ethernet-switching-options nonstop-bridging
  user@cs-4200-ab1# set routing-options nonstop-routing
  ```

  On EX4300 switches, enter:

  ```
  {master:1}[edit]
  user@cs-4300-ab3# set chassis redundancy graceful-switchover
  user@cs-4300-ab3# set protocols layer2-control nonstop-bridging
  user@cs-4300-ab31#  set routing-options nonstop-routing
  ```

Configuring the Aggregation Switches for High Availability

In location B, two EX4550 switches in a Virtual Chassis configuration function as the aggregation switch. For link redundancy, LAG interfaces ae4 and ae5 connect the aggregation switch to the access switches cs-3300-ab4 and cs-2200-ab5, respectively.

To configure the aggregation switches for high availability:

- Configure the EX4550 Virtual Chassis on page 45
- Configure the LAG Interfaces Towards the Access Layer on page 45
- Configure the High Availability Software on page 45

Configure the EX4550 Virtual Chassis

Step-by-Step Procedure

To configure the Virtual Chassis:

- Enter the following commands:

```
[edit]
user@cs-agg-01# set virtual-chassis preprovisioned
user@cs-agg-01# set virtual-chassis no-split-detection
user@cs-agg-01# set virtual-chassis member 0 role routing-engine
user@cs-agg-01# set virtual-chassis member 0 serial-number LX0213439586
user@cs-agg-01# set virtual-chassis member 1 role routing-engine
user@cs-agg-01# set virtual-chassis member 1 serial-number LX0213449606
```

Configure the LAG Interfaces Towards the Access Layer

Step-by-Step Procedure

To configure the LAG interfaces:

1. Specify the number of LAG interfaces on the device.

```
{master:0}[edit]
user@cs-agg-01# set chassis aggregated-devices ethernet device-count 10
```

2. Configure ae4.

```
{master:0}[edit]
user@cs-agg-01# set interfaces ae4 aggregated-ether-options lacp active
user@cs-agg-01# set interfaces ae4 aggregated-ether-options lacp periodic fast
user@cs-agg-01# set interfaces ae4 unit 0 family ethernet-switching port-mode
 trunk
user@cs-agg-01# set interfaces ae4 unit 0 family ethernet-switching vlan members
 all
user@cs-agg-01# set interfaces xe-0/0/30 ether-options 802.3ad ae4
user@cs-agg-01# set interfaces xe-1/0/30 ether-options 802.3ad ae4
```

3. Configure ae5.

```
{master:0}[edit]
user@cs-agg-01# set interfaces ae5 aggregated-ether-options lacp active
user@cs-agg-01# set interfaces ae5 aggregated-ether-options lacp periodic fast
user@cs-agg-01# set interfaces ae5 unit 0 family ethernet-switching port-mode
 trunk
user@cs-agg-01# set interfaces ae5 unit 0 family ethernet-switching vlan members
 all
user@cs-agg-01# set interfaces ge-0/0/23 ether-options 802.3ad ae5
user@cs-agg-01# set interfaces ge-1/0/23 ether-options 802.3ad ae5
user@cs-agg-01# set interfaces ge-0/0/31 ether-options 802.3ad ae5
user@cs-agg-01# set interfaces ge-1/0/31 ether-options 802.3ad ae5
```

Configure the High Availability Software

Step-by-Step Procedure

To enable graceful Routing Engine switchover (GRES), nonstop active routing (NSR), and nonstop bridging (NSB):

- Enter the following configuration statements:

```
{master:0}[edit]
user@cs-agg-01# set chassis redundancy graceful-switchover
user@cs-agg-01# set ethernet-switching-options nonstop-bridging
user@cs-agg-01# set routing-options nonstop-routing
```

Configuring the Core Switches for High Availability

The section provides the procedures for configuring the core switches in an active/active MC-LAG configuration.

To configure the core switches for high availability:

Configure the Number of Aggregated Ethernet Interfaces and Switch Service ID

Step-by-Step Procedure

This procedure configures two global settings for the switch:

- Number of aggregated Ethernet Interfaces—You must specify the number of aggregated Ethernet interfaces that will be configured on the device.
- Service ID—You must configure a service ID when the MC-LAG logical interfaces are part of a bridge domain, as they are in this example. The service ID is used to synchronize applications such as IGMP, ARP, and MAC learning across MC-LAG members.

1. Specify the number of aggregated Ethernet interfaces to be created.

   ```
   {master}[edit]
   user@cs-core-sw1# set chassis aggregated-devices ethernet device-count 32
   ```

2. Specify the switch service ID.

   ```
   {master}[edit]
   user@cs-core-sw1# set switch-options service-id 1
   ```

Configure the Inter-Chassis Control Protocol (ICCP) and ICCP Link

Step-by-Step Procedure

ICCP is a control plane protocol for MC-LAG. It uses TCP as a transport protocol and Bidirectional Forwarding Detection (BFD) for fast convergence. ICCP:

- Synchronizes configurations and operational states between the two MC-LAG peers
- Synchronizes MAC address and ARP entries learned from one MC-LAG node and shares them with the other peer

In the testing for this network configuration example, we achieved quicker convergence after a Routing Engine switchover by configuring a 3-second BFD timer for ICCP.

To configure ICCP and the ICCP link:

1. Specify the members that belong to interface ae0, which is used for the ICCP link.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set interfaces xe-0/3/6 ether-options 802.3ad ae0
   user@cs-core-sw1# set interfaces xe-1/3/6 ether-options 802.3ad ae0
   ```

2. Configure ae0 as a Layer 3 link.

   On cs-core-sw1, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set interfaces ae0 description "ICCP Layer 3 Link with 2
   member,xe-0/3/6,xe-1/3/6"
   user@cs-core-sw1# set interfaces ae0 vlan-tagging
   user@cs-core-sw1# set interfaces ae0 aggregated-ether-options lacp active
   user@cs-core-sw1# set interfaces ae0 aggregated-ether-options lacp periodic
   fast
   user@cs-core-sw1# set interfaces ae0 unit 0 vlan-id 4000
   user@cs-core-sw1# set interfaces ae0 unit 0 family inet address 172.16.32.9/30
   ```

   On cs-core-sw2, enter:

   ```
   {master}[edit]
   user@cs-core-sw2# set interfaces ae0 description "ICCP Layer 3 Link with 2
   member,xe-0/3/6,xe-1/3/6"
   user@cs-core-sw2# set interfaces ae0 vlan-tagging
   user@cs-core-sw2# set interfaces ae0 aggregated-ether-options lacp active
   user@cs-core-sw2# set interfaces ae0 aggregated-ether-options lacp periodic
   fast
   user@cs-core-sw2# set interfaces ae0 unit 0 vlan-id 4000
   user@cs-core-sw2# set interfaces ae0 unit 0 family inet address 172.16.32.10/30
   ```

3. Configure ICCP, using the loopback addresses of cs-core-sw1 (172.16.32.5) and cs-core-sw2 (172.16.32.6) as the local IP addresses.

   On cs-core-sw1, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set protocols iccp local-ip-addr 172.16.32.5
   user@cs-core-sw1# set protocols iccp peer 172.16.32.6 redundancy-group-id-list
   1
   ```

```
user@cs-core-sw1# set protocols iccp peer 172.16.32.6 liveness-detection
minimum-interval 1500
user@cs-core-sw1# set protocols iccp peer 172.16.32.6 liveness-detection multiplier
2
```

On cs-core-sw2, enter:

```
{master}[edit]
user@cs-core-sw2# set protocols iccp local-ip-addr 172.16.32.6
user@cs-core-sw2# set protocols iccp peer 172.16.32.5 redundancy-group-id-list
1
user@cs-core-sw2# set protocols iccp peer 172.16.32.5 liveness-detection
minimum-interval 1500
user@cs-core-sw2# set protocols iccp peer 172.16.32.5 liveness-detection multiplier
2
```

Together, the liveness-detection statements result in a BFD timer of 3 seconds (1.5 seconds * 2 multiplier).

Configure the Interchassis Link (ICL)

Step-by-Step Procedure

The ICL is a special Layer 2 link between peers in an active/active MC-LAG configuration. It provides redundancy when an active link to an MC-LAG node fails by permitting the nodes to forward traffic between them.

We recommend that you configure the ICL members with a hold-time down value that is higher than the configured BFD timer to prevent the ICL from being advertised as being down before the ICCP link is down. If the ICL goes down before the ICCP link, this causes a flap of the MC-LAG interface on the status-control standby node, which leads to a delay in convergence. This example uses a hold-time down value of 4 seconds (4000 ms), based on the ICCP BFD timer of 3 seconds. These values result in zero loss convergence during recovery of failed devices.

To configure the ICL:

1. Configure ICL members with a hold-time value higher than the configured BFD timer.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set interfaces xe-0/3/7 hold-time up 100
   user@cs-core-sw1# set interfaces xe-0/3/7 hold-time down 4000
   user@cs-core-sw1# set interfaces xe-0/3/7 ether-options 802.3ad ae29
   user@cs-core-sw1# set interfaces xe-1/3/7 hold-time up 100
   user@cs-core-sw1# set interfaces xe-1/3/7 hold-time down 4000
   user@cs-core-sw1# set interfaces xe-1/3/7 ether-options 802.3ad ae29
   ```

   NOTE: If you configure a hold-time down value, you must also configure a hold-time up value. We have chosen a minimal value for hold-time up in this configuration.

2. Configure ae29, which is the LAG for the ICL.

On both cs-core-sw1 and cs-core-sw2, enter:

```
{master}[edit]
user@cs-core-sw1#  set interfaces ae29 description "ICL Layer 2 link with 2
members,xe-0/3/7,1/3/7"
user@cs-core-sw1# set interfaces ae29 vlan-tagging
user@cs-core-sw1# set interfaces ae29 aggregated-ether-options lacp active
user@cs-core-sw1# set interfaces ae29 aggregated-ether-options lacp periodic
fast
user@cs-core-sw1# set interfaces ae29 unit 0 family ethernet-switching
interface-mode trunk
user@cs-core-sw1# set interfaces ae29 unit 0 family ethernet-switching vlan
members all
```

Configure the MC-LAG Links to the Access Layer

Step-by-Step Procedure

The core switches establish an MC-LAG link to each of the Virtual Chassis in the access layer. To create the MC-LAG link, you create an aggregated Ethernet interface, enable LACP on the interface, and configure the MC-LAG options under the **mc-ae** statement.

Table 10 on page 49 describes the **mc-ae** options.

Table 10: mc-ae Statement Options

mc-ae Option	Description
mc-ae-id	Specifies which link aggregation group the aggregated Ethernet interface belongs to. In this solution, the **mc-ae-id** used matches the number of the aggregated Ethernet interface—that is, ae1 has a **mc-ae-id** of 1, ae2 has a **mc-ae-id** of 2, and ae3 has a **mc-ae-id** of 3.
redundancy-group	Used by ICCP to associate multiple chassis that perform similar redundancy functions and to establish a communication channel so that applications on peering chassis can send messages to each other. The MC-LAG interfaces on cs-core-sw1 and cs-core-sw2 are configured with the same redundancy group number, **redundancy-group 1**.
init-delay-time	Specifies the number of seconds by which to delay bringing the MC-LAG interface back to the up state when MC-LAG peer is rebooted. By delaying the bring up of the interface until after protocol convergence, you can prevent packet loss during the recovery of failed links and devices. In this solution, we found that a delay set to 520 seconds provided the quickest convergence after core switch failover. Configure this value for all MC-LAG interfaces on the core switches.
chassis-id	Used by LACP for calculating the port number of the MC-LAG physical member links. cs-core-sw1 uses **chassis-id** 0 to identify its MC-LAG interfaces. cs-core-sw2 uses **chassis-id** 1 to identify its MC-LAG interfaces.

Table 10: mc-ae Statement Options *(continued)*

mc-ae Option	Description
mode	Indicates whether an MC-LAG is in active/standby mode or active/active mode. Chassis that are in the same group must be in the same mode. In this solution, the mode is active/active.
status-control	Specifies whether this node becomes active or goes into standby mode when an ICL failure occurs. Must be **active** on one node and **standby** on the other node.
events iccp-peer-down force-icl-down	Forces ICL down if the peer of this node goes down.
events iccp-peer-down prefer-status-control-active	Allows the LACP system ID to be retained during a reboot, which provides better convergence after a failover. Note that if you configure both nodes as **prefer-status-control-active**, as this configuration example shows, you must also configure ICCP peering using the peer's loopback address to make sure the ICCP session does not go down due to physical link failure.

The following procedure shows how to configure the ae1 MC-LAG link to cs-4200-ab1. You can use the same procedure to configure the links to the other access switches, substituting the values shown in Table 11 on page 50.

Table 11: Parameters for MC-LAGs to Access Switches

LAG	LAG Client	Member Interfaces	lacp system-id	lacp admin-key	mc-ae mc-ae-id
ae1	cs-4200-ab1	xe-0/0/0 xe-1/0/0	00:ae:01:00:00:01	1	1
ae2	cs-4300-ab2	xe-0/0/1 xe-1/0/1	00:ae:02:00:00:01	2	2
ae3	cs-4300-ab3	xe-0/0/2	00:ae:03:00:00:01	3	3

To configure the ae1 MC-LAG link to cs-4200-ab1:

1. Specify the members to be included within the aggregated Ethernet interface ae1.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set interfaces xe-0/0/0 ether-options 802.3ad ae1
   user@cs-core-sw1# set interfaces xe-1/0/0 ether-options 802.3ad ae1
   ```

2. Configure the LACP parameters on the aggregated Ethernet interface.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   {master}[edit]
   user@cs-core-sw1# set interfaces ae1 description "Layer 2 MCLAG between core
    & AB1,xe-0/0/0,1/0/0"
   ```

```
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options lacp active
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options lacp periodic fast
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options lacp
system-priority 100
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options lacp system-id
00:ae:01:00:00:01
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options lacp admin-key
1
```

3. Configure the mc-ae interface parameters.

   On cs-core-sw1, enter:

```
{master}[edit]
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id
1
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae
redundancy-group 1
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae chassis-id
0
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae mode
active-active
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae
status-control active
user@cs-core-sw1# set  interfaces ae1 aggregated-ether-options mc-ae
init-delay-time 520
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-core-sw1# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
user@cs-core-sw1# set interfaces ae1 unit 0 multi-chassis-protection 172.16.32.6
 interface ae29.0
```

   On cs-core-sw2, enter:

```
{master}[edit]
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id
1
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae
redundancy-group 1
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae chassis-id
1
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae mode
active-active
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae
status-control standby
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae
init-delay-time 520
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-core-sw2# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
user@cs-core-sw2# set interfaces ae1 unit 0 multi-chassis-protection 172.16.32.5
 interface ae29.0
```

4. Configure ae1 as a trunk port, with membership in all VLANS.

   On both cs-core-sw1 and cs-core-sw2, enter:

```
user@cs-core-sw1# set interfaces ae1 unit 0 family ethernet-switching
interface-mode trunk
user@cs-core-sw1# set interfaces ae1 unit 0 family ethernet-switching vlan
members all
```

Configure the MC-LAG Links to the Edge Firewalls

Step-by-Step Procedure

The following procedure shows how to configure the ae11 MC-LAG link to cs-edge-fw01 on cs-core-sw01 and cs-core-sw02. You can use the same procedure to configure the ae12 MC-LAG link to cs-edge-fw02 on both switches, substituting the values shown in Table 12 on page 52.

Table 12: Parameters for Edge Router MC-LAG Interfaces Connecting to Edge Firewalls

LAG	LAG Client	Member Interface	lacp system-id	lacp admin-key	mc-ae mc-ae-id
ae11	reth 0 on cs-edge-fw01	ge-2/0/0	00:ae:11:00:00:01	11	11
ae12	reth 0 on cs-edge-fw02	ge-2/0/1	00:ae:12:00:00:01	12	12

To configure the ae11 MC-LAG link to the core switches:

1. Specify the interface to be included within the aggregated Ethernet interface ae11.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   user@cs-core-sw1# set interfaces ge-2/0/0 ether-options 802.3ad ae11
   ```

2. Configure the LACP parameters on the aggregated Ethernet interface.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   user@cs-core-sw1# set interfaces ae11 description "MC-LAG to edge-fw1"
   user@cs-core-sw1# set interfaces ae11 vlan-tagging
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options lacp active
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options lacp periodic
   fast
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options lacp
   system-priority 100
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options lacp system-id
    00:ae:11:00:00:01
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options lacp admin-key
    11
   ```

3. Configure the mc-ae interface parameters.

   On cs-core-sw1, enter:

   ```
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae mc-ae-id
    11
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae
   redundancy-group 1
   user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae chassis-id
   ```

```
0
user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae mode
active-active
user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae
status-control active
user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae
init-delay-time 520
user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-core-sw1# set interfaces ae11 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
```

On cs-core-sw2, enter:

```
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae mc-ae-id
11
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae
redundancy-group 1
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae chassis-id
1
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae mode
active-active
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae
status-control standby
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae
init-delay-time 520
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-core-sw2# set interfaces ae11 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
```

4. Configure ae11.0 as a trunk interface and as a member of the Firewall-trust VLAN.

   On cs-core-sw1, enter:

```
user@cs-core-sw1# set interfaces ae11 vlan-tagging
user@cs-core-sw1# set interfaces ae11 unit 0 family ethernet-switching
interface-mode trunk
user@cs-core-sw1# set interfaces ae11 unit 0 family ethernet-switching vlan
members Firewall-trust
user@cs-core-sw1# set interfaces ae11 unit 0 multi-chassis-protection 172.16.32.6
interface ae29.0
```

   On cs-core-sw2, enter:

```
user@cs-core-sw2# set interfaces ae11 vlan-tagging
user@cs-core-sw2# set interfaces ae11 unit 0 family ethernet-switching
interface-mode trunk
user@cs-core-sw2# set interfaces ae11 unit 0 family ethernet-switching vlan
members Firewall-trust
user@cs-core-sw2# set interfaces ae11 unit 0 multi-chassis-protection 172.16.32.5
interface ae29.0
```

Configure the Bridge Domain on the MC-LAG Interfaces to the Edge Firewalls

Step-by-Step Procedure

The active node in the SRX chassis cluster uses gratuitous ARP to advertise to connecting devices that it is the next-hop gateway. This requires that the interfaces between the connecting devices and the SRX chassis cluster be in the same bridge domain.

Table 13 on page 54 summarizes the configuration of this bridge domain.

Table 13: VLAN 600 Configuration

VLAN Name	VLAN ID	IRB Name	IP Address Information			
			Mask	cs-core-sw01 Address	cs-core-sw01 Address	Virtual IP Address
Firewall-Trust	600	irb.600	/29	172.16.33.3	172.16.33.2	172.16.33.1

To configure the required bridge domain:

1. Create the bridge domain.

   On cs-core-sw1, enter:

   ```
   user@cs-core-sw1# set vlans Firewall-trust vlan-id 600
   user@cs-core-sw1# set vlans Firewall-trust l3-interface irb.600
   user@cs-core-sw1# set vlans Firewall-trust switch-options interface ae29.0
   static-mac 28:8a:1c:e5:3b:f0
   user@cs-core-sw1# set vlans Firewall-trust domain-type bridge
   ```

   On cs-core-sw2, enter:

   ```
   user@cs-core-sw2# set vlans Firewall-trust vlan-id 600
   user@cs-core-sw2# set vlans Firewall-trust l3-interface irb.600
   user@cs-core-sw2# set vlans Firewall-trust switch-options interface ae29.0
   static-mac 28:8a:1c:e3:f7:f0
   user@cs-core-sw2# set vlans Firewall-trust domain-type bridge
   ```

NOTE: The **static-mac** option on VLAN 600 (Firewall-trust) prevents traffic arriving from the SRX chassis cluster from flooding the VLAN.

The SRX chassis cluster sends traffic to both core switches using the IRB 600 MAC address for routing the packet. The IRB 600 MAC addresses on cs-core-sw1 and cs-core-sw2 are different. Because the reth1 interface on the chassis cluster is a single LAG, the reth0 LAG address hashing results in a packet destined to the cs-core-sw1 MAC address being sent to cs-core-sw2. In an MC-LAG configuration, MAC address learning does not occur on the ICL link, and, as a result, cs-core-sw2 floods the packet on VLAN 600. To avoid flooding on VLAN 600, specify the MAC address for cs-core-sw1 in the **static-mac** option on cs-core-sw2 and vice versa. When a packet destined to cs-core-sw1 arrives at cs-core-sw2, cs-core-sw2 sends the packet to cs-core-sw1 using the static MAC address.

2. Configure an IRB interface on the VLAN and enable VRRP on the IRB interface.

   On cs-core-sw1, enter:

```
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 arp 172.16.33.2 l2-interface ae29.0
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 arp 172.16.33.2 mac 28:8a:1c:e5:3b:f0
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 virtual-address 172.16.33.1
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 priority 125
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 preempt
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 accept-data
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 authentication-type md5
user@cs-core-sw1# set interfaces irb unit 600 family inet address 172.16.33.3/29
 vrrp-group 1 authentication-key "$9$9FCMt0IylMNdsEcds24DjCtu"
```

   On cs-core-sw2, enter:

```
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 arp 172.16.33.3 l2-interface ae29.0
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 arp 172.16.33.3 mac 28:8a:1c:e3:f7:f0
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 virtual-address 172.16.33.1
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 priority 125
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 preempt
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 accept-data
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 authentication-type md5
user@cs-core-sw2# set interfaces irb unit 600 family inet address 172.16.33.2/29
 vrrp-group 1 authentication-key "$9$p11sOIcKMXbs4yls4aZkquO1"
```

Configure Hold-Up Timers on Other Interfaces

Step-by-Step Procedure

In addition to the MC-LAG interfaces, the core switches have other Layer 2 and Layer 3 interfaces, such as the Layer 3 interface connecting to the aggregation switch in location B. To avoid having these interfaces come up before the MC-LAG synchronization completes after a failover, you can configure a hold-up timer on the interfaces. The interfaces will not come up until the timer expires.

In our testing, we found that a hold-up timer of 467 seconds gave the best convergence results.

To configure the hold-up timer on an interface (in this case, the interface connecting to aggregation switch):

- On both cs-core-sw1 and cs-core-sw2, enter the following configuration statements:

```
user@cs-core-sw1# set  interfaces xe-0/1/0 hold-time up 467000
user@cs-core-sw1# set  interfaces xe-0/1/0 hold-time down 10
```

Configure VRRP on IRB Interfaces

Step-by-Step Procedure

VRRP is used in conjunction with MC-LAG on the core switches. VRRP permits redundant routers to appear as a single virtual router to the other devices. In a VRRP implementation, each VRRP peer shares a common virtual IP address and virtual MAC address in addition to its unique physical IP address and MAC address. Thus, each IRB configured on the core switches must have a virtual IP address.

To configure VRRP on an IRB—in this case, the IRB that is the Layer 3 interface for the eng1_data_wired VLAN:

1. Configure the eng1_data_wired VLAN and the IRB as the routing interface for the VLAN.

   On both cs-core-sw1 and cs-core-sw2, enter:

   ```
   user@cs-core-sw1# set vlans eng1_data_wired vlan-id 60
   user@cs-core-sw1# set vlans eng1_data_wired l3-interface irb.60
   user@cs-core-sw1# set vlans eng1_data_wired domain-type bridge
   ```

2. Configure the IRB and enable VRRP on it.

   On cs-core-sw1, enter:

   ```
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20 arp
    10.32.0.2 l2-interface ae29.0
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20 arp
    10.32.0.2 mac 28:8a:1c:e5:3b:f0
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 virtual-address 10.32.0.1
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 priority 125
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 preempt
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 accept-data
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 authentication-type md5
   user@cs-core-sw1# set interfaces irb unit 60 family inet address 10.32.0.3/20
   vrrp-group 1 authentication-key "$9$lN3v87wYojHm-VHmfT/9evW"
   ```

   On cs-core-sw2, enter:

   ```
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20 arp
    10.32.0.3 l2-interface ae29.0
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20 arp
    10.32.0.3 mac 28:8a:1c:e3:f7:f0
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
   vrrp-group 1 virtual-address 10.32.0.1
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
   vrrp-group 1 priority 125
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
   vrrp-group 1 preempt
   user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
   ```

```
vrrp-group 1 accept-data
user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
vrrp-group 1 authentication-type md5
user@cs-core-sw2# set interfaces irb unit 60 family inet address 10.32.0.2/20
vrrp-group 1 authentication-key "$9$bIY4ZHqfn/tUj/tuOcSwYg"
```

Configure the High Availability Software

Step-by-Step Procedure

To enable graceful Routing Engine switchover (GRES), nonstop active routing (NSR), and nonstop bridging (NSB):

- On both cs-core-sw1 and cs-core-sw2, enter the following configuration statements:

```
user@cs-core-sw1# set chassis redundancy graceful-switchover
user@cs-core-sw1# set protocols layer2-control nonstop-bridging
user@cs-core-sw1# set routing-options nonstop-routing
```

Configuring the Edge Firewalls for High Availability

The section provides the procedures for configuring the edge firewalls in a chassis cluster configuration and for configuring the redundant Ethernet interfaces.

To configure the edge firewalls for high availability:

- Enable Chassis Cluster Mode on page 57
- Configure the Chassis Cluster Data Fabric on page 58
- Configure Chassis Clustering Groups on page 58
- Configure Chassis Cluster Redundancy Groups on page 59
- Configure the Redundant Ethernet Interfaces on page 59
- Configure the Bridge Domains on page 61

Enable Chassis Cluster Mode

Step-by-Step Procedure

The command for enabling chassis cluster mode is an operational command, not a configuration statement, and must be executed on each member. The command causes the cluster member to reboot.

When you enable chassis cluster mode, you specify a cluster ID for the cluster. Because this network configuration example has only a single cluster, it uses cluster ID 1 for the cluster, with cs-edge-fw01 configured as node 0 and cs-edge-fw02 configured as node 1.

After you enable chassis clustering, the cluster members share a single, common configuration. All subsequent configuration steps can be done from the primary cluster member (node 0).

To enable chassis clustering on each member:

1. On cs-edge-fw01, enter the following operational command:

```
user@cs-edge-fw01> set chassis cluster cluster-id 1 node 0 reboot
```

2. On cs-edge-fw02, enter the following operational command:

   user@cs-edge-fw02> set chassis cluster cluster-id 1 node 1 reboot

   After the chassis members finish rebooting, the slot numbering on node 1 is changed so that numbering begins with slot 9 instead of slot 0. In addition, the interfaces shown in Table 14 on page 58 are automatically mapped to the fxp0 and fxp1 interfaces.

Table 14: Mapping of Interfaces After Chassis Clustering Is Enabled

Interface on Node 0	Interface on Node 1	Mapped to	Purpose
ge-0/0/0	ge-9/0/0	fxp0	Out-of-band management
ge-0/0/1	ge-9/0/1	fxp1	Chassis cluster control link

Configure the Chassis Cluster Data Fabric

Step-by-Step Procedure

After the chassis cluster has formed, you must configure the fabric ports for the cluster. These ports are used to pass real-time objects (RTOs) in active/passive mode. RTOs are messages that the cluster members use to synchronize information with each other.

To configure the data fabric, you must configure two fabric interfaces (one on each chassis) as shown:

1. Configure the fabric link for cs-edge-fw01.

   user@user@cs-edge-fw01# set interfaces fab0 fabric-options member-interfaces ge-0/0/2

2. Configure the fabric link for cs-edge-fw02.

   user@user@cs-edge-fw01# set interfaces fab1 fabric-options member-interfaces ge-9/0/2

Configure Chassis Clustering Groups

Step-by-Step Procedure

Although the chassis cluster configuration is held within a single common configuration, some elements of the configuration need to be applied to a specific member. Examples include the host name and the out-of-band management interface.

To apply the configuration to a specific member, you use the node-specific configuration method called groups.

To configure chassis clustering groups:

1. Configure node-specific information for cs-edge-fw01 (node 0):

   user@cs-edge-fw01-node0# set groups node0 system host-name cs-edge-fw01-node0
   user@cs-edge-fw01-node0# set groups node0 interfaces fxp0 unit 0 family inet address 10.92.76.63/23

2. Configure node-specific information for cs-edge-fw02 (node 1):

```
user@cs-edge-fw01-node0# set groups node1 system host-name
cs-edge-fw02-node1
user@cs-edge-fw01-node0# set groups node1 interfaces fxp0 unit 0 family inet
address 10.92.76.64/23
```

3. Configure apply groups.

```
user@cs-edge-fw01-node0# set apply-groups "${node}"
```

This command uses the node variable to define how the groups are applied to the nodes (each node will recognize its number and accept the configuration accordingly).

Configure Chassis Cluster Redundancy Groups

Step-by-Step Procedure

The next step in configuring chassis clustering is to configure redundancy groups. Redundancy group 0 is always for the control plane, while redundancy group 1+ is always for the data plane ports. Because active/backup mode allows only one chassis member to be active at a time, you define only redundancy groups 0 and 1.

You also need to define which device has priority for the control plane, as well as which device has priority for the data plane. Although the control plane can be active on a different chassis than the data plane in active/passive clustering, many administrators prefer having both the control plane and data plane active on the same chassis member. This example gives node 0 priority for both the control plane and data plane.

To configure chassis cluster redundancy groups:

- Enter the following commands:

```
user@cs-edge-fw01-node0# set chassis cluster redundancy-group 1 node 0 priority
100
user@cs-edge-fw01-node0# set chassis cluster redundancy-group 1 node 1 priority
1
user@cs-edge-fw01-node0# set chassis cluster redundancy-group 0 node 0
priority 100
user@cs-edge-fw01-node0# set chassis cluster redundancy-group 0 node 1 priority
1
```

Configure the Redundant Ethernet Interfaces

Step-by-Step Procedure

The redundant Ethernet interfaces connect the SRX chassis cluster to the core switches and edge routers. They allow the backup chassis member to take over the connections seamlessly in the event of a data plane failover. To configure the redundant Ethernet interfaces, you define which interfaces belong to the redundant Ethernet interface, define which redundancy group the redundant Ethernet interface belongs to (in an active/passive cluster, the interface always belongs to redundancy group 1), and define the redundant Ethernet interface information, such as the IP address of the interface.

To configure redundant Ethernet interfaces on the chassis cluster:

1. Specify the number of redundant Ethernet interfaces to be configured.

This is similar to how you configure the number of aggregated Ethernet interfaces on a switch.

```
user@cs-edge-fw01-node0# set chassis cluster reth-count 2
```

2. Configure redundant Ethernet interface reth0 toward the core switches.

```
user@cs-edge-fw01-node0# set interfaces reth0 description "Trust Zone towards
 Core"
user@cs-edge-fw01-node0# set interfaces reth0 vlan-tagging
user@cs-edge-fw01-node0# set interfaces reth0 redundant-ether-options
redundancy-group 1
user@cs-edge-fw01-node0# set interfaces reth0 redundant-ether-options
minimum-links 1
user@cs-edge-fw01-node0# set interfaces reth0 redundant-ether-options lacp
active
user@cs-edge-fw01-node0# set interfaces reth0 redundant-ether-options lacp
periodic fast
user@cs-edge-fw01-node0# set interfaces reth0 unit 0 vlan-id 600
user@cs-edge-fw01-node0# set interfaces reth0 unit 0 family inet address
172.16.33.4/29
```

3. Configure the member links for reth0.

```
user@cs-edge-fw01-node0# set interfaces ge-2/0/16 gigether-options
redundant-parent reth0
user@cs-edge-fw01-node0# set interfaces ge-2/0/17 gigether-options
redundant-parent reth0
user@cs-edge-fw01-node0# set interfaces ge-11/0/16 gigether-options
redundant-parent reth0
user@cs-edge-fw01-node0# set interfaces ge-11/0/17 gigether-options
redundant-parent reth0
```

4. Configure redundant Ethernet interface reth1 toward the edge routers.

```
user@cs-edge-fw01-node0# set interfaces reth1 description "Untrust Zone towards
 Edge-routers"
user@cs-edge-fw01-node0# set interfaces reth1 vlan-tagging
user@cs-edge-fw01-node0# set interfaces reth1 redundant-ether-options
redundancy-group 1
user@cs-edge-fw01-node0# set interfaces reth1 redundant-ether-options
minimum-links 1
user@cs-edge-fw01-node0# set interfaces reth1 redundant-ether-options lacp
active
user@cs-edge-fw01-node0# set interfaces reth1 redundant-ether-options lacp
periodic fast
user@cs-edge-fw01-node0# set interfaces reth1 unit 0 vlan-id 601
user@cs-edge-fw01-node0# set interfaces reth1 unit 0 family inet address
172.16.33.12/29
```

5. Configure the member links for reth1.

```
user@cs-edge-fw01-node0# set interfaces ge-2/0/18 gigether-options
redundant-parent reth1
user@cs-edge-fw01-node0# set interfaces ge-2/0/19 gigether-options
redundant-parent reth1
user@cs-edge-fw01-node0# set interfaces ge-11/0/18 gigether-options
redundant-parent reth1
```

```
user@cs-edge-fw01-node0# set interfaces ge-11/0/19 gigether-options
redundant-parent reth1
```

Configure the Bridge Domains

Step-by-Step Procedure

As previously described, the active node uses gratuitous Address Resolution Protocol (ARP) to advertise to the connecting devices that it is the next-hop gateway. This requires that the redundant Ethernet interface members and their connecting interfaces on the other devices belong to the same bridge domain.

To configure the bridge domains for reth0 and reth1:

- Enter the following commands:

```
user@cs-edge-fw01-node0# set bridge-domains reth-bd vlan-id-list 600
user@cs-edge-fw01-node0# set bridge-domains reth-bd vlan-id-list 601
```

Configuring the Edge Routers for High Availability

The section provides the procedures for configuring the edge routers in an MC-LAG configuration and for configuring the high availability software.

To configure the edge routers for high availability:

- Configure the Number of Aggregated Ethernet Interfaces and the Service ID on page 61
- Configure the Inter-Chassis Control Protocol (ICCP) and ICCP Link on page 62
- Configure the Interchassis Link (ICL) on the Edge Routers on page 63
- Configure the MC-LAG Links from the Routers to the Firewalls on page 64
- Configure the Bridge Domain on the MC-LAG Interfaces to the Firewalls on page 66
- Configure the High Availability Software on page 68

Configure the Number of Aggregated Ethernet Interfaces and the Service ID

Step-by-Step Procedure

This procedure configures two global settings for the router:

- Number of aggregated Ethernet interfaces—You must specify the number of aggregated Ethernet interfaces that will be configured on the device.
- Service ID—You must configure a service ID when the MC-LAG logical interfaces are part of a bridge domain, as they are in this example. The service ID is used to synchronize applications such as IGMP, ARP, and MAC learning across MC-LAG members.

On both cs-edge-r01 and cs-edge-r02:

1. Specify the number of aggregated Ethernet interfaces to be created.

```
{master}[edit]
user@cs-edge-r01# set chassis aggregated-devices ethernet device-count 5
```

2. Specify the switch service ID.

```
{master}[edit]
user@cs-edge-r01# set switch-options service-id 1
```

Configure the Inter-Chassis Control Protocol (ICCP) and ICCP Link

Step-by-Step Procedure

To configure ICCP and the ICCP link:

1. Specify the member interface that belongs to interface ae0, which will be used for the ICCP link.

   On both cs-edge-r01 and cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ge-1/2/4 gigether-options 802.3ad ae0
   ```

2. Configure ae0 as a Layer 3 link for ICCP.

   On cs-edge-r01, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ae0 flexible-vlan-tagging
   user@cs-edge-r01# set interfaces ae0 encapsulation flexible-ethernet-services
   user@cs-edge-r01# set interfaces ae0 aggregated-ether-options link-speed 1g
   user@cs-edge-r01# set interfaces ae0 aggregated-ether-options lacp active
   user@cs-edge-r01# set interfaces ae0 aggregated-ether-options lacp periodic
   slow
   user@cs-edge-r01# set interfaces ae0 unit 0 description "ICCP Link between
   edge-r1 & edge-r2"
   user@cs-edge-r01# set interfaces ae0 unit 0 vlan-id 4000
   user@cs-edge-r01# set interfaces ae0 unit 0 family inet address 172.16.32.41/30
   ```

   On cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r02# set interfaces ae0 flexible-vlan-tagging
   user@cs-edge-r02# set interfaces ae0 encapsulation flexible-ethernet-services
   user@cs-edge-r02# set interfaces ae0 aggregated-ether-options link-speed 1g
   user@cs-edge-r02# set interfaces ae0 aggregated-ether-options lacp active
   user@cs-edge-r02# set interfaces ae0 aggregated-ether-options lacp periodic
   slow
   user@cs-edge-r02# set interfaces ae0 unit 0 description "ICCP link between
   edge-r2 to edge-r1"
   user@cs-edge-r02# set interfaces ae0 unit 0 vlan-id 4000
   user@cs-edge-r02# set interfaces ae0 unit 0 family inet address 172.16.32.42/30
   ```

3. Configure ICCP, using the loopback addresses of cs-edge-r01 (172.16.32.33) and cs-edge-r02 (172.16.32.34) as the local IP addresses.

   On cs-edge-r01, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set protocols iccp local-ip-addr 172.16.32.33
   user@cs-edge-r01# set protocols iccp peer 172.16.32.34 redundancy-group-id-list
    1
   user@cs-edge-r01# set protocols iccp peer 172.16.32.34 liveness-detection
   minimum-interval 500
   user@cs-edge-r01# set protocols iccp peer 172.16.32.34 liveness-detection
   multiplier 3
   ```

   On cs-edge-r02, enter:

```
{master}[edit]
user@cs-edge-r02# set protocols iccp local-ip-addr 172.16.32.34
user@cs-edge-r02# set protocols iccp peer 172.16.32.33 redundancy-group-id-list
1
user@cs-edge-r02# set protocols iccp peer 172.16.32.33 liveness-detection
minimum-interval 500
user@cs-edge-r02# set protocols iccp peer 172.16.32.33 liveness-detection
multiplier 3
```

NOTE: The BFD timer is configured to be 1.5 sec, which provides faster convergence in this network configuration.

Configure the Interchassis Link (ICL) on the Edge Routers

Step-by-Step Procedure

To configure the ICL link on the edge routers:

1. Configure the ICL member link.

   On both cs-edge-r01 and cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ge-1/2/5 hold-time up 100
   user@cs-edge-r01# set interfaces ge-1/2/5 hold-time down 3000
   user@cs-edge-r01# set interfaces ge-1/2/5 gigether-options 802.3ad ae4
   ```

   For faster convergence, the hold-down timer is configured to be greater than the ICCP BFD timer, which is set to 1.5 seconds.

2. Configure ae4, which will be used for the ICL link.

   On both cs-edge-r01 and cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ae4 description ICL
   user@cs-edge-r01# set interfaces ae4 flexible-vlan-tagging
   user@cs-edge-r01# set interfaces ae4 encapsulation flexible-ethernet-services
   user@cs-edge-r01# set interfaces ae4 aggregated-ether-options link-speed 1g
   user@cs-edge-r01# set interfaces ae4 aggregated-ether-options lacp active
   user@cs-edge-r01# set interfaces ae4 aggregated-ether-options lacp periodic
   slow
   user@cs-edge-r01# set interfaces ae4 unit 0 description "ICL Link to
   edge-r2-vlan-601"
   user@cs-edge-r01# set interfaces ae4 unit 0 encapsulation vlan-bridge
   user@cs-edge-r01# set interfaces ae4 unit 0 vlan-id 601
   ```

Configure the MC-LAG Links from the Routers to the Firewalls

Step-by-Step Procedure

The edge routers establish MC-LAG links to each of the SRX Series gateways in the chassis cluster. To create the MC-LAG link, you create an aggregated Ethernet interface, enable LACP on the interface, and configure the MC-LAG options under the mc-ae option. Table 10 on page 49 in [xref target has no title] describes the MC-LAG options.

The following procedure shows how to configure the ae1 MC-LAG link to edge-fw-1. You can use the same procedure to configure the ae3 link to edge-fw-2, substituting the values shown in Table 15 on page 64.

Table 15: Parameters for MC-LAG Interfaces from Routers to Firewalls

LAG	LAG Client	Description String	Member Interface	lacp system-id	lacp admin-key	mc-ae mc-ae-id
ae1	reth 1 on cs-edge-fw01	"To-Firewall-reth1"	ge-1/0/0	00:ae:01:00:00:01	1	1
ae3	reth 1 on cs-edge-fw02	"To-Firewall-Standby"	ge-1/0/1	00:ae:03:00:00:01	3	3

To configure the MC-LAG interfaces to the firewalls:

1. Specify the members to be included within the aggregated Ethernet interface ae1.

   On both cs-edge-r01 and cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r01#  set interfaces ge-1/0/0 gigether-options 802.3ad ae1
   ```

2. Configure flexible VLAN tagging and the LACP parameters on the aggregated Ethernet interface.

   On cs-edge-r01 and cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ae1 description To-Firewall-reth1
   user@cs-edge-r01# set interfaces ae1 flexible-vlan-tagging
   user@cs-edge-r01# set interfaces ae1 encapsulation flexible-ethernet-services
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options link-speed 1g
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options lacp active
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options lacp periodic fast
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options lacp
   system-priority 100
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options lacp system-id
   00:ae:01:00:00:01
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options lacp admin-key
    1
   ```

3. Configure the mc-ae interface parameters.

   On cs-edge-r01, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id
   ```

```
1
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae
redundancy-group 1
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae chassis-id
0
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae mode
active-active
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae
status-control active
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-edge-r01# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
```

On cs-edge-r02, enter:

```
{master}[edit]
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id
1
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae
redundancy-group 1
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae chassis-id
1
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae mode
active-active
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae
status-control standby
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down force-icl-down
user@cs-edge-r02# set interfaces ae1 aggregated-ether-options mc-ae events
iccp-peer-down prefer-status-control-active
```

4. Configure a logical interface on ae1, with membership in VLAN 601.

   On cs-edge-r01, enter:

```
{master}[edit]
user@cs-edge-r01# set interfaces ae1 unit 0 encapsulation vlan-bridge
user@cs-edge-r01# set interfaces ae1 unit 0 vlan-id 601
user@cs-edge-r01# set interfaces ae1 unit 0 multi-chassis-protection 172.16.32.34
 interface ae4.0
```

   On cs-edge-r02, enter:

```
{master}[edit]
user@cs-edge-r02# set interfaces ae1 unit 0 encapsulation vlan-bridge
user@cs-edge-r02# set interfaces ae1 unit 0 vlan-id 601
user@cs-edge-r02# set interfaces ae1 unit 0 multi-chassis-protection 172.16.32.33
 interface ae4.0
```

Configure the Bridge Domain on the MC-LAG Interfaces to the Firewalls

Step-by-Step Procedure

The active node in the SRX chassis cluster uses gratuitous ARP to advertise to connecting devices that it is the next-hop gateway. This requires that the interfaces between the connecting devices and the SRX chassis cluster be in the same bridge domain.

Table 16 on page 66 summarizes the configuration of this bridge domain.

Table 16: Bridge Domain 601 Configuration

Name	ID	IRB Name	IP Address Information			
			Mask	cs-edge-r01 Address	cs-edge-r02 Address	Virtual IP Address
bd1	601	irb.601	/29	172.16.33.10	172.16.33.11	172.16.33.9

To configure the required bridge domain:

1. Create the bridge domain.

   On cs-edge-r01, enter:

   ```
   {master}[edit]
   user@cs-edge-r01# set bridge-domains bd1 domain-type bridge
   user@cs-edge-r01# set bridge-domains bd1 vlan-id 601
   user@cs-edge-r01# set bridge-domains bd1 interface ae1.0
   user@cs-edge-r01# set bridge-domains bd1 interface ae3.0
   user@cs-edge-r01# set bridge-domains bd1 interface ae4.0
   user@cs-edge-r01# set bridge-domains bd1 routing-interface irb.601
   user@cs-edge-r01# set bridge-domains bd1 bridge-options interface ae4.0
   static-mac 3c:8a:b0:cf:1f:f0
   ```

   On cs-edge-r02, enter:

   ```
   {master}[edit]
   user@cs-edge-r02# set bridge-domains bd1 domain-type bridge
   user@cs-edge-r02# set bridge-domains bd1 vlan-id 601
   user@cs-edge-r02# set bridge-domains bd1 interface ae1.0
   user@cs-edge-r02# set bridge-domains bd1 interface ae3.0
   user@cs-edge-r02# set bridge-domains bd1 interface ae4.0
   user@cs-edge-r02# set bridge-domains bd1 routing-interface irb.601
   user@cs-edge-r02# set bridge-domains bd1 bridge-options interface ae4.0
   static-mac 3c:8a:b0:ce:0f:f0
   ```

NOTE: The static-mac option on bridge domain 601 (bd1) prevents traffic arriving from the SRX chassis cluster from flooding the VLAN.

The SRX chassis cluster sends traffic to both edge routers using the IRB 601 MAC address for routing the packet. The IRB 601 MAC addresses on cs-edge-r01 and cs-edge-r02 are different. Because the reth1 interface on the chassis cluster is a single LAG, the reth1 LAG address hashing results in a packet destined to the cs-edge-r01 MAC address being sent to cs-edge-r02. In an MC-LAG configuration, MAC address learning does not occur on the ICL link, and, as a result, cs-edge-r02 floods the packet on bridge domain 601. To avoid flooding on bridge domain 601, specify the MAC address for cs-edge-r01 in the static-mac option on cs-edge-r02 and vice versa. When a packet destined to cs-edge-r01 arrives at cs-edge-r02, cs-edge-r02 sends the packet to cs-edge-r01 using the static MAC address.

2. Configure an IRB interface on the bridge domain and enable VRRP on the IRB interface.

   On cs-edge-r01, enter:

```
{master}[edit]
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 arp 172.16.33.11 l2-interface ae0.1
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 arp 172.16.33.11 mac 3c:8a:b0:cf:1f:f0
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 arp 172.16.33.11 publish
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 virtual-address 172.16.33.9
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 priority 250
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 preempt
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 accept-data
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 authentication-type md5
user@cs-edge-r01# set interfaces irb unit 601 family inet address 172.16.33.10/29
 vrrp-group 1 authentication-key "$9$nDoy9tOhSeX7V1R7VwYZG69A"
```

   On cs-edge-r02, enter:

```
{master}[edit]
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 arp 172.16.33.10 l2-interface ae0.1
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 arp 172.16.33.10 mac 3c:8a:b0:ce:0f:f0
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 arp 172.16.33.10 publish
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 virtual-address 172.16.33.9
```

```
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 priority 125
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 preempt
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 accept-data
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 authentication-type md5
user@cs-edge-r02# set interfaces irb unit 601 family inet address 172.16.33.11/29
 vrrp-group 1 authentication-key "$9$H.fz9A0hSe36SevW-dk.P"
```

Configure the High Availability Software

Step-by-Step Procedure

To enable graceful Routing Engine switchover (GRES), nonstop active routing (NSR), and nonstop bridging (NSB):

- On both cs-edge-r01 and cs-edge-r02, enter the following configuration statements:

```
{master}[edit]
user@cs-edge-r01# set chassis redundancy graceful-switchover
user@cs-edge-r01# set protocols layer2-control nonstop-bridging
user@cs-edge-r01# set routing-options nonstop-routing
```

Verification

Confirm that the configuration is working properly.

- Verifying the High Availability Configuration of the Access Switches on page 68
- Verifying the High Availability Configuration of the Aggregation Switches on page 70
- Verifying the High Availability Configuration of the Core Switches on page 71
- Verifying the High Availability Configuration of the Edge Firewalls on page 82
- Verifying the High Availability Configuration of the Edge Routers on page 83

Verifying the High Availability Configuration of the Access Switches

Purpose

Verify the Virtual Chassis, LAG, and high availability software configuration on the access switches.

Action

Perform the following steps for each Virtual Chassis in the access layer:

1. Verify the Virtual Chassis status.

```
user@cs-4200-ab1> show virtual-chassis status
Preprovisioned Virtual Chassis
Virtual Chassis ID: 0315.fd43.9a83
Virtual Chassis Mode: Enabled
                                                Mstr           Mixed Neighbor List
Member ID  Status   Serial No    Model     prio  Role      Mode ID  Interface
0 (FPC 0)  Prsnt    BP0213230308 ex4200-48t   0  Linecard     N  2  vcp-0
                                                                9  vcp-1
1 (FPC 1)  Prsnt    BP0213260624 ex4200-48t 129  Master*      N  3  vcp-0
                                                                2  vcp-1
2 (FPC 2)  Prsnt    BP0213260668 ex4200-48t 129  Backup       N  1  vcp-0
                                                                0  vcp-1
```

```
3 (FPC 3)  Prsnt    BP0213260540 ex4200-48t   0  Linecard     N  4  vcp-0
                                                                1  vcp-1
4 (FPC 4)  Prsnt    BP0213260532 ex4200-48t   0  Linecard     N  5  vcp-0
                                                                3  vcp-1
5 (FPC 5)  Prsnt    BP0213230346 ex4200-48t   0  Linecard     N  6  vcp-0
                                                                4  vcp-1
6 (FPC 6)  Prsnt    FP0213313963 ex4200-48px    0 Linecard     N  7  vcp-0
                                                                5  vcp-1
7 (FPC 7)  Prsnt    BP0213310009 ex4200-48t   0  Linecard     N  8  vcp-0
                                                                6  vcp-1
8 (FPC 8)  Prsnt    BP0213260607 ex4200-48t   0  Linecard     N  9  vcp-0
                                                                7  vcp-1
9 (FPC 9)  Prsnt    BP0213230403 ex4200-48t   0  Linecard     N  0  vcp-0
                                                                8  vcp-1
```

2. Verify the LACP status of the uplink aggregated Ethernet interface.

```
user@cs-4200-ab1> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity

      xe-4/1/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-4/1/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-3/1/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-3/1/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-1/1/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-1/1/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-2/1/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-2/1/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

    LACP protocol:        Receive State  Transmit State          Mux State
      xe-4/1/0                Current   Fast periodic Collecting distributing

      xe-3/1/0                Current   Fast periodic Collecting distributing

      xe-1/1/0                Current   Fast periodic Collecting distributing

      xe-2/1/0                Current   Fast periodic Collecting distributing
```

3. Verify that GRES is enabled by entering the following command on the backup Virtual Chassis member:

```
user@cs-4200-ab1> show system switchover

fpc2:
--------------------------------------------------------------------------
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
```

Verifying the High Availability Configuration of the Aggregation Switches

Purpose Verify the Virtual Chassis, LAG, and high availability software configuration on the EX4550 switches in location B.

Action 1. Verify the Virtual Chassis status.

```
user@cs-agg-01> show virtual-chassis status

Preprovisioned Virtual Chassis
Virtual Chassis ID: 0cf5.0cd4.e2f3
Virtual Chassis Mode: Enabled
                                          Mstr           Mixed Neighbor List
Member ID  Status   Serial No    Model     prio  Role      Mode ID  Interface
0 (FPC 0)  Prsnt    LX0213439586 ex4550-32f 129  Master*     N  1  vcp-255/0/14

                                                             1  vcp-255/0/15
1 (FPC 1)  Prsnt    LX0213449606 ex4550-32f 129  Backup      N  0  vcp-255/0/14

                                                             0  vcp-255/0/15
```

2. Verify the LACP status of the aggregated Ethernet interfaces to the access switches.

```
user@cs-agg-01> show lacp interfaces
Aggregated interface: ae4
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity

      xe-0/0/30      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-0/0/30    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-1/0/30      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      xe-1/0/30    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/30               Current   Fast periodic Collecting distributing

      xe-1/0/30               Current   Fast periodic Collecting distributing

Aggregated interface: ae5
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity

      ge-1/0/23      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-1/0/23    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-0/0/23      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-0/0/23    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-0/0/31      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-0/0/31    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-1/0/31      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active

      ge-1/0/31    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active

    LACP protocol:        Receive State  Transmit State          Mux State
```

```
ge-1/0/23               Current   Fast periodic Collecting distributing

ge-0/0/23               Current   Fast periodic Collecting distributing

ge-0/0/31               Current   Fast periodic Collecting distributing

ge-1/0/31               Current   Fast periodic Collecting distributing
```

3. Verify that GRES is enabled by entering the following command on the backup Virtual Chassis member:

```
{backup:1}
user@cs-agg-01> show system switchover
fpc1:
--------------------------------------------------------------------------
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
```

4. Verify that nonstop active routing is enabled.

```
user@cs-agg-01> show task replication
Stateful Replication: Enabled
        RE mode: Master

    Protocol                Synchronization Status
    OSPF                    Complete
    PIM                     Complete
```

NOTE: If you have not configured routing yet, you might not see the protocols and their synchronization status listed.

Verifying the High Availability Configuration of the Core Switches

Purpose Verify the MC-LAG configuration and high availability software configuration on the core switches.

Action Perform the following steps on both cs-core-sw01 and cs-core-sw02:

1. Verify that ICCP is configured.

```
user@cs-core-sw01> show iccp
Redundancy Group Information for peer 172.16.32.6
  TCP Connection       : Established
  Liveliness Detection : Up
  Redundancy Group ID          Status
    1                           Up

Client Application: MCSNOOPD
  Redundancy Group IDs Joined: 1

Client Application: lacpd
  Redundancy Group IDs Joined: 1

Client Application: l2ald_iccpd_client
  Redundancy Group IDs Joined: 1
```

2. Verify that the ICL link has been configured with membership in all the VLANs.

```
user@cs-core-sw01> show configuration interfaces ae29

description "ICL Layer 2 link with 2 members,xe-0/3/7,1/3/7";
vlan-tagging;
aggregated-ether-options {
    lacp {
        active;
        periodic fast;
    }
}
unit 0 {
    family ethernet-switching {
        interface-mode trunk;
        vlan {
            members all;
        }
    }
}
```

3. Verify the status of the ICL link.

```
user@cs-core-sw01> show interfaces ae29 extensive
Physical interface: ae29, Enabled, Physical link is Up
  Interface index: 157, SNMP ifIndex: 738, Generation: 160
  Description: ICL Layer 2 link with 2 members,xe-0/3/7,1/3/7
  Link-level type: Ethernet, MTU: 1518, Speed: 20Gbps, BPDU Error: None,
MAC-REWRITE Error: None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled,
Minimum links needed: 1,
  Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 2a:8a:1c:e3:f1:46, Hardware address: 2a:8a:1c:e3:f1:46
  Last flapped   : 2014-06-02 03:34:58 PDT (14:50:58 ago)
  Statistics last cleared: 2014-06-02 18:23:16 PDT (00:02:40 ago)
  Traffic statistics:
   Input  bytes  :            102872394              5144888 bps
   Output bytes  :            103878646              5145608 bps
   Input  packets:               830281                 5206 pps
   Output packets:               845410                 5238 pps
```

```
   IPv6 transit statistics:
    Input  bytes  :                  0
    Output bytes  :                  0
    Input  packets:                  0
    Output packets:                  0
  Dropped traffic statistics due to STP State:
   Input  bytes  :                   0
   Output bytes  :                   0
   Input  packets:                   0
   Output packets:                   0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed
discards: 0,
    Resource errors: 0
  Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
 0
  Ingress queues: 8 supported, 6 in use
  Queue counters:      Queued packets  Transmitted packets     Dropped packets

    0 Best-Effort                    0                    0
 0
    1 Mission-Crit                   0                    0
 0
    2 assured-forw                   0                    0
 0
    3 Video                          0                    0
 0
    5 Voice                          0                    0
 0
    7 Network-Cont                   0                    0
 0
  Egress queues: 8 supported, 6 in use
  Queue counters:      Queued packets  Transmitted packets     Dropped packets

    0 Best-Effort               825903               825903
 0
    1 Mission-Crit                   0                    0
 0
    2 assured-forw                   0                    0
 0
    3 Video                      19696                19696
 0
    5 Voice                          0                    0
 0
    7 Network-Cont                 131                  131
 0
  Queue number:         Mapped forwarding classes
    0                   Best-Effort
    1                   Mission-Critical
    2                   assured-forwarding
    3                   Video
    5                   Voice
    7                   Network-Control

  Logical interface ae29.0 (Index 338) (SNMP ifIndex 744) (Generation 147)
    Flags: SNMP-Traps 0x20024000 Encapsulation: Ethernet-Bridge
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :        829950       5204     102829392      5142904
        Output:        845398       5216     104067298      5131000
```

```
    Link:
      xe-1/3/7.0
        Input :        413483       2609      51119271      2580464
        Output:        420951       2616      51342053      2544200
      xe-0/3/7.0
        Input :        416467       2595      51710121      2562440
        Output:        424447       2600      52725245      2586800
    Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
      xe-1/3/7.0               0           0            0            0
      xe-0/3/7.0               0           0            0            0
    Protocol eth-switch, MTU: 1518, Generation: 169, Route table: 5
      Flags: Trunk-Mode

  Logical interface ae29.32767 (Index 337) (SNMP ifIndex 806) (Generation 146)

    Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ]  Encapsulation: ENET2
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :           320          2         39680         1984
        Output:             0          0             0            0
    Link:
      xe-1/3/7.32767
        Input :           159          1         19716          992
        Output:             6          0          1812            0
      xe-0/3/7.32767
        Input :           161          1         19964          992
        Output:             6          0          1812            0
    LACP info:        Role     System             System      Port    Port
Port
                             priority          identifier  priority  number
 key
      xe-1/3/7.32767    Actor      127 28:8a:1c:e3:f7:c0       127      23
 30
      xe-1/3/7.32767  Partner      127 28:8a:1c:e5:3b:c0       127      23
 30
      xe-0/3/7.32767    Actor      127 28:8a:1c:e3:f7:c0       127      11
 30
      xe-0/3/7.32767  Partner      127 28:8a:1c:e5:3b:c0       127      11
 30
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      xe-1/3/7.32767           150         150            0            0
      xe-0/3/7.32767           150         150            0            0
    Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
      xe-1/3/7.32767             0           0            0            0
      xe-0/3/7.32767             0           0            0            0
    Protocol multiservice, MTU: Unlimited, Generation: 168, Route table: 0
      Flags: None
```

4. Verify that all the MC-LAG interfaces are up.

```
user@cs-core-sw01> show interfaces mc-ae
Member Link                  : ae1
 Current State Machine's State: mcae active state
 Local Status                : active
 Local State                 : up
 Peer Status                 : active
 Peer State                  : up
     Logical Interface       : ae1.0
     Topology Type           : bridge
     Local State             : up
     Peer State              : up
     Peer Ip/MCP/State       : 172.16.32.6 ae29.0 up
```

```
Member Link                  : ae2
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae2.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up

Member Link                  : ae3
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae3.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up

Member Link                  : ae7
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae7.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up

Member Link                  : ae11
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae11.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up

Member Link                  : ae12
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae12.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up
```

```
Member Link                  : ae30
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae30.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up

Member Link                  : ae31
Current State Machine's State: mcae active state
Local Status                 : active
Local State                  : up
Peer Status                  : active
Peer State                   : up
    Logical Interface        : ae31.0
    Topology Type            : bridge
    Local State              : up
    Peer State               : up
    Peer Ip/MCP/State        : 172.16.32.6 ae29.0 up
```

5. Verify that ICL (ae29) and the MC-LAG interfaces are in the same broadcast domains.

   In following example, the broadcast domain eng1_data_wired is used.

```
user@cs-core-sw01> show vlans eng1_data_wired

Routing instance        VLAN name             Tag          Interfaces
default-switch          eng1_data_wired       60
                                                           ae1.0*

                                                           ae29.0*
```

6. Verify the status of VRRP.

   a. On cs-core-sw01, enter:

```
user@cs-core-sw01> show vrrp summary
Interface     State       Group   VR state       VR Mode    Type   Address
irb.10        up              1   master         Active     lcl    10.16.0.3

                                                            vip    10.16.0.1
irb.11        up              1   master         Active     lcl    10.16.16.3

                                                            vip    10.16.16.1
irb.12        up              1   master         Active     lcl    10.16.32.3

                                                            vip    10.16.32.1
irb.13        up              1   master         Active     lcl    10.16.48.3

                                                            vip    10.16.48.1
irb.20        up              1   master         Active     lcl    10.17.0.3

                                                            vip    10.17.0.1
irb.21        up              1   master         Active     lcl    10.17.4.3

                                                            vip    10.17.4.1
irb.22        up              1   master         Active     lcl    10.17.8.3
```

```
                                                                vip    10.17.8.1
irb.23       up             1   master         Active    lcl    10.17.12.3

                                                               vip    10.17.12.1
irb.30       up             1   master         Active    lcl    10.17.64.3

                                                               vip    10.17.64.1
irb.31       up             1   master         Active    lcl    10.17.68.3

                                                               vip    10.17.68.1
irb.32       up             1   master         Active    lcl    10.17.72.3

                                                               vip    10.17.72.1
irb.33       up             1   master         Active    lcl    10.17.76.3

                                                               vip    10.17.76.1
irb.40       up              1   master          Active    lcl
10.17.128.3
                                                                 vip
10.17.128.1
irb.41       up              1   master          Active    lcl
10.17.132.3
                                                                 vip
10.17.132.1
irb.42       up              1   master          Active    lcl
10.17.136.3
                                                                 vip
10.17.136.1
irb.43       up              1   master          Active    lcl
10.17.140.3
                                                                 vip
10.17.140.1
irb.50       up             1   master         Active    lcl    10.18.0.3

                                                                vip    10.18.0.1
irb.51       up             1   master         Active    lcl    10.18.16.3

                                                               vip    10.18.16.1
irb.52       up             1   master         Active    lcl    10.18.32.3

                                                               vip    10.18.32.1
irb.53       up             1   master         Active    lcl    10.18.48.3

                                                               vip    10.18.48.1
irb.60       up             1   master         Active    lcl    10.32.0.3

                                                                vip    10.32.0.1
irb.61       up             1   master         Active    lcl    10.32.16.3

                                                               vip    10.32.16.1
irb.62       up             1   master         Active    lcl    10.32.32.3

                                                               vip    10.32.32.1
irb.63       up             1   master         Active    lcl    10.32.48.3

                                                               vip    10.32.48.1
irb.70       up             1   master         Active    lcl    10.33.0.3

                                                                vip    10.33.0.1
irb.71       up             1   master         Active    lcl    10.33.16.3
```

```
                                                                vip    10.33.16.1
irb.72       up             1   master         Active    lcl    10.33.32.3

                                                                vip    10.33.32.1
irb.73       up             1   master         Active    lcl    10.33.48.3

                                                                vip    10.33.48.1
irb.80       up             1   master         Active    lcl    10.34.0.3

                                                                vip    10.34.0.1
irb.81       up             1   master         Active    lcl    10.34.16.3

                                                                vip    10.34.16.1
irb.82       up             1   master         Active    lcl    10.34.32.3

                                                                vip    10.34.32.1
irb.83       up             1   master         Active    lcl    10.34.48.3

                                                                vip    10.34.48.1
irb.90       up             1   master         Active    lcl    10.35.0.3

                                                                vip    10.35.0.1
irb.91       up             1   master         Active    lcl    10.35.16.3

                                                                vip    10.35.16.1
irb.92       up             1   master         Active    lcl    10.35.32.3

                                                                vip    10.35.32.1
irb.93       up             1   master         Active    lcl    10.35.48.3

                                                                vip    10.35.48.1
irb.100      up             1   master         Active    lcl    10.36.0.3

                                                                vip    10.36.0.1
irb.101      up             1   master         Active    lcl    10.36.16.3

                                                                vip    10.36.16.1
irb.102      up             1   master         Active    lcl    10.36.32.3

                                                                vip    10.36.32.1
irb.103      up             1   master         Active    lcl    10.36.48.3

                                                                vip    10.36.48.1
irb.201      up             1   master         Active    lcl
172.16.128.3
                                                                  vip
172.16.128.1
irb.399      up             1   master         Active    lcl
172.16.12.3
                                                                  vip
172.16.12.1
irb.400      up             1   master         Active    lcl
172.16.35.67
                                                                  vip
172.16.35.65
irb.500      up             1   master         Active    lcl
172.16.11.3
                                                                  vip
172.16.11.1
irb.600      up             1   master         Active    lcl
172.16.33.3
```

```
                                                                  vip
172.16.33.1
irb.786       up              1   master          Active    lcl    78.1.1.3

                                                                 vip    78.1.1.1
irb.1000      up              1   master          Active     lcl    3.3.0.3
                                                                  vip    3.3.0.1
irb.1001      up              1   master          Active     lcl    3.4.0.3
                                                                  vip    3.4.0.1
```

b. On cs-core-sw02, enter:

```
user@cs-core-sw02> show vrrp summary
Interface     State       Group   VR state       VR Mode    Type   Address
irb.10        up              1   backup         Active    lcl    10.16.0.2

                                                                 vip    10.16.0.1
irb.11        up              1   backup         Active    lcl    10.16.16.2

                                                                vip    10.16.16.1
irb.12        up              1   backup         Active    lcl    10.16.32.2

                                                                vip    10.16.32.1
irb.13        up              1   backup         Active    lcl    10.16.48.2

                                                                vip    10.16.48.1
irb.20        up              1   backup         Active    lcl    10.17.0.2

                                                                 vip    10.17.0.1
irb.21        up              1   backup         Active    lcl    10.17.4.2

                                                                 vip    10.17.4.1
irb.22        up              1   backup         Active    lcl    10.17.8.2

                                                                 vip    10.17.8.1
irb.23        up              1   backup         Active    lcl    10.17.12.2

                                                                vip    10.17.12.1
irb.30        up              1   backup         Active    lcl    10.17.64.2

                                                                vip    10.17.64.1
irb.31        up              1   backup         Active    lcl    10.17.68.2

                                                                vip    10.17.68.1
irb.32        up              1   backup         Active    lcl    10.17.72.2

                                                                vip    10.17.72.1
irb.33        up              1   backup         Active    lcl    10.17.76.2

                                                                vip    10.17.76.1
irb.40        up              1   backup         Active     lcl
10.17.128.2
                                                                  vip
10.17.128.1
irb.41        up              1   backup         Active     lcl
10.17.132.2
                                                                  vip
10.17.132.1
irb.42        up              1   backup         Active     lcl
10.17.136.2
```

```
                                                                  vip
10.17.136.1
irb.43          up              1   backup          Active    lcl
10.17.140.2
                                                                  vip
10.17.140.1
irb.50          up              1   backup          Active    lcl    10.18.0.2

                                                                 vip    10.18.0.1
irb.51          up              1   backup          Active    lcl    10.18.16.2

                                                                vip    10.18.16.1
irb.52          up              1   backup          Active    lcl    10.18.32.2

                                                                vip    10.18.32.1
irb.53          up              1   backup          Active    lcl    10.18.48.2

                                                                vip    10.18.48.1
irb.60          up              1   backup          Active    lcl    10.32.0.2

                                                                 vip    10.32.0.1
irb.61          up              1   backup          Active    lcl    10.32.16.2

                                                                vip    10.32.16.1
irb.62          up              1   backup          Active    lcl    10.32.32.2

                                                                vip    10.32.32.1
irb.63          up              1   backup          Active    lcl    10.32.48.2

                                                                vip    10.32.48.1
irb.70          up              1   backup          Active    lcl    10.33.0.2

                                                                 vip    10.33.0.1
irb.71          up              1   backup          Active    lcl    10.33.16.2

                                                                vip    10.33.16.1
irb.72          up              1   backup          Active    lcl    10.33.32.2

                                                                vip    10.33.32.1
irb.73          up              1   backup          Active    lcl    10.33.48.2

                                                                vip    10.33.48.1
irb.80          up              1   backup          Active    lcl    10.34.0.2

                                                                 vip    10.34.0.1
irb.81          up              1   backup          Active    lcl    10.34.16.2

                                                                vip    10.34.16.1
irb.82          up              1   backup          Active    lcl    10.34.32.2

                                                                vip    10.34.32.1
irb.83          up              1   backup          Active    lcl    10.34.48.2

                                                                vip    10.34.48.1
irb.90          up              1   backup          Active    lcl    10.35.0.2

                                                                 vip    10.35.0.1
irb.91          up              1   backup          Active    lcl    10.35.16.2

                                                                vip    10.35.16.1
irb.92          up              1   backup          Active    lcl    10.35.32.2
```

```
                                                                vip    10.35.32.1
irb.93          up              1   backup          Active      lcl    10.35.48.2

                                                                vip    10.35.48.1
irb.100         up              1   backup          Active      lcl    10.36.0.2

                                                                vip    10.36.0.1
irb.101         up              1   backup          Active      lcl    10.36.16.2

                                                                vip    10.36.16.1
irb.102         up              1   backup          Active      lcl    10.36.32.2

                                                                vip    10.36.32.1
irb.103         up              1   backup          Active      lcl    10.36.48.2

                                                                vip    10.36.48.1
irb.201         up              1   backup          Active      lcl
172.16.128.2
                                                                  vip
172.16.128.1
irb.399         up              1   backup          Active      lcl
172.16.12.2
                                                                  vip
172.16.12.1
irb.400         up              1   backup          Active      lcl
172.16.35.66
                                                                  vip
172.16.35.65
irb.500         up              1   backup          Active      lcl
172.16.11.2
                                                                  vip
172.16.11.1
irb.600         up              1   backup          Active      lcl
172.16.33.2
                                                                  vip
172.16.33.1
irb.786         up              1   backup          Active      lcl    78.1.1.2

                                                                vip    78.1.1.1
irb.1000        up              1   backup          Active      lcl    3.3.0.2
                                                                vip    3.3.0.1
irb.1001        up              1   backup          Active      lcl    3.4.0.2
                                                                vip    3.4.0.1
irb.1001        up              1   master          Active      lcl    3.4.0.3
                                                                vip    3.4.0.1
```

7. Verify that GRES is enabled.

   a. On the backup Routing Engine of cs-core-sw01, enter:

      ```
      user@cs-core-sw01-1> show system switchover
      Graceful switchover: On
      Configuration database: Ready
      Kernel database: Synchronizing
      Peer state: Steady State
      ```

   b. On the backup Routing Engine of cs-core-sw02, enter:

      ```
      user@cs-core-sw02-1> show system switchover
      ```

```
    Graceful switchover: On
    Configuration database: Ready
    Kernel database: Ready
    Peer state: Steady State
```

8. Verify that nonstop active routing is enabled.

```
user@cs-core-sw01> show task replication
Stateful Replication: Enabled
        RE mode: Master

    Protocol                Synchronization Status
    OSPF                    Complete
    PIM                     Complete
```

NOTE: If you have not configured routing yet, you might not see the protocols and their synchronization status listed.

Verifying the High Availability Configuration of the Edge Firewalls

Purpose Verify the chassis cluster configuration and the status of the control, fabric, and redundant Ethernet interfaces.

Action

1. Verify the chassis cluster configuration and status.

```
user@cs-edge-fw01-node0> show chassis cluster status
Cluster ID: 1
Node                  Priority          Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   100         primary        no       no
    node1                   1           secondary      no       no

Redundancy group: 1 , Failover count: 1
    node0                   100         primary        no       no
    node1                   1           secondary      no       no
```

2. Verify the status of the control, fabric, and redundant Ethernet interfaces.

```
user@cs-edge-fw01-node0> show chassis cluster interfaces
Control link status: Up

Control interfaces:
    Index   Interface        Status
    0       fxp1             Up

Fabric link status: Up

Fabric interfaces:
    Name    Child-interface    Status
                               (Physical/Monitored)
    fab0    ge-0/0/2           Up   / Up
    fab0
    fab1    ge-9/0/2           Up   / Up
    fab1
```

```
Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
    reth1        Up          1
    reth2        Down        Not configured
    reth3        Down        Not configured

Redundant-pseudo-interface Information:
    Name         Status      Redundancy-group
    lo0          Up          0
```

Verifying the High Availability Configuration of the Edge Routers

Purpose Verify the status of the MC-LAG interfaces and that the router is forwarding traffic to the SRX chassis cluster correctly.

Action Perform the following steps on both cs-edge-r01 and cs-edge-r02.

1. Verify the status of the MC-LAG interfaces.

```
user@cs-edge-r01> show interfaces mc-ae
 Member Link                  : ae1
 Current State Machine's State: mcae active state
 Local Status                 : active
 Local State                  : up
 Peer Status                  : active
 Peer State                   : up
     Logical Interface        : ae1.0
     Topology Type            : bridge
     Local State              : up
     Peer State               : up
     Peer Ip/MCP/State        : 172.16.32.34 ae0.1 up

 Member Link                  : ae3
 Current State Machine's State: mcae active state
 Local Status                 : active
 Local State                  : up
 Peer Status                  : active
 Peer State                   : up
     Logical Interface        : ae3.0
     Topology Type            : bridge
     Local State              : up
     Peer State               : up
     Peer Ip/MCP/State        : 172.16.32.34 ae0.1 up
```

2. Verify that the router is forwarding traffic to the active firewall node, based on the gratuitous ARP message sent by the active node.

   a. Display route information for 172.16.4.0/24.

```
user@cs-edge-r01> show route 172.16.4.0/24

inet.0: 3165 destinations, 3166 routes (3165 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.4.0/24      *[OSPF/10] 00:04:30, metric 1601
                    > to 172.16.33.12 via irb.601
```

   b. Check the forwarding table to see if the next hop and interface are chosen correctly.

```
user@cs-edge-r01> show route forwarding-table destination 172.16.4.0/24

Routing table: default.inet
Internet:
Destination        Type RtRef Next hop           Type Index    NhRef Netif
172.16.4.0/24      user     0 172.16.33.12       ucst      607  3148 ae1.0

Routing table: __master.anon__.inet
Internet:
Destination        Type RtRef Next hop           Type Index    NhRef Netif
default            perm     0                   rjct      519     1
```

3. Verify the LACP state of the LAG interfaces.

   Both LAGs should be up, even though only the LAG connecting to the active firewall node forwards traffic.

   a. Show the LACP state for interface ae1.

```
user@cs-edge-r01> show lacp interfaces ae1
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout
Activity
      ge-1/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast
Active
      ge-1/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast
Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-1/0/0                  Current   Fast periodic Collecting
distributing
```

   b. Show the LACP state for interface ae3.

```
user@cs-edge-r01> show lacp interfaces ae3
Aggregated interface: ae3
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout
Activity
      ge-1/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast
Active
      ge-1/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast
Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-1/0/1                  Current   Fast periodic Collecting
distributing
```

4. Verify that nonstop active routing is enabled.

```
user@cs-edge-r01> show task replication
Stateful Replication: Enabled
        RE mode: Master

    Protocol                Synchronization Status
    OSPF                    Complete
    BGP                     Complete
```

NOTE: If you have not configured routing yet, you might not see the protocols and their synchronization status listed.

Related Documentation

- Understanding the Benefits of the Midsize Enterprise Campus Solution on page 6
- Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus on page 85
- Example: Configuring Access Policy and Security for the Midsize Enterprise Campus on page 114
- Example: Configuring Class of Service for the Midsize Enterprise Campus on page 137

Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus

This example details the configuration for BGP and OSPF routing, as well as multicast and DHCP relay for campus networks. This is based on a validated design architecture.

Requirements

Table 17 on page 85 shows the hardware and software requirements for this example.Table 18 on page 86 shows the scaling and performance targets used for this example.

Table 17: Hardware and Software Requirements

Hardware	Device Name	Software
MX240	cs-edge-r01, cs-edge-r02	13.2 R2.4
SRX650	cs-edge-fw-01, cs-edge-fw02	12.1 X44-D39.4
EX9214	cs-core-sw01, cs-core-sw02	13.2 R3.7
EX4550	cs-agg-01	12.3 R3.4
EX2200	cs-2200-ab5	12.3 R3.4
EX3300	cs-3300-ab4	12.3 R3.4
EX4200	cs-4200-ab1	12.3 R3.4
EX4300	cs-4300-ab2, cs-4300-ab3	13.2 X51-D21.1

Table 18: Node Features and Performance/Scalability

Node	Features	Performance/Scalability Target Value
Edge (MX240, SRX650)	MC-LAG, OSPF, BGP, IRB	3k IPv4
Core (EX9214)	VLANs, MC-LAG, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, IRB	3k IPv4 routes 128k MAC table entries 16k ARP entries
Aggregation (EX4550)	VLANs, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, RVI	3k IPv4 routes 5 IGMP groups
Access (EX3300, EX4300, EX4200)	VLANs, LAG, 802.1X, IGMP snooping, DHCP snooping, ARP inspection, IP source guard	55k MAC table entries 13k 8021.x users 5 IGMP groups

The configuration details that follow assume that:

- All physical cabling necessary has been completed.
- All basic logical interfaces have been configured.
- All devices have loopback interfaces configured.

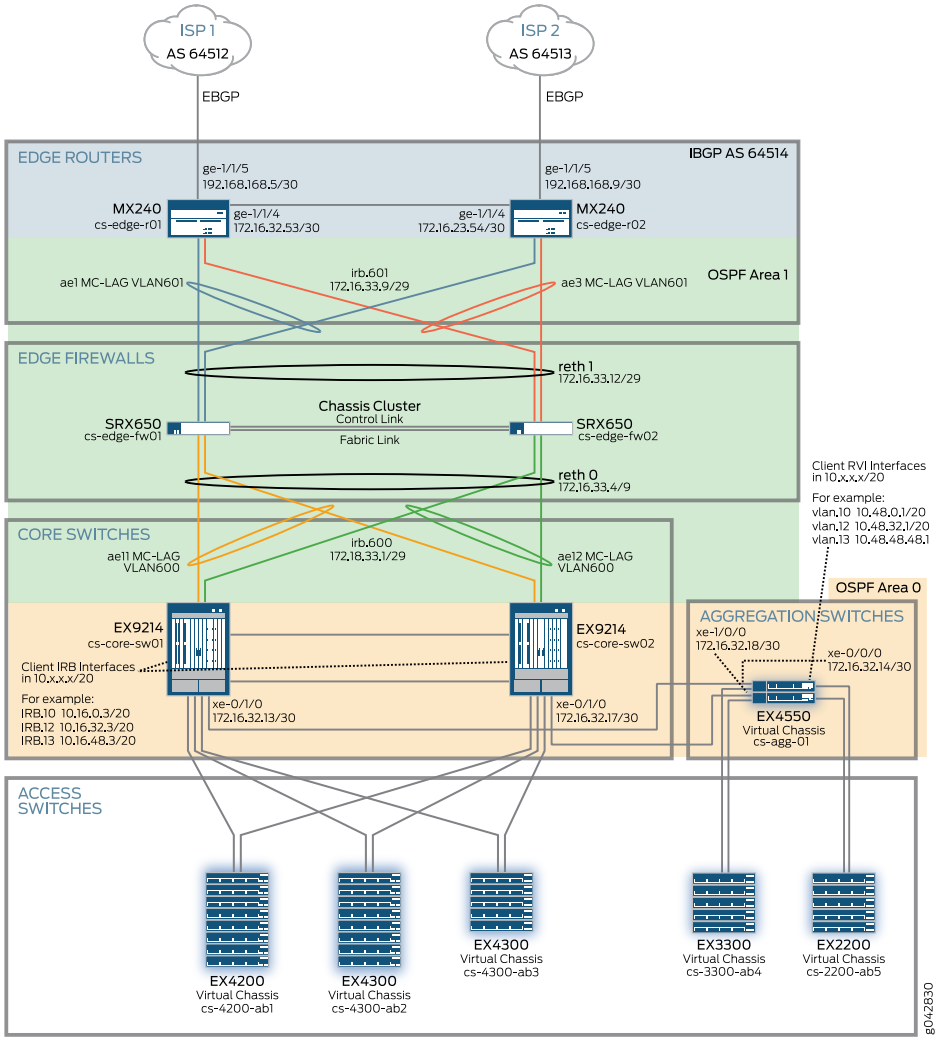
Overview

This configuration example details advanced Layer 2 and Layer 3 connectivity that has been validated to support a modern enterprise campus. The campus is designed to scale and facilitate connectivity for an assortment of wired devices to the network.

Topology

The midsize enterprise campus design is comprised of separate modules: edge, core, access, and aggregation. After the Layer 3 interfaces have been configured, the dynamic routing protocols can then be provisioned. BGP is used at the edge, and OSPF is used inside the campus network. Figure 12 on page 87 shows the routing topology used.

Figure 12: Routing Topology Diagram



Configuration

To configure Layer 2 and Layer 3 network services for the midsize enterprise campus, perform these tasks:

- Configuring Layer 3 Interfaces for the Midsize Enterprise Campus on page 88
- Configuring DHCP Relay in Midsize Enterprise Campus on page 90
- Configuring Multicast on Core Devices on page 91
- Configuring Multicast on Aggregation and Access Devices on page 93
- Configuring BGP Routing on page 94
- Configuring OSPF Routing for the Midsize Enterprise Campus on page 96

Configuring Layer 3 Interfaces for the Midsize Enterprise Campus

Step-by-Step Procedure

To configure Layer 3 interfaces for the midsize enterprise campus, follow these steps:

1. Configure bridge-domains on edge devices.

   This configuration was used for cs-edge-r01 and cs-edge-r02.

   ```
   [edit]
   user@host# set bridge-domains bd1 domain-type bridge
   user@host# set bridge-domains bd1 vlan-id 601
   user@host# set bridge-domains bd1 interface ae1.0
   user@host# set bridge-domains bd1 interface ae3.0
   user@host# set bridge-domains bd1 interface ae4.0
   user@host# set bridge-domains bd1 routing-interface irb.601
   user@host# set bridge-domains bd1 bridge-options interface ae4.0 static-mac
     3c:8a:b0:cf:1f:f0
   ```

   In this example, the SRX cluster sends traffic to either cs-edge-r01 or cs-edge-r02 using the IRB 601 MAC address for routing the packet. (The IRB 601 MAC address on cs-edge-r01 is different than the IRB 601 MAC address on cs-edge-r02.) The reth1 interface on the SRX cluster is a single LAG. The LAG address hashing results in a packet destined to the cs-edge-r01 MAC address being sent to cs-edge-r02. In an MC-LAG configuration, MAC address learning does not occur on the ICL link. As a result, cs-edge-r02 floods the packet on VLAN 601.

   To avoid flooding on VLAN 601, we specified the MAC address for cs-edge-r01 in the **static-mac**option on cs-edge-r02 and vice versa. Now when a packet destined to cs-edge-r01 arrives at cs-edge-r02, cs-edge-r02 sends the packet to cs-edge-r01 using the static MAC address configured.

2. Configure IRB interfaces on edge devices for dynamic routing.

   This configuration was used for cs-edge-r01 and cs-edge-r02.

   ```
   [edit]
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 arp
     172.16.33.11 l2-interface ae0.1
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 arp
     172.16.33.11 mac 3c:8a:b0:cf:1f:f0
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 arp
     172.16.33.11 publish
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 virtual-address 172.16.33.9
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 priority 250
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 preempt
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 accept-data
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 authentication-type md5
   user@host# set interfaces irb unit 601 family inet address 172.16.33.10/29 vrrp-group
     1 authentication-key "$9$nDoy9tOhSeX7V1R7VwYZG69A"
   ```

3. Configure VLAN interfaces on the core.

This configuration was used for cs-core-sw01 and cs-core-sw02.

```
[edit]
user@host# set vlans Firewall-trust vlan-id 600
user@host# set vlans Firewall-trust l3-interface irb.600
user@host# set vlans Firewall-trust domain-type bridge
user@host# set vlans Firewall-trust switch-options interface ae29.0 static-mac
  28:8a:1c:e3:f7:f0
```

NOTE: The static-macoption on firewall-trust VLAN 600 prevents traffic arriving from the SRX cluster from flooding the VLAN.

The SRX cluster sends traffic to both core switches using the IRB 600 MAC address for routing the packet. The IRB 600 MAC address is different on cs-core-sw1 from cs-core-sw2. Because the reth0 interface on the chassis cluster is a single LAG, the reth0 LAG address hashing results in a packet destined to the cs-core-sw1 MAC address being sent to cs-core-sw2. In an MC-LAG configuration, MAC address learning does not occur on the ICL link. As a result, cs-core-sw2 floods the packet on VLAN 600.

To avoid flooding on VLAN 600, we specifed the MAC address for cs-core-sw1 in the static-macoption on cs-core-sw2 and the MAC address for cs-core-sw2 on cs-core-sw1 and vice versa. Now when a packet that was destined to cs-core-sw1 arrives at cs-core-sw2, cs-core-sw2 sends the packet to cs-core-sw1 using the static MAC address.

4. Configure IRB interfaces on the core for dynamic routing.

   This configuration was used for cs-core-sw01 and cs-core-sw02.

   ```
   [edit]
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 arp
     172.16.33.2 l2-interface ae29.0
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 arp
     172.16.33.2 mac 28:8a:1c:e5:3b:f0
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 virtual-address 172.16.33.1
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 priority 125
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 preempt
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 accept-data
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 authentication-type md5
   user@host# set interfaces irb unit 600 family inet address 172.16.33.3/29 vrrp-group
     1 authentication-key "$9$9FCMt0IylMNdsEcds24DjCtu"
   ```

5. On the core devices, create client VLANs that map to the access.

   ```
   [edit]
   user@host# set vlans eng1_data_wired vlan-id 60
   ```

```
user@host# set vlans eng1_data_wired domain-type bridge
```

This example configuration is shown for one client VLAN. Configure this for all relevant client VLANs in your campus.

6. Create the IRB interface in the VLAN.

```
[edit]
user@host# set interfaces irb unit 60 family inet address 10.32.0.3/20 arp 10.32.0.2
  l2-interface ae29.0
user@host# set interfaces irb unit 60 family inet address 10.32.0.3/20 arp 10.32.0.2
  mac 28:8a:1c:e5:3b:f0
```

7. Configure the IRB routing interface for client VLANs.

```
[edit]
user@host# set vlans eng1_data_wired l3-interface irb.60
```

8. Add voice VLAN ports to access switches where needed.

   - On access devices that are EX4200, EX3300, and EX2200 switches the configuration is as follows:

```
[edit]
user@host# set ethernet-switching-options voip interface ge-0/0/42.0 vlan
  eng1_voice_wired
user@host# set ethernet-switching-options voip interface ge-0/0/42.0
  forwarding-class voice
```

   - On access devices that are EX4300 switches the configuration is as follows:

```
[edit]
user@host# set switch-options voip interface ge-0/0/42.0 vlan eng1_voice_wired
user@host# set switch-options voip interface ge-0/0/42.0 forwarding-class
  voice
```

Configuring DHCP Relay in Midsize Enterprise Campus

Step-by-Step Procedure

DHCP relay is set up in order to properly support DHCP clients downstream.

To configure DHCP relay:

1. Configure DHCP relay in the aggregation.

```
[edit]
root@cs-agg-01# set forwarding-options helpers bootp server 172.16.4.102
root@cs-agg-01# set forwarding-options helpers bootp interface vlan.202
root@cs-agg-01# set forwarding-options helpers bootp interface ge-0/0/21
root@cs-agg-01# set forwarding-options helpers bootp interface vlan.10
```

2. Configure DHCP relay in the core.

```
root@core-sw-01# set forwarding-options dhcp-relay forward-snooped-clients
  all-interfaces
root@core-sw-01# set forwarding-options dhcp-relay overrides
  allow-snooped-clients
root@core-sw-01# set forwarding-options dhcp-relay server-group dhcp-srv
  172.16.4.102
root@core-sw-01# set forwarding-options dhcp-relay active-server-group dhcp-srv
```

```
root@core-sw-01# set forwarding-options dhcp-relay route-suppression destination
root@core-sw-01# set forwarding-options dhcp-relay group all interface ge-2/0/4.0
root@core-sw-01# set forwarding-options dhcp-relay group all interface irb.10
```

The same configuration is placed on core-sw-02.

NOTE: Configure dhcp-relay group all interface on all IRB interfaces in the core on both devices.

Configuring Multicast on Core Devices

Step-by-Step Procedure

To enabled multicast in the campus, multicast must be configured on the core, aggregation, and access.

To configure multicast on core devices:

1. Enable tunnel services on campus core device core-sw01.

```
[edit]
user@cs-core-sw01# set chassis fpc 0 pic 0 tunnel-services bandwidth 10g
user@cs-core-sw01# set chassis fpc 1 pic 0 tunnel-services bandwidth 10g
```

2. Configure core device core-sw01 as the primary rendezvous point (RP).

```
[edit]
user@cs-core-sw01# set protocols pim rp bootstrap-priority 200
user@cs-core-sw01# set protocols pim rp local address 172.16.32.5
```

NOTE: A higher number priority setting indicates the devices as the primary RP in the bootstrap configuration.

3. Configure PIM on all Layer 3 and IRB interfaces on core-sw01.

```
[edit]
user@cs-core-sw01# set protocols pim interface irb.10 hello-interval 2
user@cs-core-sw01# set protocols pim interface lo0.0
user@cs-core-sw01# set protocols pim interface xe-0/1/0.0 hello-interval 2
user@cs-core-sw01# set protocols pim interface ae10.0 hello-interval 2
user@cs-core-sw01# set protocols pim interface ae0.0 hello-interval 2
```

4. Configure IGMP on core-sw-01.

   Configure IGMP query settings.

```
[edit]
user@cs-core-sw01# set protocols igmp query-interval 3
user@cs-core-sw01# set protocols igmp query-response-interval 2
```

   Configure IGMP snooping on all VLAN interfaces.

```
[edit]
user@cs-core-sw01# set protocols igmp-snooping vlan eng1_data_wired interface
  ae29.0 multicast-router-interface
```

```
user@cs-core-sw01# set multicast-snooping-options
  multichassis-lag-replicate-state
```

Enable IGMP on IRB interfaces.

```
[edit]
user@cs-core-sw01# set protocols igmp interface irb.10
```

NOTE: At the global level, IGMP join and leave messages are replicated from the active link to the standby link of an MC-LAG interface, which enables faster recovery of membership information after failover. This command synchronizes multicast state across MC-LAG neighbors when bridge domains are configured.

5. Enable tunnel services on campus core device core-sw02.

```
[edit]
user@cs-core-sw02# set chassis fpc 0 pic 0 tunnel-services bandwidth 10g
user@cs-core-sw02# set chassis fpc 1 pic 0 tunnel-services bandwidth 10g
```

6. Configure core device core-sw02 as the secondary RP.

```
[edit]
user@cs-core-sw02# set protocols pim rp bootstrap-priority 100
user@cs-core-sw02# set protocols pim rp local address 172.16.32.6
```

NOTE: A lower priority setting indicates this devices is the secondary RP in the bootstrap configuration.

7. Configure PIM on all Layer 3 and IRB interfaces on core-sw02.

```
[edit]
user@cs-core-sw02# set protocols pim interface irb.10 hello-interval 2
user@cs-core-sw02# set protocols pim interface lo0.0
user@cs-core-sw02# set protocols pim interface xe-0/1/0.0 hello-interval 2
user@cs-core-sw02# set protocols pim interface ge-2/1/3.0
user@cs-core-sw02# set protocols pim interface ae0.0 hello-interval 2
```

8. Configure IGMP on core-sw-02.

Configure IGMP query settings.

```
[edit]
user@cs-core-sw02# set protocols igmp query-interval 3
user@cs-core-sw02# set protocols igmp query-response-interval 2
```

Enable IGMP on all VLAN interfaces.

```
[edit]
user@cs-core-sw02# set protocols igmp-snooping vlan eng1_data_wired interface
  ae29.0 multicast-router-interface
```

Enable IGMP on IRB interfaces.

```
[edit]
user@cs-core-sw02# set protocols igmp interface irb.10
```

Configuring Multicast on Aggregation and Access Devices

Step-by-Step Procedure

To enable multicast in the campus, multicast must be configured on the core, aggregation, and access.

To configure multicast on the aggregation and access devices (cs-agg-01, cs-4200-ab1, cs-4300-ab2, cs-4300-ab3, cs-3300-ab4, and cs-2200-ab5):

1. Enable PIM.

```
[edit]
user@host# set protocols pim traceoptions file pim.log
user@host# set protocols pim traceoptions flag all
user@host# set protocols pim interface vlan.11
user@host# set protocols pim interface xe-0/0/0.0 hello-interval 2
user@host# set protocols pim interface xe-1/0/0.0 hello-interval 2
```

2. Enable IGMP on all relevant VLANs connected to multicast clients.

   The following example is for one RVI:

```
[edit]
user@host# set protocols igmp interface vlan.10
```

NOTE: Enable IGMP on all RVIs.

3. Enable IGMP snooping on all VLAN interfaces.

```
[edit]
user@host# set protocols igmp-snooping vlan all
```

Configuring BGP Routing

Step-by-Step Procedure

The edge layer of the campus is defined where the ISP handoff occurs. Here, open standard EBGP is configured with two different ISP connections for ISP1 and ISP2, which are connected to cs-edge-r01 and cs-edge-r02, respectively. In this example, cs-edge-r01 and cs-edge-r02 peer to each other using IBGP with an export policy to enable next-hop self. The BGP local preference has been configured to prefer the ISP1 gateway connected to cs-edge-r01.

Client device Internet access is provided using source NAT on the edge firewall and forwarded to the edge routers for Internet access to service provider networks. Remote access users connecting from the Internet will use the public IP address of the VPN gateway, so the appliance hosting the gateway IP subnet is advertised to the Internet using the export policy from the edge routers. To support redundancy, each edge router is advertising the same prefix into the Internet.

To configure BGP routing:

1. Configure cs-edge-r01 interface to connect to ISP1.

```
[edit]
user@cs-edge-r01# set interfaces ge-1/1/5 hold-time up 46000
user@cs-edge-r01# set interfaces ge-1/1/5 hold-time down 100
user@cs-edge-r01# set interfaces ge-1/1/5 unit 0 family inet address
  192.168.168.5/30
```

NOTE: The hold-time setting has been tuned on this interface to get better convergence. If this is not added, higher convergence might be observed because this interface could be waiting to receive traffic while the underlying MC-LAG has not yet converged.

2. Configure BGP on cs-edge-r01.

```
[edit]
user@cs-edge-r01# set routing-options autonomous-system 64514
user@cs-edge-r01# set protocols bgp group ebgp-edge-r1 type external
user@cs-edge-r01# set protocols bgp group ebgp-edge-r1 export exp-pub-net
  #Export 10.92.84.0/24 network for SA access to internet
user@cs-edge-r01# set protocols bgp group ebgp-edge-r1 peer-as 64512
user@cs-edge-r01# set protocols bgp group ebgp-edge-r1 neighbor 192.168.168.6
```

3. Configure IBGP peering on cs-edge-r01 to cs-edge-r02.

```
[edit]
user@cs-edge-r01# set protocols bgp group ibgp type internal
user@cs-edge-r01# set protocols bgp group ibgp local-preference 150
user@cs-edge-r01# set protocols bgp group ibgp local-address 172.16.32.53
user@cs-edge-r01# set protocols bgp group ibgp peer-as 64514
user@cs-edge-r01# set protocols bgp group ibgp bfd-liveness-detection
  minimum-interval 300
user@cs-edge-r01# set protocols bgp group ibgp neighbor 172.16.32.54
```

4. Configure next-hop self.

```
[edit]
user@cs-edge-r01# set protocols bgp group ibgp export next-hop-self
```

5. Configure the routing policy on cs-edge-r01 for remote access.

```
[edit]
user@cs-edge-r01# set policy-options policy-statement exp-pub-net from protocol
  ospf
user@cs-edge-r01# set policy-options policy-statement exp-pub-net from route-filter
  10.92.84.0/24 exact accept
user@cs-edge-r01# set policy-options policy-statement exp-pub-net then accept
```

6. Configure the next-hop self policy.

```
[edit]
user@cs-edge-r01# set policy-options policy-statement next-hop-self term next-hop
  then next-hop self
```

7. Configure BGP on cs-edge-r02.

```
[edit]
user@cs-edge-r02# set routing-options autonomous-system 64514
user@cs-edge-r02# set protocols bgp group ebgp-edge-r2 type external
user@cs-edge-r02# set protocols bgp group ebgp-edge-r2 export exp-pub-net
user@cs-edge-r02# set protocols bgp group ebgp-edge-r2 peer-as 64513
user@cs-edge-r02# set protocols bgp group ebgp-edge-r2 neighbor 192.168.168.10
```

8. Configure IBGP peering on cs-edge-r02 to cs-edge-r01.

```
[edit]
user@cs-edge-r02# set protocols bgp group ibgp type internal
user@cs-edge-r02# set protocols bgp group ibgp local-address 172.16.32.54
user@cs-edge-r02# set protocols bgp group ibgp export next-hop-self
user@cs-edge-r02# set protocols bgp group ibgp peer-as 64514
user@cs-edge-r02# set protocols bgp group ibgp bfd-liveness-detection
  minimum-interval 300
user@cs-edge-r02# set protocols bgp group ibgp neighbor 172.16.32.53
```

9. Configure the remote access policy on cs-edge-r02.

```
[edit]
user@cs-edge-r02# set policy-options policy-statement exp-pub-net from protocol
  ospfuser@cs-edge-r02#
user@cs-edge-r02# set policy-options policy-statement exp-pub-net from
  route-filter 10.92.84.0/24 exact accept
user@cs-edge-r02# set policy-options policy-statement exp-pub-net then accept
```

10. Configure the next-hop self policy on cs-edge-r02.

```
[edit]
user@cs-edge-r02# set policy-options policy-statement next-hop-self term next-hop
  then next-hop self
```

Configuring OSPF Routing for the Midsize Enterprise Campus

Step-by-Step Procedure

This solution uses OSPF as the IGP protocol because of the widespread familiarity of the protocol.

Key configuration parameters:

- Two OSPF areas (area 0 and area 1) are configured to localize the failure with the area boundary.
- Edge routers and firewalls are configured with MC-LAG and IRB (Layer 3) interfaces in area 1 .
- The link between core devices is in area 0.
- The link between core devices, aggregation device, and WAN are in area 0.
- Each core switch and edge router is to be configured with an OSPF priority of 255 and 254 to strictly enforce that the core and edge devices always become the designated router and backup designated router for that bridge domain.
- All IRBs and VRRP addresses are advertised into OSPF as passive so that sessions do not get established.
- Conditional-based default aggregate routes from edge routers are redistributed towards the core and other devices to connect to the Internet.
- LFA is configured on all OSPF links to improve convergence.

To configure OSPF routing:

1. Enable LFA on OSPF links.

   The following command should be configured on all devices that will participate in OSPF.

   ```
   [edit]
   user@host# set protocols ospf area 0.0.0.1 interface irb.600 node-link-protection
   ```

   The IRB participating in OSPF should also be set to LFA.

2. Configure per-packet load balancing to allow the Packet Forward Engine to retain the LFA backup next hops.

   ```
   [edit]
   user@host# set policy-options policy-statement pplb then load-balance per-packet
   user@host# set policy-options policy-statement pplb then accept
   ```

3. Configure OSPF on edge devices, cs-edge-r01 and cs-edge-r02.

   ```
   [edit]
   user@host# set protocols ospf export ospf-default
   user@host# set protocols ospf reference-bandwidth 1000g
   user@host# set protocols ospf area 0.0.0.1 interface ae0.0 node-link-protection
   user@host# set protocols ospf area 0.0.0.1 interface ae0.0 priority 254
   ```

4. Enable the BFD protection IRB routing interface on cs-edge-r01 and cs-edge-r02.

   ```
   [edit]
   ```

```
user@host# set protocols ospf area 0.0.0.1 interface ae0.0 node-link-protection
user@host# set protocols ospf area 0.0.0.1 interface ae0.0 priority 254
user@host# set protocols ospf area 0.0.0.1 interface ae0.0 authentication md5 200
  key "$9$E6OSlM7-waZj8XZjHqQzhSre8XNdb2oJ"
user@host# set protocols ospf area 0.0.0.1 interface ae0.0 bfd-liveness-detection
  minimum-interval 300
user@host# set protocols ospf area 0.0.0.1 interface ae0.0 bfd-liveness-detection
  detection-time threshold 2000
user@host# set protocols ospf area 0.0.0.1 interface lo0.0
user@host# set protocols ospf area 0.0.0.1 interface irb.601 node-link-protection
user@host# set protocols ospf area 0.0.0.1 interface irb.601 priority 254
user@host# set protocols ospf area 0.0.0.1 interface irb.601 authentication md5
  200 key "$9$tPnx01hevLVwgSrwgoJHkp0BISrKM87db"
user@host# set protocols ospf area 0.0.0.1 interface irb.601 bfd-liveness-detection
  minimum-interval 2400
```

5. Configure the condition policy for the OSPF default route based on the BGP route on cs-edge-r01 and cs-edge-r02.

```
[edit]
user@host# set policy-options policy-statement ospf-default from protocol
  aggregate
user@host# set policy-options policy-statement ospf-default from route-filter
  0.0.0.0/0 exact
user@host# set policy-options policy-statement ospf-default then external type
  1user@host#
user@host# set policy-options policy-statement ospf-default then accept
user@host# set policy-options policy-statement filter-contributors term 1 from
  neighbor 192.168.168.6
user@host# set policy-options policy-statement filter-contributors term 1 from
  next-hop 192.168.168.6
user@host# set policy-options policy-statement filter-contributors term 1 then
  accept
user@host# set policy-options policy-statement filter-contributors term 2 then
  reject
user@host# set policy-options policy-statement pplb then load-balance per-packet
user@host# set policy-options policy-statement pplb then accept
user@host# set routing-options generate route 0.0.0.0/0 policy filter-contributors
user@host# set routing-options forwarding-table export pplb
```

6. Configure OSPF on the edge firewall devices.

```
[edit]
user@host-fw# set protocols ospf export pub-network
user@host-fw# set protocols ospf reference-bandwidth 1000g
user@host-fw# set protocols ospf area 0.0.0.1 interface reth0.0 node-link-protection
user@host-fw# set protocols ospf area 0.0.0.1 interface reth0.0 priority 255
user@host-fw# set protocols ospf area 0.0.0.1 interface reth0.0 authentication
  md5 200 key "$9$69OnCpBcyKxNbIENbs2GU/CtuIESreWX7"
user@host-fw# set protocols ospf area 0.0.0.1 interface reth0.0
  bfd-liveness-detection minimum-interval 2400
user@host-fw# set protocols ospf area 0.0.0.1 interface reth1.0 node-link-protection
user@host-fw# set protocols ospf area 0.0.0.1 interface reth1.0 authentication md5
  200 key "$9$qPT3ApBSrv69rvWLVb.P5Q69tuORcy"
user@host-fw# set protocols ospf area 0.0.0.1 interface reth1.0
  bfd-liveness-detection minimum-interval 2400
```

7. Export the subnet used for source NAT to the edge firewall.

```
[edit]
user@host-fw# set policy-options policy-statement pub-network term 1 from
  protocol static
user@host-fw# set policy-options policy-statement pub-network term 1 from
  route-filter 10.92.84.0/24 exact accept
user@host-fw# set policy-options policy-statement pub-network term 1 to neighbor
  172.16.33.10
user@host-fw# set policy-options policy-statement pub-network term 1 to neighbor
  172.16.33.11
user@host-fw# set policy-options policy-statement pub-network term 1 then accept
user@host-fw# set routing-options static route 10.92.84.0/24 receive
```

8. Configure OSPF on the aggregation device.

```
[edit]
user@agg# set protocols ospf reference-bandwidth 1000g
user@agg# set protocols ospf area 0.0.0.0 interface vlan.13 passive
user@agg# set protocols ospf area 0.0.0.0 interface vlan.20 passive ## configure
  on all RVI's##
user@agg# set protocols ospf area 0.0.0.0 interface xe-0/0/0.0
  node-link-protectionuser@agg#
user@agg# set protocols ospf area 0.0.0.0 interface xe-0/0/0.0 priority 255
user@agg# set protocols ospf area 0.0.0.0 interface xe-0/0/0.0 authentication
  md5 100 key "$9$IEXhyKX7V4aUM8aUjH5TRhS"
user@agg# set protocols ospf area 0.0.0.0 interface xe-0/0/0.0
  bfd-liveness-detection minimum-interval 300
user@agg# set protocols ospf area 0.0.0.0 interface xe-1/0/0.0 node-link-protection
user@agg# set protocols ospf area 0.0.0.0 interface xe-1/0/0.0 priority 255
user@agg# set protocols ospf area 0.0.0.0 interface xe-1/0/0.0 authentication
  md5 100 key "$9$ZcDHmz39O1hfT1hSr8LGDi"
user@agg# set protocols ospf area 0.0.0.0 interface xe-1/0/0.0
  bfd-liveness-detection minimum-interval 300
```

Verification

Confirm that the configuration is working properly.

Verifying BGP Routing on Edge Devices

Purpose Verify that BGP routing is configured properly and running on the edge devices.

Action

- Check the BGP summary table on edge devices.

```
root@cs-edge-r01# run show bgp summary
Groups: 2 Peers: 2 Down peers: 0 Table          Tot Paths  Act Paths Suppressed
    History Damp State    Pending inet.0                     1          1
        0          0          0          0 Peer                    AS
InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
```

```
State|#Active/Received/Accepted/Damped... 172.16.32.34         64514     47618
      47618       0       0     2w0d23h 0/0/0/0              0/0/0/0
192.168.168.6         64512      48034      48222       0       1  1d 1:47:05
1/1/1/0              0/0/0/0

root@cs-edge-r02# run show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                       2          1          0          0          0
0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
172.16.32.33          64514      47621      47622       0       0     2w0d23h
1/1/1/0              0/0/0/0
192.168.168.10        64513      48580      48190       0       0     2w0d23h
0/1/1/0              0/0/0/0
```

- Verify the routing table on cs-edge-r01. Check that the ISP1 route advertisement is received in the route table. Check that the ISP1 route is advertised as well.

```
root@cs-edge-r01# run show route receive-protocol bgp 192.168.168.6

inet.0: 165 destinations, 165 routes (165 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 172.16.32.49/32         192.168.168.6                           64512 64515
I


root@cs-edge-r01# run show route advertising-protocol bgp 192.168.168.6

inet.0: 165 destinations, 165 routes (165 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.92.84.0/24           Self                 0                  I
```

- Verify the routing table on cs-edge-r02. Check that the ISP2 route advertisement received is in the route table. Check that the ISP2 route is advertised as well.

```
root@cs-edge-r02# run show route receive-protocol bgp 192.168.168.10
inet.0: 165 destinations, 167 routes (165 active, 0 holddown, 1 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  172.16.32.49/32         192.168.168.10                          64513 64515
I

root@cs-edge-r02# run show route advertising-protocol bgp 192.168.168.10
inet.0: 165 destinations, 167 routes (165 active, 0 holddown, 1 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.92.84.0/24           Self                 0                  I
* 172.16.32.49/32         Self                                    64512 64515
I
```

Meaning Confirm that dynamic routing protocols are running and that static and dynamic routes are properly learned and advertised.

Verifying OSPF Routing

Purpose Verify that OSPF routing and LFA has been properly configured on devices.

Action

- Verify that all OSPF sessions are up.

```
root@cs-core-sw01# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.32.10     ae0.0                  Full      2.2.2.2          128    38
172.16.32.58     ae10.0                 Full      172.16.32.97     255    30
172.16.32.14     xe-0/1/0.0             Full      8.8.8.8          255    38
172.16.32.22     xe-0/1/2.0             Full      9.9.9.9          255    30
172.16.33.4      irb.600                Full      3.3.3.3          255    32
172.16.33.2      irb.600                Full      2.2.2.2          255    32

root@cs-core-sw02# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.32.9      ae0.0                  Full      1.1.1.1          128    31
172.16.32.62     ae10.0                 Full      172.16.32.97     255    35
172.16.32.18     xe-0/1/0.0             Full      8.8.8.8          255    36
172.16.32.26     xe-0/1/2.0             Full      9.9.9.9          255    34
172.16.33.4      irb.600                Full      3.3.3.3          255    33
172.16.33.3      irb.600                Full      1.1.1.1          255    37

root@cs-agg-01# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.32.13     xe-0/0/0.0             Full      1.1.1.1          255    38
172.16.32.17     xe-1/0/0.0             Full      2.2.2.2          255    35

root@cs-edge-fw01-node0# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.33.2      reth0.0                Full      2.2.2.2          255    39
172.16.33.3      reth0.0                Full      1.1.1.1          255    32
172.16.33.10     reth1.0                Full      4.4.4.4          254    38
172.16.33.11     reth1.0                Full      5.5.5.5          254    37

root@cs-edge-r01# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.32.42     ae0.0                  Full      5.5.5.5          254    39
172.16.32.54     ge-1/1/4.0             Full      5.5.5.5          128    34
172.16.33.12     irb.601                Full      3.3.3.3          128    39
172.16.33.11     irb.601                Full      5.5.5.5          254    35

root@cs-edge-r02# run show ospf neighbor
Address          Interface              State     ID               Pri  Dead
172.16.32.41     ae0.0                  Full      4.4.4.4          254    38
172.16.32.53     ge-1/1/4.0             Full      4.4.4.4          128    38
172.16.33.12     irb.601                Full      3.3.3.3          128    38
172.16.33.10     irb.601                Full      4.4.4.4          254    35
```

- Verify the OSPF conditional-based default route advertisement into OSPF.

```
root@cs-core-sw01# run show route 0.0.0.0
inet.0: 1012 destinations, 1012 routes (1012 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 04:41:12, metric 1500, tag 0
                    > to 172.16.33.4 via irb.600

root@cs-edge-fw01-node0# run show route 0.0.0.0

inet.0: 167 destinations, 168 routes (167 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[OSPF/150] 11:36:45, metric 500, tag 0
                    > to 172.16.33.10 via reth1.0


root@cs-edge-r01# run show route 0.0.0.0
```

```
inet.0: 165 destinations, 165 routes (165 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Aggregate/130] 2w1d 00:34:35
                    > to 192.168.168.6 via ge-1/1/5.0
```

- Verify the OSPF LFA routes.

```
root@cs-core-sw01# run show ospf backup coverage
Topology default coverage:

Node Coverage:

Area             Covered  Total  Percent
                   Nodes  Nodes  Covered
0.0.0.0                3      4   75.00%
0.0.0.1                0      4    0.00%

Route Coverage:

Path Type  Covered   Total  Percent
           Routes  Routes  Covered
Intra          71     150   47.33%
Inter           0       0  100.00%
Ext1            0       1    0.00%
Ext2            0       1    0.00%
All            71     152   46.71%
```

```
root@cs-agg-01# run show ospf backup coverage
Topology default coverage:

Node Coverage:

Area             Covered  Total  Percent
                   Nodes  Nodes  Covered
0.0.0.0                4      4  100.00%

Route Coverage:

Path Type  Covered   Total  Percent
           Routes  Routes  Covered
Intra          99     142   69.72%
Inter           8       8  100.00%
Ext1            1       1  100.00%
Ext2            1       1  100.00%
All           109     152   71.71%
```

Meaning Confirm the OSPF is configured properly and advertising routes from IBGP. LFA is enabled and working properly.

Verifying DHCP Relay

Purpose Verify that DHCP relay has been properly configured and enabled on devices.

Action

- Verify DHCP relay information on aggregation device.

```
root@cs-agg-01# run show helper statistics
 BOOTP:
  Received packets: 4435
```

```
  Forwarded packets: 4435
  Dropped packets: 0
    Due to no interface in DHCP Relay database: 0
    Due to no matching routing instance: 0
    Due to an error during packet read: 0
    Due to an error during packet send: 0
    Due to invalid server address: 0
    Due to no valid local address: 0
    Due to no route to server/client: 0
```

- Verify DHCP relay on the core devices.

```
root@cs-core-sw01# run show dhcp relay binding summary
1862 clients, (0 init, 1855 bound, 0 selecting, 0 requesting, 0 renewing, 7
rebinding, 0 releasing)

root@cs-core-sw01# run show dhcp relay binding | match ae3.0
10.32.0.57        2981        00:10:94:00:04:47  670489      BOUND      ae3.0
10.16.0.53        2982        00:10:94:00:04:48  670489      BOUND      ae3.0
10.17.0.52        2983        00:10:94:00:04:49  670489      BOUND      ae3.0
10.32.0.55        2980        00:10:94:00:64:01  670489      BOUND      ae3.0
10.32.17.23       2995        00:22:22:00:04:0b  670592      BOUND      ae3.0
10.32.17.20       2997        00:22:22:00:04:0c  670592      BOUND      ae3.0
10.32.17.19       2996        00:22:22:00:04:0d  670592      BOUND      ae3.0
10.32.17.14       2999        00:22:22:00:04:0e  670592      BOUND      ae3.0
```

Meaning Confirm that DHCP relay is configured properly and has been enabled.

Verifying Multicast in the Midsize Enterprise Campus

Purpose Verify that multicast has been properly configured on devices.

Action

- Verify multicast routing on the aggregation device.

```
root@cs-agg-01# run show multicast route
Instance: master Family: INET

Group: 230.1.1.1
    Source: 172.16.34.10/32
    Upstream interface: xe-0/0/0.0
    Downstream interface list:
        vlan.20 vlan.30 vlan.50 vlan.60

Group: 230.1.1.2
    Source: 172.16.34.10/32
    Upstream interface: xe-0/0/0.0
    Downstream interface list:
        vlan.20 vlan.30 vlan.50 vlan.60

Group: 230.1.1.3
    Source: 172.16.34.10/32
    Upstream interface: xe-0/0/0.0
    Downstream interface list:
        vlan.20 vlan.30 vlan.50 vlan.60

Group: 230.1.1.4
    Source: 172.16.34.10/32
    Upstream interface: xe-0/0/0.0
    Downstream interface list:
```

```
        vlan.20 vlan.30 vlan.50 vlan.60

Group: 230.1.1.5
    Source: 172.16.34.10/32
    Upstream interface: xe-0/0/0.0
    Downstream interface list:
        vlan.20 vlan.30 vlan.50 vlan.60

Instance: master Family: INET6
```

- Verify PIM neighbors and PIM interfaces on the aggregation device.

```
root@cs-agg-01# run show pim neighbors
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.master
Interface           IP V Mode        Option       Uptime Neighbor addr
xe-0/0/0.0           4 2             HPLGT   1d 07:03:44 172.16.32.13
xe-1/0/0.0           4 2             HPLGT   3d 09:02:54 172.16.32.17
```

```
root@cs-agg-01# run show pim interfaces
Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name              Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
pime.32769         Up   S     4 2 P2P,NotCap        0 0/0
pime.32770         Up   S     4 2 P2P,NotCap        0 0/0
vlan.10            Up   S     4 2 DR,NotCap         0 0/0            10.48.0.1
vlan.100           Up   S     4 2 DR,NotCap         0 0/0            10.68.0.1
vlan.101           Up   S     4 2 DR,NotCap         0 0/0           10.68.16.1
vlan.102           Up   S     4 2 DR,NotCap         0 0/0           10.68.32.1
vlan.103           Up   S     4 2 DR,NotCap         0 0/0           10.68.48.1
vlan.11            Up   S     4 2 DR,NotCap         0 0/0           10.48.16.1
vlan.12            Up   S     4 2 DR,NotCap         0 0/0           10.48.32.1
vlan.13            Up   S     4 2 DR,NotCap         0 0/0           10.48.48.1
vlan.20            Up   S     4 2 DR,NotCap         0 0/0            10.49.0.1
vlan.202           Up   S     4 2 DR,NotCap         0 0/0          172.16.144.1
vlan.21            Up   S     4 2 DR,NotCap         0 0/0            10.49.4.1
vlan.22            Up   S     4 2 DR,NotCap         0 0/0            10.49.8.1
vlan.23            Up   S     4 2 DR,NotCap         0 0/0           10.49.12.1
vlan.30            Up   S     4 2 DR,NotCap         0 0/0           10.49.64.1
vlan.31            Up   S     4 2 DR,NotCap         0 0/0           10.49.68.1
vlan.32            Up   S     4 2 DR,NotCap         0 0/0           10.49.72.1
vlan.33            Up   S     4 2 DR,NotCap         0 0/0           10.49.76.1
vlan.40            Up   S     4 2 DR,NotCap         0 0/0          10.49.128.1
vlan.41            Up   S     4 2 DR,NotCap         0 0/0          10.49.132.1
vlan.42            Up   S     4 2 DR,NotCap         0 0/0          10.49.136.1
vlan.43            Up   S     4 2 DR,NotCap         0 0/0          10.49.140.1
vlan.50            Up   S     4 2 DR,NotCap         0 0/0            10.50.0.1
vlan.51            Up   S     4 2 DR,NotCap         0 0/0           10.50.16.1
vlan.52            Up   S     4 2 DR,NotCap         0 0/0           10.50.32.1
vlan.53            Up   S     4 2 DR,NotCap         0 0/0           10.50.48.1
vlan.60            Up   S     4 2 DR,NotCap         0 0/0            10.64.0.1
vlan.61            Up   S     4 2 DR,NotCap         0 0/0           10.64.16.1
vlan.62            Up   S     4 2 DR,NotCap         0 0/0           10.64.32.1
vlan.63            Up   S     4 2 DR,NotCap         0 0/0           10.64.48.1
vlan.70            Up   S     4 2 DR,NotCap         0 0/0            10.65.0.1
```

```
vlan.71             Up    S      4 2 DR,NotCap         0 0/0            10.65.16.1
vlan.72             Up    S      4 2 DR,NotCap         0 0/0            10.65.32.1
vlan.73             Up    S      4 2 DR,NotCap         0 0/0            10.65.48.1
vlan.80             Up    S      4 2 DR,NotCap         0 0/0            10.66.0.1
vlan.81             Up    S      4 2 DR,NotCap         0 0/0            10.66.16.1
vlan.82             Up    S      4 2 DR,NotCap         0 0/0            10.66.32.1
vlan.83             Up    S      4 2 DR,NotCap         0 0/0            10.66.48.1
vlan.90             Up    S      4 2 DR,NotCap         0 0/0            10.67.0.1
vlan.91             Up    S      4 2 DR,NotCap         0 0/0            10.67.16.1
vlan.92             Up    S      4 2 DR,NotCap         0 0/0            10.67.32.1
vlan.93             Up    S      4 2 DR,NotCap         0 0/0            10.67.48.1
xe-0/0/0.0          Up    S      4 2 DR,NotCap         1 0/5          172.16.32.14
xe-1/0/0.0          Up    S      4 2 DR,NotCap         1 0/0          172.16.32.18
```

- Verify PIM rendezvous points on the aggregation device.

```
root@cs-agg-01# run show pim rps
Instance: PIM.master

address-family INET
RP address      Type        Mode   Holdtime Timeout Groups Group prefixes
172.16.32.5     bootstrap   sparse      150     131      5 224.0.0.0/4
172.16.32.6     bootstrap   sparse      150     131      0 224.0.0.0/4

address-family INET6
```

- Verify IGMP interfaces and IGMP snooping on the aggregation device.

```
root@cs-agg-01# run show igmp interface
Interface: vlan.10
    Querier: 10.48.0.1
    State:         Up Timeout:    None Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: vlan.11
    Querier: 10.48.16.1
    State:         Up Timeout:    None Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: vlan.12
    Querier: 10.48.32.1
    State:         Up Timeout:    None Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: vlan.13
    Querier: 10.48.48.1
    State:         Up Timeout:    None Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: vlan.20
    Querier: 10.49.0.1
    State:         Up Timeout:    None Version:  2 Groups:      5
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
```

```
root@cs-agg-01# run show igmp-snooping membership
 VLAN: Radius-vlan
VLAN: default
```

```
VLAN: eng1_data_wired
    230.1.1.1      *
        Interfaces: ae4.0, ae5.0
    230.1.1.2      *
        Interfaces: ae4.0, ae5.0
    230.1.1.3      *
        Interfaces: ae4.0, ae5.0
    230.1.1.4      *
        Interfaces: ae4.0, ae5.0
    230.1.1.5      *
        Interfaces: ae4.0, ae5.0
VLAN: eng1_data_wireless
VLAN: eng1_voice_wired
VLAN: eng1_voice_wireless
:
:
:
VLAN: exec_voice_wireless
VLAN: finance_data_wired
    230.1.1.1      *
        Interfaces: ae4.0
    230.1.1.2      *
        Interfaces: ae4.0
    230.1.1.3      *
        Interfaces: ae4.0
    230.1.1.4      *
        Interfaces: ae4.0
    230.1.1.5      *
        Interfaces: ae4.0
VLAN: finance_data_wireless
VLAN: finance_voice_wired
VLAN: finance_voice_wireless
VLAN: guest
VLAN: guest_cap
VLAN: legal_data_wired
    230.1.1.1      *
        Interfaces: ae4.0
    230.1.1.2      *
        Interfaces: ae4.0
    230.1.1.3      *
        Interfaces: ae4.0
    230.1.1.4      *
        Interfaces: ae4.0
    230.1.1.5      *
        Interfaces: ae4.0
VLAN: legal_data_wireless
VLAN: legal_voice_wired
VLAN: legal_voice_wireless
VLAN: marketing_data_wired
    230.1.1.1      *
        Interfaces: ae5.0
    230.1.1.2      *
        Interfaces: ae5.0
    230.1.1.3      *
        Interfaces: ae5.0
    230.1.1.4      *
        Interfaces: ae5.0
    230.1.1.5      *
        Interfaces: ae5.0
VLAN: remediation
```

- Verify multicast routing on the core devices.

```
root@cs-core-sw01# run show multicast route
Instance: master Family: INET

Group: 230.1.1.1
    Source: 172.16.34.10/32
    Upstream interface: ae10.0
    Downstream interface list:
        irb.10 irb.20 irb.30 irb.50 irb.60 xe-0/1/0.0

Group: 230.1.1.2
    Source: 172.16.34.10/32
    Upstream interface: ae10.0
    Downstream interface list:
        irb.10 irb.20 irb.30 irb.50 irb.60 xe-0/1/0.0

Group: 230.1.1.3
    Source: 172.16.34.10/32
    Upstream interface: ae10.0
    Downstream interface list:
        irb.10 irb.20 irb.30 irb.50 irb.60 xe-0/1/0.0

Group: 230.1.1.4
    Source: 172.16.34.10/32
    Upstream interface: ae10.0
    Downstream interface list:
        irb.10 irb.20 irb.30 irb.50 irb.60 xe-0/1/0.0

Group: 230.1.1.5
    Source: 172.16.34.10/32
    Upstream interface: ae10.0
    Downstream interface list:
        irb.10 irb.20 irb.30 irb.50 irb.60 xe-0/1/0.0

Instance: master Family: INET6
```

- Verify PIM neighbors, PIM interfaces, and PIM joins on the core devices.

```
root@cs-core-sw01# run show pim neighbors
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.master
Interface           IP V Mode        Option       Uptime Neighbor addr
ae0.0                4 2             HPLGT    1d 07:05:55 172.16.32.10
ae10.0               4 2             HPLGT    1d 07:05:55 172.16.32.58
irb.10               4 2             HPLGT    1d 07:05:55 10.16.0.2
irb.100              4 2             HPLGT    1d 07:05:55 10.36.0.2
irb.101              4 2             HPLGT    1d 07:05:55 10.36.16.2
irb.102              4 2             HPLGT    1d 07:05:55 10.36.32.2
irb.103              4 2             HPLGT    1d 07:05:55 10.36.48.2
irb.11               4 2             HPLGT    1d 07:05:55 10.16.16.2
irb.12               4 2             HPLGT    1d 07:05:55 10.16.32.2
irb.13               4 2             HPLGT    1d 07:05:55 10.16.48.2
irb.20               4 2             HPLGT    1d 07:05:55 10.17.0.2
irb.201              4 2             HPLGT    1d 07:05:55 172.16.128.2
irb.21               4 2             HPLGT    1d 07:05:55 10.17.4.2
irb.22               4 2             HPLGT    1d 07:05:55 10.17.8.2
irb.23               4 2             HPLGT    1d 07:05:55 10.17.12.2
irb.30               4 2             HPLGT    1d 07:05:55 10.17.64.2
```



```
irb.31              4 2             HPLGT   1d 07:05:55 10.17.68.2
irb.32              4 2             HPLGT   1d 07:05:55 10.17.72.2
irb.33              4 2             HPLGT   1d 07:05:55 10.17.76.2
irb.40              4 2             HPLGT   1d 07:05:55 10.17.128.2
irb.41              4 2             HPLGT   1d 07:05:55 10.17.132.2
irb.42              4 2             HPLGT   1d 07:05:55 10.17.136.2
irb.43              4 2             HPLGT   1d 07:05:55 10.17.140.2
irb.50              4 2             HPLGT   1d 07:05:55 10.18.0.2
irb.51              4 2             HPLGT   1d 07:05:55 10.18.16.2
irb.52              4 2             HPLGT   1d 07:05:55 10.18.32.2
irb.53              4 2             HPLGT   1d 07:05:55 10.18.48.2
irb.60              4 2             HPLGT   1d 07:05:55 10.32.0.2
irb.61              4 2             HPLGT   1d 07:05:55 10.32.16.2
irb.62              4 2             HPLGT   1d 07:05:55 10.32.32.2
irb.63              4 2             HPLGT   1d 07:05:55 10.32.48.2
irb.70              4 2             HPLGT   1d 07:05:55 10.33.0.2
irb.71              4 2             HPLGT   1d 07:05:55 10.33.16.2
irb.72              4 2             HPLGT   1d 07:05:55 10.33.32.2
irb.73              4 2             HPLGT   1d 07:05:55 10.33.48.2
irb.80              4 2             HPLGT   1d 07:05:55 10.34.0.2
irb.81              4 2             HPLGT   1d 07:05:55 10.34.16.2
irb.82              4 2             HPLGT   1d 07:05:55 10.34.32.2
irb.83              4 2             HPLGT   1d 07:05:55 10.34.48.2
irb.90              4 2             HPLGT   1d 07:05:55 10.35.0.2
irb.91              4 2             HPLGT   1d 07:05:55 10.35.16.2
irb.92              4 2             HPLGT   1d 07:05:55 10.35.32.2
irb.93              4 2             HPLGT   1d 07:05:55 10.35.48.2
xe-0/1/0.0          4 2             HPLGT   1d 07:05:55 172.16.32.14
```

```
root@cs-core-sw01# run show pim interfaces
Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name               Stat Mode IP V State        NbrCnt JoinCnt(sg/*g) DR address
ae0.0               Up   S     4 2 NotDR,NotCap        1 0/0
172.16.32.10
ae10.0              Up   S     4 2 NotDR,NotCap        1 0/0
172.16.32.58
irb.10             Up   S     4 2 DR,NotCap          1 0/0           10.16.0.3
irb.100            Up   S     4 2 DR,NotCap          1 0/0           10.36.0.3
irb.101            Up   S     4 2 DR,NotCap          1 0/0           10.36.16.3
irb.102            Up   S     4 2 DR,NotCap          1 0/0           10.36.32.3
irb.103            Up   S     4 2 DR,NotCap          1 0/0           10.36.48.3
irb.11             Up   S     4 2 DR,NotCap          1 0/0           10.16.16.3
irb.12             Up   S     4 2 DR,NotCap          1 0/0           10.16.32.3
irb.13             Up   S     4 2 DR,NotCap          1 0/0           10.16.48.3
irb.20             Up   S     4 2 DR,NotCap          1 0/0           10.17.0.3
irb.201             Up   S     4 2 DR,NotCap          1 0/0
172.16.128.3
irb.21             Up   S     4 2 DR,NotCap          1 0/0           10.17.4.3
irb.22             Up   S     4 2 DR,NotCap          1 0/0           10.17.8.3
irb.23             Up   S     4 2 DR,NotCap          1 0/0           10.17.12.3
irb.30             Up   S     4 2 DR,NotCap          1 0/0           10.17.64.3
irb.31             Up   S     4 2 DR,NotCap          1 0/0           10.17.68.3
irb.32             Up   S     4 2 DR,NotCap          1 0/0           10.17.72.3
irb.33             Up   S     4 2 DR,NotCap          1 0/0           10.17.76.3
irb.40              Up   S     4 2 DR,NotCap          1 0/0
10.17.128.3
irb.41              Up   S     4 2 DR,NotCap          1 0/0
```

```
10.17.132.3
irb.42              Up   S     4 2 DR,NotCap           1 0/0
10.17.136.3
irb.43              Up   S     4 2 DR,NotCap           1 0/0
10.17.140.3
irb.50             Up   S     4 2 DR,NotCap           1 0/0            10.18.0.3
irb.51             Up   S     4 2 DR,NotCap           1 0/0            10.18.16.3
irb.52             Up   S     4 2 DR,NotCap           1 0/0            10.18.32.3
irb.53             Up   S     4 2 DR,NotCap           1 0/0            10.18.48.3
irb.60             Up   S     4 2 DR,NotCap           1 0/0            10.32.0.3
irb.61             Up   S     4 2 DR,NotCap           1 0/0            10.32.16.3
irb.62             Up   S     4 2 DR,NotCap           1 0/0            10.32.32.3
irb.63             Up   S     4 2 DR,NotCap           1 0/0            10.32.48.3
irb.70             Up   S     4 2 DR,NotCap           1 0/0            10.33.0.3
irb.71             Up   S     4 2 DR,NotCap           1 0/0            10.33.16.3
irb.72             Up   S     4 2 DR,NotCap           1 0/0            10.33.32.3
irb.73             Up   S     4 2 DR,NotCap           1 0/0            10.33.48.3
irb.80             Up   S     4 2 DR,NotCap           1 0/0            10.34.0.3
irb.81             Up   S     4 2 DR,NotCap           1 0/0            10.34.16.3
irb.82             Up   S     4 2 DR,NotCap           1 0/0            10.34.32.3
irb.83             Up   S     4 2 DR,NotCap           1 0/0            10.34.48.3
irb.90             Up   S     4 2 DR,NotCap           1 0/0            10.35.0.3
irb.91             Up   S     4 2 DR,NotCap           1 0/0            10.35.16.3
irb.92             Up   S     4 2 DR,NotCap           1 0/0            10.35.32.3
irb.93             Up   S     4 2 DR,NotCap           1 0/0            10.35.48.3
lo0.0              Up   S     4 2 DR,NotCap           0 0/0
172.16.32.5
pd-0/0/0.32769     Up   S     4 2   P2P,NotCap        0 0/0
pe-1/0/0.32770     Up   S     4 2   P2P,NotCap        0 0/0
xe-0/1/0.0         Up   S     4 2 NotDR,NotCap        1 0/0
172.16.32.14
```

```
root@cs-core-sw01# run show pim join
 Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 230.1.1.1
    Source: *
    RP: 172.16.32.5
    Flags: sparse,rptree,wildcard
    Upstream interface: Local

Group: 230.1.1.1
    Source: 172.16.34.10
    Flags: sparse,spt
    Upstream interface: ae10.0

Group: 230.1.1.2
    Source: *
    RP: 172.16.32.5
    Flags: sparse,rptree,wildcard
    Upstream interface: Local

Group: 230.1.1.2
    Source: 172.16.34.10
    Flags: sparse,spt
    Upstream interface: ae10.0

Group: 230.1.1.3
    Source: *
    RP: 172.16.32.5
    Flags: sparse,rptree,wildcard
```

```
    Upstream interface: Local

Group: 230.1.1.3
    Source: 172.16.34.10
    Flags: sparse,spt
    Upstream interface: ae10.0

Group: 230.1.1.4
    Source: *
    RP: 172.16.32.5
    Flags: sparse,rptree,wildcard
    Upstream interface: Local

Group: 230.1.1.4
    Source: 172.16.34.10
    Flags: sparse,spt
    Upstream interface: ae10.0

Group: 230.1.1.5
    Source: *
    RP: 172.16.32.5
    Flags: sparse,rptree,wildcard
    Upstream interface: Local

Group: 230.1.1.5
    Source: 172.16.34.10
    Flags: sparse,spt
    Upstream interface: ae10.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

- Verify PIM rendezvous points on the core devices.

```
root@cs-core-sw01# run show pim rps
Instance: PIM.master

address-family INET
RP address      Type        Mode   Holdtime Timeout Groups Group prefixes
172.16.32.5     bootstrap   sparse      150    None      5 224.0.0.0/4
172.16.32.6     bootstrap   sparse      150      98      0 224.0.0.0/4
172.16.32.5     static      sparse      150    None      5 224.0.0.0/4

address-family INET6
```

- Verify IGMP interfaces, IGMP groups, and IGMP snooping on the core devices.

```
root@cs-core-sw01# run show igmp interface
Interface: irb.52
    Querier: 10.18.32.2
    State:         Up Timeout:       4 Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: xe-0/1/0.0
    Querier: 172.16.32.13
    State:         Up Timeout:    None Version:  2 Groups:      5
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: irb.70
    Querier: 10.33.0.2
```

```
    State:         Up Timeout:       5 Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: irb.82
    Querier: 10.34.32.2
    State:         Up Timeout:       5 Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
Interface: irb.11
    Querier: 10.16.16.2
    State:         Up Timeout:       6 Version:  2 Groups:      0
    Immediate leave: Off
    Promiscuous mode: Off
    Passive: Off
```

```
root@cs-core-sw01# run show igmp group
Interface: ae0.0, Groups: 5
    Group: 224.0.0.2
        Source: 0.0.0.0
        Last reported by: 172.16.32.10
        Timeout:       7 Type: Dynamic
    Group: 224.0.0.5
        Source: 0.0.0.0
        Last reported by: 172.16.32.10
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.6
        Source: 0.0.0.0
        Last reported by: 172.16.32.10
        Timeout:       7 Type: Dynamic
    Group: 224.0.0.13
        Source: 0.0.0.0
        Last reported by: 172.16.32.10
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.22
        Source: 0.0.0.0
        Last reported by: 172.16.32.10
        Timeout:       5 Type: Dynamic
Interface: irb.20, Groups: 5
    Group: 230.1.1.1
        Source: 0.0.0.0
        Last reported by: 10.17.0.51
        Timeout:       3 Type: Dynamic
    Group: 230.1.1.2
        Source: 0.0.0.0
        Last reported by: 10.17.0.52
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.3
        Source: 0.0.0.0
        Last reported by: 10.17.0.52
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.4
        Source: 0.0.0.0
        Last reported by: 10.17.0.51
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.5
        Source: 0.0.0.0
        Last reported by: 10.17.0.51
        Timeout:       7 Type: Dynamic
Interface: irb.10, Groups: 5
    Group: 230.1.1.1
```

```
            Source: 0.0.0.0
            Last reported by: 10.16.0.53
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.2
            Source: 0.0.0.0
            Last reported by: 10.16.0.51
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.3
            Source: 0.0.0.0
            Last reported by: 10.16.0.53
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.4
            Source: 0.0.0.0
            Last reported by: 10.16.0.53
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.5
            Source: 0.0.0.0
            Last reported by: 10.16.0.51
            Timeout:       7 Type: Dynamic
    Interface: irb.60, Groups: 5
        Group: 230.1.1.1
            Source: 0.0.0.0
            Last reported by: 10.32.0.53
            Timeout:       6 Type: Dynamic
        Group: 230.1.1.2
            Source: 0.0.0.0
            Last reported by: 10.32.0.52
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.3
            Source: 0.0.0.0
            Last reported by: 10.32.0.57
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.4
            Source: 0.0.0.0
            Last reported by: 10.32.0.57
            Timeout:       7 Type: Dynamic
        Group: 230.1.1.5
            Source: 0.0.0.0
            Last reported by: 10.32.0.56
            Timeout:       7 Type: Dynamic
    Interface: irb.50, Groups: 5
        Group: 230.1.1.1
            Source: 0.0.0.0
            Last reported by: 10.18.0.51
            Timeout:       6 Type: Dynamic
        Group: 230.1.1.2
            Source: 0.0.0.0
            Last reported by: 10.18.0.52
            Timeout:       5 Type: Dynamic
        Group: 230.1.1.3
            Source: 0.0.0.0
            Last reported by: 10.18.0.52
            Timeout:       5 Type: Dynamic
        Group: 230.1.1.4
            Source: 0.0.0.0
            Last reported by: 10.18.0.51
            Timeout:       6 Type: Dynamic
        Group: 230.1.1.5
            Source: 0.0.0.0
            Last reported by: 10.18.0.51
            Timeout:       5 Type: Dynamic
```

```
Interface: xe-0/1/0.0, Groups: 5
    Group: 224.0.0.2
        Source: 0.0.0.0
        Last reported by: 172.16.32.14
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.5
        Source: 0.0.0.0
        Last reported by: 172.16.32.14
        Timeout:       7 Type: Dynamic
    Group: 224.0.0.6
        Source: 0.0.0.0
        Last reported by: 172.16.32.14
        Timeout:       5 Type: Dynamic
    Group: 224.0.0.13
        Source: 0.0.0.0
        Last reported by: 172.16.32.14
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.22
        Source: 0.0.0.0
        Last reported by: 172.16.32.14
        Timeout:       5 Type: Dynamic
Interface: irb.30, Groups: 5
    Group: 230.1.1.1
        Source: 0.0.0.0
        Last reported by: 10.17.64.51
        Timeout:       4 Type: Dynamic
    Group: 230.1.1.2
        Source: 0.0.0.0
        Last reported by: 10.17.64.51
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.3
        Source: 0.0.0.0
        Last reported by: 10.17.64.51
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.4
        Source: 0.0.0.0
        Last reported by: 10.17.64.51
        Timeout:       7 Type: Dynamic
    Group: 230.1.1.5
        Source: 0.0.0.0
        Last reported by: 10.17.64.51
        Timeout:       7 Type: Dynamic
Interface: ae10.0, Groups: 5
    Group: 224.0.0.2
        Source: 0.0.0.0
        Last reported by: 172.16.32.58
        Timeout:       5 Type: Dynamic
    Group: 224.0.0.5
        Source: 0.0.0.0
        Last reported by: 172.16.32.58
        Timeout:       5 Type: Dynamic
    Group: 224.0.0.6
        Source: 0.0.0.0
        Last reported by: 172.16.32.58
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.13
        Source: 0.0.0.0
        Last reported by: 172.16.32.58
        Timeout:       6 Type: Dynamic
    Group: 224.0.0.22
        Source: 0.0.0.0
```

```
        Last reported by: 172.16.32.58
        Timeout:       6 Type: Dynamic
Interface: local, Groups: 6
    Group: 224.0.0.2
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
    Group: 224.0.0.5
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
    Group: 224.0.0.6
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
    Group: 224.0.0.13
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
    Group: 224.0.0.18
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
    Group: 224.0.0.22
        Source: 0.0.0.0
        Last reported by: Local
        Timeout:       0 Type: Dynamic
```

```
root@cs-core-sw01# run show igmp snooping membership
Instance: default-switch

Vlan: eng1_data_wired

Learning-Domain: default
Interface: ae1.0, Groups: 5
    Group: 230.1.1.1
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.54
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.2
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.51
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.3
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.53
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.4
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.54
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.5
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.52
        Group timeout:     259 Type: Dynamic
Interface: ae2.0, Groups: 0
Interface: ae3.0, Groups: 5
```

```
    Group: 230.1.1.1
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.55
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.2
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.55
        Group timeout:     258 Type: Dynamic
    Group: 230.1.1.3
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.55
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.4
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.55
        Group timeout:     259 Type: Dynamic
    Group: 230.1.1.5
        Group mode: Exclude
        Source: 0.0.0.0
        Last reported by: 10.32.0.55
        Group timeout:     259 Type: Dynamic
Interface: ae7.0, Groups: 0
Interface: ae13.0, Groups: 0
```

Meaning Confirm that multicast has been properly configured and is now enabled on all devices.

Related Documentation

- Understanding the Benefits of the Midsize Enterprise Campus Solution on page 6
- Example: Configuring High Availability for the Midsize Enterprise Campus on page 39
- Example: Configuring Access Policy and Security for the Midsize Enterprise Campus on page 114
- Example: Configuring Class of Service for the Midsize Enterprise Campus on page 137

Example: Configuring Access Policy and Security for the Midsize Enterprise Campus

Requirements

Table 19 on page 115 shows the hardware and software requirements for this example.Table 20 on page 115 shows the scaling and performance targets used for this example.

Table 19: Hardware and Software Requirements

Hardware	Device Name	Software
MX240	cs-edge-r01, cs-edge-r02	13.2 R2.4
SRX650	cs-edge-fw-01, cs-edge-fw02	12.1 X44-D39.4
EX9214	cs-core-sw01, cs-core-sw02	13.2 R3.7
EX4550	cs-agg-01	12.3 R3.4
EX2200	cs-2200-ab5	12.3 R3.4
EX3300	cs-3300-ab4	12.3 R3.4
EX4200	cs-4200-ab1	12.3 R3.4
EX4300	cs-4300-ab2, cs-4300-ab3	13.2 X51-D21.1

Table 20: Node Features and Performance/Scalability

Node	Features	Performance/Scalability Target Value
Edge (MX240, SRX650)	MC-LAG, OSPF, BGP, IRB	3k IPv4
Core (EX9214)	VLANs, MC-LAG, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, IRB	3k IPv4 routes 128k MAC table entries 16k ARP entries
Aggregation (EX4550)	VLANs, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, RVI	3k IPv4 routes 5 IGMP groups
Access (EX3300, EX4300, EX4200)	VLANs, LAG, 802.1X, IGMP snooping, DHCP snooping, ARP inspection, IP source guard	55k MAC table entries 13k 8021.x users 5 IGMP groups

The configuration details that follow assume that:

- All physical cabling necessary has been completed.
- All basic logical interfaces have been configured.
- All devices have loopback interfaces configured.

Overview

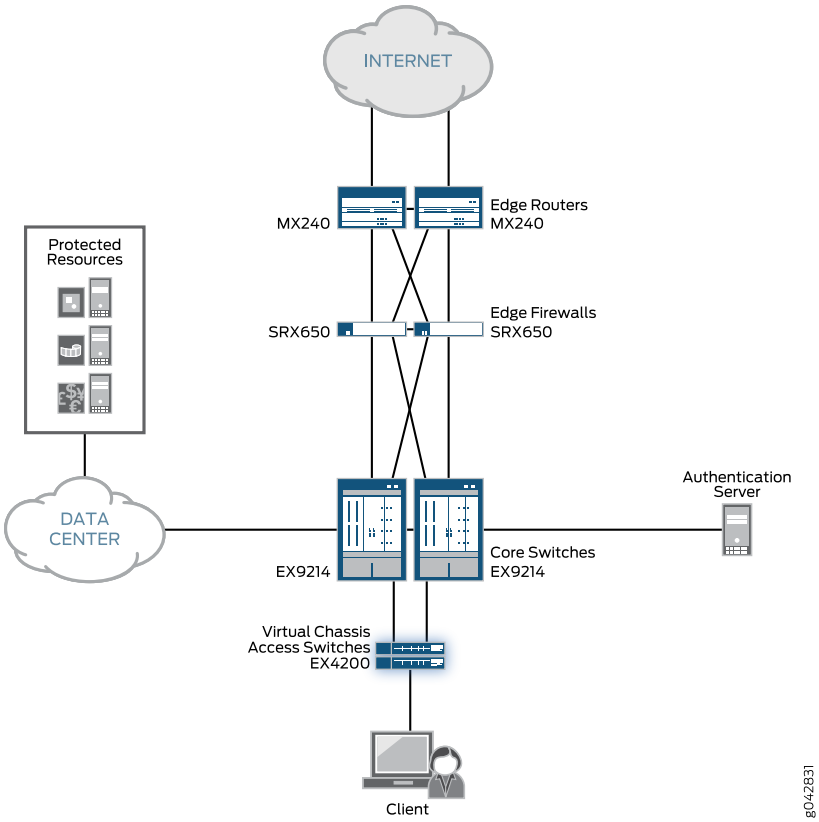
This example covers access policy and security for the midsize enterprise campus solution. This includes the complete configuration for 802.1X policy and access, as well as firewall

provisioning for Juniper Networks devices. This configuration was tested with active LAN, RADIUS server, and supplicant environment.

Topology

Figure 13 on page 116 shows the topology used in the example configuration.

Figure 13: Access Security and Policy Topology



Configuration

To configure access policy and security, follow these procedures:

- Configuring Access Port Security for the Midsize Enterprise Campus on page 116
- Configuring 802.1X in the Midsize Enterprise Campus on page 118
- Configuring NAT Security for the Midsize Enterprise Campus on page 127
- Configuring the Firewall Zones on page 128

Configuring Access Port Security for the Midsize Enterprise Campus

Step-by-Step Procedure

To configure access port security:

1. Enable ARP inspection and DHCP snooping.

- To enable ARP inspection on access devices that are EX4200, EX3300, and EX2200 switches:

```
[edit]
user@host# set ethernet-switching-options secure-access-port vlan all
  arp-inspection
user@host# set ethernet-switching-options secure-access-port vlan
  eng1_voice_wired arp-inspection
```

- To enable DHCP snooping on access devices that are EX4200, EX3300, and EX2200 switches:

```
[edit]
user@host# set ethernet-switching-options secure-access-port vlan all
  examine-dhcp
user@host# set ethernet-switching-options secure-access-port vlan
  eng1_voice_wired examine-dhcp
```

- To enable ARP inspection and DHCP snooping on access devices that are EX4300 switches:

```
[edit]
user@host# set vlans eng1_data_wired forwarding-options dhcp-security
  arp-inspection
```

2. Enable IP source guard.

   Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

```
[edit]
user@host# set ethernet-switching-options secure-access-port vlan all
  ip-source-guard
```

NOTE: IP Source Guard was disabled in the configuration for the EX4300 switches. This is a known hardware issue. *PR 1001232 - Enabling IPsource guard on the data vlans impact the traffic on the voice vlan*.

Configuring 802.1X in the Midsize Enterprise Campus

Step-by-Step Procedure

To configure 802.1X:

1. On access devices, create the access policy for wired endpoints that will use RADIUS authentication and authorization as a condition of access to the network.

   The RADIUS profile here is named MY-RADIUS-profile.

   - Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

     ```
     [edit]
     user@host# set access radius-server 172.16.4.205 secret
       "$9$TF6ABIcvWxp0WxNdg4QFn"
     user@host# set access radius-server 172.16.4.205 timeout 90Tune timer for your
       environment
     user@host# set access radius-server 172.16.4.205 source-address 172.16.35.68
     user@host# set access profile MY-RADIUS-profile authentication-order radius
     user@host# set access profile MY-RADIUS-profile radius authentication-server
       172.16.4.205
     user@host# set access profile MY-RADIUS-profile radius accounting-server
       172.16.4.205
     user@host# set access profile MY-RADIUS-profile accounting order radius
     user@host# set access profile MY-RADIUS-profile accounting
       accounting-stop-on-failure
     user@host# set access profile MY-RADIUS-profile accounting
       accounting-stop-on-access-deny
     ```

   - Configuration on access devices that are EX4300 switches is as follows:

     ```
     [edit]
     user@host# set access radius-server 172.16.4.205 secret
       "$9$LO47dsaZjP5F245Fn/0OX7-"
     user@host# set access radius-server 172.16.4.205 timeout 90
     user@host# set access radius-server 172.16.4.205 source-address 172.16.35.69
     user@host# set access profile MY-RADIUS-profile authentication-order radius
     user@host# set access profile MY-RADIUS-profile radius authentication-server
       172.16.4.205
     user@host# set access profile MY-RADIUS-profile radius accounting-server
       172.16.4.205
     user@host# set access profile MY-RADIUS-profile accounting order radius
     user@host# set access profile MY-RADIUS-profile accounting
       accounting-stop-on-failure
     user@host# set access profile MY-RADIUS-profile accounting
       accounting-stop-on-access-deny
     ```

   NOTE: You can adjust the RADIUS timer to timeout according to your network by configuring set access radius-server <$ip-address$> timeout <$value$> to your preference.

2. Configure the 802.1X authenticator interface that is connected to the RADIUS server on the access device.

- Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

```
[edit]
user@host# set protocols dot1x authenticator authentication-profile-name
  MY-RADIUS-profile
user@host# set protocols dot1x authenticator no-mac-table-binding
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 supplicant
  multiple
user@host# set protocols dot1x authenticator interface ge-0/0/0.0
  supplicant-timeout 60Tune timer for your environment
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 guest-vlan
  guest
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 server-fail
  use-cache
```

- Configuration on access devices that are EX4300 switches is as follows:

```
[edit]
user@host# set protocols dot1x authenticator authentication-profile-name
  MY-RADIUS-profile
user@host# set protocols dot1x authenticator no-mac-table-binding
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 supplicant
  multiple
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant-timeout 60
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 guest-vlan
  guest
user@host# set protocols dot1x authenticator interface ge-0/0/0.0 server-fail
  use-cache
```

NOTE: You can adjust the supplicant timer to timeout according to your network by configuring set protocols dot1x authenticator interface <int_name> supplicant-timeout <$value$>to your preference.

3. Configure MAC authentication with 802.1X.

- Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

```
[edit]
user@host# set protocols dot1x authenticator interface ge-5/0/42.0 supplicant
  multiple
user@host# set protocols dot1x authenticator interface ge-5/0/42.0 mac-radius
user@host# set protocols dot1x authenticator interface ge-5/0/42.0
  supplicant-timeout 3
user@host# set protocols dot1x authenticator interface ge-5/0/42.0 guest-vlan
  guest
user@host# set protocols dot1x authenticator interface ge-5/0/42.0 server-fail
  use-cache
```

- Configuration on access devices that are EX4300 switches is as follows:

```
[edit]
```

```
user@host# set protocols dot1x authenticator interface ge-2/0/42.0 supplicant
  multiple
user@host# set protocols dot1x authenticator interface ge-2/0/42.0 mac-radius
user@host# set protocols dot1x authenticator interface ge-2/0/42.0
  supplicant-timeout 3
user@host# set protocols dot1x authenticator interface ge-2/0/42.0 guest-vlan
  guest
user@host# set protocols dot1x authenticator interface ge-2/0/42.0 server-fail
  use-cache
```

You can either configure MAC RADIUS authentication on an interface that also has 802.1X authentication configured, or you can configure either authentication method alone. If both MAC RADIUS and 802.1X authentication are enabled on the same interface, the switch first sends three EAPOL requests to the host. If there is no response from the host, the switch sends the host MAC address to the RADIUS server to determine if it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the host on the interface to which it is connected.

If MAC RADIUS authentication only is configured on the interface (by using the **mac-radius restrict** option only), the switch attempts to authenticate the MAC address with the RADIUS server directly without delay.

4. Configure firewall filters for each group profile.

   This configuration assumes that the RADIUS server has the coordinating group policy.

   - Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

     ```
     [edit]
     user@host# set firewall family ethernet-switching filter ENG term 1 from
       destination-address 172.16.32.70/32
     user@host# set firewall family ethernet-switching filter ENG term 1 then discard
     user@host# set firewall family ethernet-switching filter ENG term 2 from
       destination-address 172.16.32.78/32
     :
     :
     user@host# set firewall family ethernet-switching filter ENG term 10 then discard
     user@host# set firewall family ethernet-switching filter ENG term 11 then accept

     user@host# set firewall family ethernet-switching filter Finance term 1 from
       destination-address 172.16.32.66/32
     user@host# set firewall family ethernet-switching filter Finance term 1 then discard
     user@host# set firewall family ethernet-switching filter Finance term 2 from
       destination-address 172.16.32.74/32
     set firewall family ethernet-switching filter Finance term 2 then discard
     :
     :
     user@host# set firewall family ethernet-switching filter Finance term 10 then
       discard
     user@host# set firewall family ethernet-switching filter Finance term 11 then
       accept
     ```

```
user@host# set firewall family ethernet-switching filter Sales term 1 from
  destination-address 172.16.32.66/32
user@host# set firewall family ethernet-switching filter Sales term 1 then discard
user@host# set firewall family ethernet-switching filter Sales term 2 from
  destination-address 172.16.32.74/32
user@host# set firewall family ethernet-switching filter Sales term 2 then discard
:
:
user@host# set firewall family ethernet-switching filter Sales term 10 then discard
user@host# set firewall family ethernet-switching filter Sales term 11 then accept
```

- Configuration on access devices that are EX4300 switches is as follows:

```
[edit]
user@host# set firewall family ethernet-switching filter ENG term 1 from
  ip-destination-address 172.16.32.70/32
user@host# set firewall family ethernet-switching filter ENG term 1 then discard
user@host# set firewall family ethernet-switching filter ENG term 2 from
  ip-destination-address 172.16.32.78/32
user@host# set firewall family ethernet-switching filter ENG term 2 then discard
user@host# set firewall family ethernet-switching filter ENG term 3 from
  ip-destination-address 172.16.32.86/32
:
:
user@host# set firewall family ethernet-switching filter ENG term 9 from
  ip-destination-address 172.16.52.0/24
user@host# set firewall family ethernet-switching filter ENG term 9 then discard
user@host# set firewall family ethernet-switching filter ENG term 10 from
  ip-destination-address 172.16.53.0/24
user@host# set firewall family ethernet-switching filter ENG term 10 then discard
user@host# set firewall family ethernet-switching filter ENG term 11 then accept
user@host# set firewall family ethernet-switching filter Finance term 1 from
  ip-destination-address 172.16.32.66/32
user@host# set firewall family ethernet-switching filter Finance term 1 then discard
user@host# set firewall family ethernet-switching filter Finance term 2 from
  ip-destination-address 172.16.32.74/32
user@host# set firewall family ethernet-switching filter Finance term 2 then
  discard
user@host# set firewall family ethernet-switching filter Finance term 3 from
  ip-destination-address 172.16.32.82/32
user@host# set firewall family ethernet-switching filter Finance term 3 then
  discard
:
:
user@host# set firewall family ethernet-switching filter Finance term 10 from
  ip-destination-address 172.16.53.0/24
user@host# set firewall family ethernet-switching filter Finance term 10 then
  discard
user@host# set firewall family ethernet-switching filter Finance term 11 then
  accept
user@host# set firewall family ethernet-switching filter Sales term 1 from
  ip-destination-address 172.16.32.66/32
user@host# set firewall family ethernet-switching filter Sales term 1 then discard
user@host# set firewall family ethernet-switching filter Sales term 2 from
  ip-destination-address 172.16.32.74/32
user@host# set firewall family ethernet-switching filter Sales term 2 then discard
```

```
:
:
user@host# set firewall family ethernet-switching filter Sales term 9 from
  ip-destination-address 172.16.52.0/24
user@host# set firewall family ethernet-switching filter Sales term 9 then discard
user@host# set firewall family ethernet-switching filter Sales term 10 from
  ip-destination-address 172.16.53.0/24
user@host# set firewall family ethernet-switching filter Sales term 10 then discard
```

5. In some cases the client will not have an 802.1X supplicant, or there could be a supplicant that is non-responsive. For those scenarios, we have created a guest VLAN where the switch will assign the port to and filter access only to the RADIUS server and remediation server.

   Configure the guest VLAN.

   - Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

```
[edit]
user@host# set firewall family ethernet-switching filter Guest term 1 from
  destination-port dhcp
user@host# set firewall family ethernet-switching filter Guest term 1 then accept
user@host# set firewall family ethernet-switching filter Guest term 1 then count
  term1
user@host# set firewall family ethernet-switching filter Guest term 2 from
  ether-type arp
set firewall family ethernet-switching filter Guest term 2 then accept
user@host# set firewall family ethernet-switching filter Guest term 3 from
  destination-address 172.16.12.0/24
user@host# set firewall family ethernet-switching filter Guest term 3 then accept
user@host# set firewall family ethernet-switching filter Guest term 4 from
  destination-address 172.16.4.101/32
user@host# set firewall family ethernet-switching filter Guest term 4 from
  destination-port 53
user@host# set firewall family ethernet-switching filter Guest term 4 then accept
user@host# set firewall family ethernet-switching filter Guest term 4 then count
  term2
user@host# set firewall family ethernet-switching filter Guest term 5 from
  destination-address 172.16.4.102/32
user@host# set firewall family ethernet-switching filter Guest term 5 from
  destination-port 67user@host#
user@host# set firewall family ethernet-switching filter Guest term 5 then accept
user@host# set firewall family ethernet-switching filter Guest term 5 then count
  term3
user@host# set firewall family ethernet-switching filter Guest term 6 from
  destination-address 172.16.4.205/32
user@host# set firewall family ethernet-switching filter Guest term 6 then accept
user@host# set firewall family ethernet-switching filter Guest term 6 then count
  term4
user@host# set firewall family ethernet-switching filter Guest term 7 from
  destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Guest term 7 from
  destination-port 443
user@host# set firewall family ethernet-switching filter Guest term 7 then accept
```

```
user@host# set firewall family ethernet-switching filter Guest term 7 then count
  term7
user@host# set firewall family ethernet-switching filter Guest term 8 from
  destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Guest term 8 from
  destination-port 80
user@host# set firewall family ethernet-switching filter Guest term 8 then accept
user@host# set firewall family ethernet-switching filter Guest term 8 then count
  term8
user@host# set firewall family ethernet-switching filter Guest term 9 from
  destination-mac-address 1:80:c2:00:00:03/48
user@host# set firewall family ethernet-switching filter Guest term 9 then accept
user@host# set firewall family ethernet-switching filter Guest term 10 then discard
user@host# set firewall family ethernet-switching filter Guest term 10 then count
  term9
```

- Configuration on access devices that are EX4300 switches is as follows:

```
[edit]
set firewall family ethernet-switching filter Guest term 1 from destination-port
  dhcp
set firewall family ethernet-switching filter Guest term 1 then accept
set firewall family ethernet-switching filter Guest term 1 then count term1
set firewall family ethernet-switching filter Guest term 2 from ether-type arp
set firewall family ethernet-switching filter Guest term 2 then accept
set firewall family ethernet-switching filter Guest term 3 from
  ip-destination-address 172.16.12.0/24
set firewall family ethernet-switching filter Guest term 3 then accept
set firewall family ethernet-switching filter Guest term 4 from destination-port
  53
set firewall family ethernet-switching filter Guest term 4 from
  ip-destination-address 172.16.4.101/32
set firewall family ethernet-switching filter Guest term 4 then accept
set firewall family ethernet-switching filter Guest term 4 then count term2
set firewall family ethernet-switching filter Guest term 5 from destination-port
  67
set firewall family ethernet-switching filter Guest term 5 from
  ip-destination-address 172.16.4.102/32
set firewall family ethernet-switching filter Guest term 5 then accept
set firewall family ethernet-switching filter Guest term 5 then count term3
set firewall family ethernet-switching filter Guest term 6 from
  ip-destination-address 172.16.4.205/32
set firewall family ethernet-switching filter Guest term 6 then accept
set firewall family ethernet-switching filter Guest term 6 then count term4
set firewall family ethernet-switching filter Guest term 7 from destination-port
  80
set firewall family ethernet-switching filter Guest term 7 from
  ip-destination-address 172.16.10.100/32
set firewall family ethernet-switching filter Guest term 7 then accept
set firewall family ethernet-switching filter Guest term 7 then count term7
set firewall family ethernet-switching filter Guest term 8 from destination-port
  443
set firewall family ethernet-switching filter Guest term 8 from
  ip-destination-address 172.16.10.100/32
set firewall family ethernet-switching filter Guest term 8 then accept
set firewall family ethernet-switching filter Guest term 8 then count term8
```

```
set firewall family ethernet-switching filter Guest term 9 from
    destination-mac-address 01:80:c2:00:00:03/48
set firewall family ethernet-switching filter Guest term 9 then accept
set firewall family ethernet-switching filter Guest term 10 then discard
set firewall family ethernet-switching filter Guest term 10 then count term9
```

NOTE: In this example, guest access does not mean that the user will be granted minimum access to the Internet and other resources.

6. Include a filter for remediation if a remediation service available.

   The following configuration assumes that a VLAN for remediation has already been configured.

   - Configuration on access devices that are EX4200, EX3300, and EX2200 switches is as follows:

```
[edit]
user@host# set firewall family ethernet-switching filter Remediation term 1 from
    destination-port dhcp
user@host# set firewall family ethernet-switching filter Remediation term 1 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 1 then
    count term1
user@host# set firewall family ethernet-switching filter Remediation term 2 from
    ether-type arp
user@host# set firewall family ethernet-switching filter Remediation term 2 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 2 then
    count term2
user@host# set firewall family ethernet-switching filter Remediation term 3 from
    destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Remediation term 3 from
    destination-port 80
user@host# set firewall family ethernet-switching filter Remediation term 3 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 3 then
    count term3
user@host# set firewall family ethernet-switching filter Remediation term 4 from
    destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Remediation term 4 from
    destination-port 443
user@host# set firewall family ethernet-switching filter Remediation term 4 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 4 then
    count term4
user@host# set firewall family ethernet-switching filter Remediation term 5 from
    destination-address 172.16.4.101/32
user@host# set firewall family ethernet-switching filter Remediation term 5 from
    destination-port 53
user@host# set firewall family ethernet-switching filter Remediation term 5 then
    accept
```

```
user@host# set firewall family ethernet-switching filter Remediation term 5 then
  count term5
user@host# set firewall family ethernet-switching filter Remediation term 6 from
  destination-address 172.16.4.102/32
user@host# set firewall family ethernet-switching filter Remediation term 6 from
  destination-port 67
user@host# set firewall family ethernet-switching filter Remediation term 6 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 6 then
  count term6
user@host# set firewall family ethernet-switching filter Remediation term 7 from
  destination-address 172.16.4.205/32
user@host# set firewall family ethernet-switching filter Remediation term 7 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 7 then
  count term7
user@host# set firewall family ethernet-switching filter Remediation term 8 from
  destination-mac-address 01:80:c2:00:00:03/48
user@host# set firewall family ethernet-switching filter Remediation term 8 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 9 then
  discard
user@host# set firewall family ethernet-switching filter Remediation term 9 then
  count term9
```

- Configuration on access devices that are EX4300 switches is as follows:

```
user@host# set firewall family ethernet-switching filter Remediation term 1 from
  destination-port dhcp
user@host# set firewall family ethernet-switching filter Remediation term 1 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 1 then
  count term1
user@host# set firewall family ethernet-switching filter Remediation term 2 from
  ether-type arp
user@host# set firewall family ethernet-switching filter Remediation term 2 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 2 then
  count term2
user@host# set firewall family ethernet-switching filter Remediation term 3 from
  destination-port 80
user@host# set firewall family ethernet-switching filter Remediation term 3 from
  ip-destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Remediation term 3 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 3 then
  count term3
user@host# set firewall family ethernet-switching filter Remediation term 4 from
  destination-port 443
user@host# set firewall family ethernet-switching filter Remediation term 4 from
  ip-destination-address 172.16.10.100/32
user@host# set firewall family ethernet-switching filter Remediation term 4 then
  accept
user@host# set firewall family ethernet-switching filter Remediation term 4 then
  count term4
```

```
user@host# set firewall family ethernet-switching filter Remediation term 5 from
    destination-port 53
user@host# set firewall family ethernet-switching filter Remediation term 5 from
    ip-destination-address 172.16.4.101/32
user@host# set firewall family ethernet-switching filter Remediation term 5 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 5 then
    count term5
user@host# set firewall family ethernet-switching filter Remediation term 6 from
    destination-port 67
user@host# set firewall family ethernet-switching filter Remediation term 6 from
    ip-destination-address 172.16.4.102/32
user@host# set firewall family ethernet-switching filter Remediation term 6 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 6 then
    count term6
user@host# set firewall family ethernet-switching filter Remediation term 7 from
    ip-destination-address 172.16.4.205/32
user@host# set firewall family ethernet-switching filter Remediation term 7 then
    accept
user@host# set firewall family ethernet-switching filter Remediation term 7 then
    count term7
user@host# set firewall family ethernet-switching filter Guest term 9 from
    destination-mac-address 01:80:c2:00:00:03/48
user@host# set firewall family ethernet-switching filter Guest term 9 then accept
user@host# set firewall family ethernet-switching filter Remediation term 9 then
    discard
user@host# set firewall family ethernet-switching filter Remediation term 9 then
    count term9
```

Configuring NAT Security for the Midsize Enterprise Campus

Step-by-Step Procedure

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either the source or destination address, or both addresses, in a network packet can be translated. NAT can include the translation of port numbers in addition to IP addresses.

In this example, we used source and destination NAT:

- Source NAT is the translation of the source IP address of a packet leaving the device. Source NAT is used to allow hosts with private IP addresses to access a public network. In this example, we have defined the translation of the original source IP address to an IP address from a user-defined address pool with port address translation. The association between the original source IP address to the translated source IP address is dynamic. Proxy ARP is also configured on the device. This allows the security device to respond to ARP requests received on the interface for a translated address.
- Destination NAT is the translation of the destination IP address of a packet entering the device. Destination NAT is used to redirect traffic destined to a virtual host (identified by the original destination IP address) to the real host (identified by the translated destination IP address). When destination NAT is performed, the destination IP address is translated according to configured destination NAT rules first and then security policies are applied after translation. Remote access connections also use destination NAT. Proxy ARP is also configured on the device. This allows the security device to respond to ARP requests received on the interface for a translated address.

  In this example, NAT security was configured on the SRX650 firewall device.

  To configure NAT security:

1. Configure source NAT interface on the security device.

```
[edit]
user@host# set security nat source pool Source-NAT6 address 10.92.84.65/32 to
  10.92.84.80/32
user@host# set security nat source rule-set SNAT1 from zone trust
user@host# set security nat source rule-set SNAT1 to zone untrust
user@host# set security nat source rule-set SNAT1 rule Ru7 match source-address
  172.16.4.0/24
user@host# set security nat source rule-set SNAT1 rule Ru7 match source-address
  10.0.0.0/8
user@host# set security nat source rule-set SNAT1 rule Ru7 match
  destination-address 0.0.0.0/0
user@host# set security nat source rule-set SNAT1 rule Ru7 then source-nat pool
  Source-NAT6
```

2. Configure proxy ARP for source NAT.

```
[edit]
user@host# set security nat proxy-arp interface reth1.0 address 10.92.84.60/32 to
  10.92.84.80/32
```

3. Configure destination NAT on the security device.

```
[edit]
user@host# set security nat destination pool SA address 172.16.7.103/32
```

```
user@host# set security nat destination rule-set SA-rule from zone untrust
user@host# set security nat destination rule-set SA-rule rule rs1 match
  source-address 0.0.0.0/0
user@host# set security nat destination rule-set SA-rule rule rs1 match
  destination-address 10.92.84.50/32
user@host# set security nat destination rule-set SA-rule rule rs1 then destination-nat
  pool SA
```

4. Configure proxy ARP for the destination NAT interface.

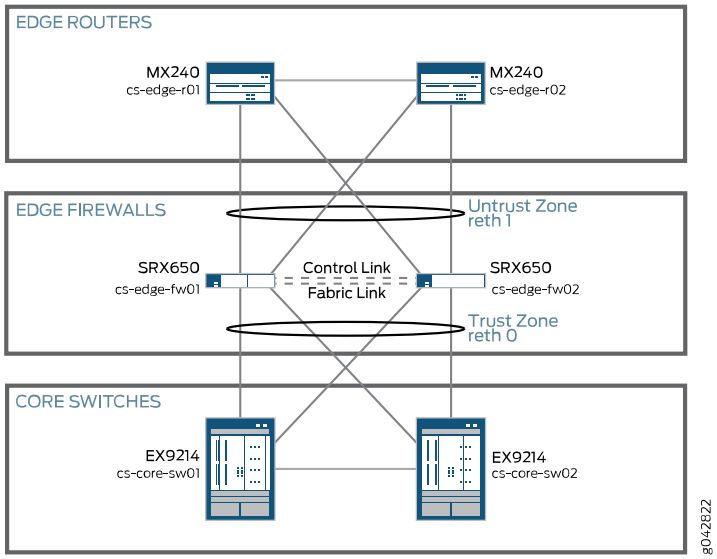
```
[edit]
user@host# set security nat proxy-arp interface reth1.0 address 10.92.84.50/32
```

Configuring the Firewall Zones

Step-by-Step Procedure

The midsize enterprise campus security gateway is configured with two zones, for trusted and untrusted traffic. This example configuration follows the topology shown in Figure 14 on page 128.

Figure 14: Security Firewall Zone Topology



To configure the firewall zones:

1. Set reth interfaces to the appropriate zones and virtual routers.

```
[edit]
user@host# set security zones security-zone untrust interfaces reth1.0
user@host# set security zones security-zone trust interfaces reth0.0
```

2. Configure security zones and address books.

   The reth0 and reth1 interfaces were left in the default virtual router inet.0.

```
[edit]
user@host# set security zones security-zone trust address-book address sales
  10.16.0.0/20
```

```
user@host# set security zones security-zone trust address-book address SA-Address
  172.16.7.103/32
user@host# set security zones security-zone trust host-inbound-traffic
  system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols
  all
user@host# set security zones security-zone trust interfaces reth0.0
user@host# set security zones security-zone untrust interfaces reth1.0
  host-inbound-traffic system-services all
user@host# set security zones security-zone untrust interfaces reth1.0
  host-inbound-traffic protocols all
```

3. Configure security policies for traffic coming from the trust zone (reth0) to the untrust zone (reth1).

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match source-address any
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-http
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-https
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-dns-udp
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-dns-tcp
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-ntp
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  match application junos-icmp-ping
user@host# set security policies from-zone trust to-zone untrust policy trust-untrust
  then permit
```

4. Configure security policies for traffic coming from the untrust zone (reth1) to the trust zone (reth0).

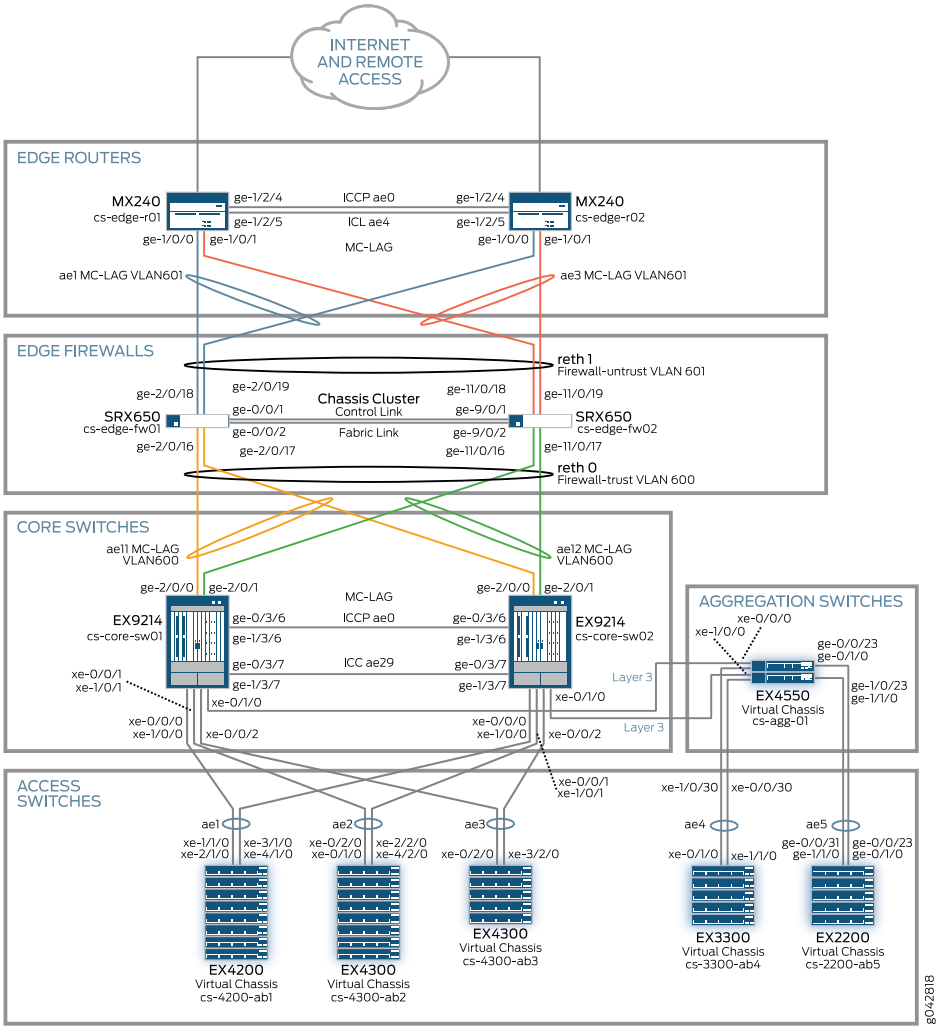
```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy Remote-SA
  match source-address any
user@host# set security policies from-zone untrust to-zone trust policy Remote-SA
  match destination-address SA-Address
user@host# set security policies from-zone untrust to-zone trust policy Remote-SA
  match application junos-https
user@host# set security policies from-zone untrust to-zone trust policy Remote-SA
  match application junos-http
user@host# set security policies from-zone untrust to-zone trust policy Remote-SA
  then permit
user@host# set security policies from-zone untrust to-zone trust policy untrust-trust
  match source-address any
user@host# set security policies from-zone untrust to-zone trust policy untrust-trust
  match destination-address any
user@host# set security policies from-zone untrust to-zone trust policy untrust-trust
  match application junos-http
user@host# set security policies from-zone untrust to-zone trust policy untrust-trust
  match application junos-https
```

```
user@host# set security policies from-zone untrust to-zone trust policy untrust-trust
    then permit
```

Verification

This section covers verifying the configuration described for access security and policy in the midsize enterprise campus. Figure 15 on page 130 shows the topology used for testing and the verification output details that follow.

Figure 15: Test Topology for the Midsize Enterprise Campus



- Verifying 802.1X on Access Devices on page 131
- Verifying Port Security on Access Devices on page 133
- Verifying Security Zone Configuration on page 135
- Verifying Source NAT Security on page 135

Verifying 802.1X on Access Devices

Purpose Verify that 802.1X has been properly configured on access ports.

Action

- Verify that clients are able to authenticate properly on wired ports.

  This is example verification output on an access device that is an EX4200.

```
root@cs-4200-ab1# run show dot1x interface | match 42.0
ge-0/0/42.0   Authenticator  Authenticated   00:10:94:00:04:3C    user101
ge-0/0/42.0                  Authenticated   00:22:22:00:04:01    phone1
ge-1/0/42.0   Authenticator  Authenticated   00:10:94:00:04:3E    user103
ge-1/0/42.0                  Authenticated   00:22:22:00:04:03    phone3
ge-2/0/42.0   Authenticator  Authenticated   00:10:94:00:04:3D    user102
ge-2/0/42.0                  Authenticated   00:22:22:00:04:02    phone2
ge-3/0/42.0   Authenticator  Authenticated   00:10:94:00:04:3F    user104
ge-3/0/42.0                  Authenticated   00:22:22:00:04:04    phone17
ge-4/0/42.0   Authenticator  Authenticated   00:10:94:00:04:40    user105
ge-4/0/42.0                  Authenticated   00:22:22:00:04:05    phone5
ge-5/0/42.0   Authenticator  Authenticated   00:10:94:00:04:41    user501
ge-5/0/42.0                  Authenticated   00:22:22:00:04:06    phone15
ge-6/0/42.0   Authenticator  Authenticated   00:10:94:00:04:42    user502
ge-6/0/42.0                  Authenticated   00:22:22:00:04:07    phone16
ge-7/0/42.0   Authenticator  Authenticated   00:10:94:00:04:43    user201
ge-7/0/42.0                  Authenticated   00:22:22:00:04:08    phone19
ge-8/0/42.0   Authenticator  Authenticated   00:10:94:00:04:44    user401
ge-8/0/42.0                  Authenticated   00:22:22:00:04:09    phone7
ge-9/0/42.0   Authenticator  Authenticated   00:10:94:00:04:45    user301
ge-9/0/42.0                  Authenticated   00:22:22:00:04:0A    phone8
```

  This is example verification output on an access device that is an EX4300.

```
root@cs-4300-ab3# run show dot1x interface | match 42.0
ge-0/0/42.0   Authenticator  Authenticated   00:10:94:00:04:47    user107
ge-0/0/42.0                  Authenticated   00:22:22:00:04:0C    phone11
ge-1/0/42.0   Authenticator  Authenticated   00:10:94:00:04:49    user202
ge-1/0/42.0                  Authenticated   00:22:22:00:04:0E    phone4
ge-2/0/42.0   Authenticator  Authenticated   00:10:94:00:04:48    user503
ge-2/0/42.0                  Authenticated   00:22:22:00:04:0D    phone12
ge-3/0/42.0   Authenticator  Authenticated   00:10:94:00:64:01    user106
ge-3/0/42.0                  Authenticated   00:22:22:00:04:0B    phone21
ge-4/0/42.0   Authenticator  Authenticated   00:10:94:00:04:4A    user402
ge-4/0/42.0                  Authenticated   00:22:22:00:04:0F    phone9
```

- Display detailed authentication reports by using the **detail** command.

  This is example verification output on an access device that is an EX4200.

```
root@cs-4200-ab1# run show dot1x interface ge-0/0/42.0 detail
ge-0/0/42.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
```

```
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 60 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest
  Number of connected supplicants: 2
    Supplicant: user101, 00:10:94:00:04:3C
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentcation method: Radius
      Authenticated VLAN: eng1_data_wired
      Dynamic Filter: ENG
      Session Reauth interval: 3600 seconds
      Reauthentication due in 256 seconds
    Supplicant: phone1, 00:22:22:00:04:01
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentcation method: Radius
      Authenticated VLAN: default
      Session Reauth interval: 3600 seconds
      Reauthentication due in 240 seconds
```

This is example verification output on an access devices that is an EX4300.

```
root@cs-4300-ab3# run show dot1x interface ge-2/0/42.0 detail
ge-2/0/42.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 60 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest
  Number of connected supplicants: 2
    Supplicant: user503, 00:10:94:00:04:48
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentcation method: Radius
      Authenticated VLAN: sales_data_wired
      Dynamic Filter: Sales
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3330 seconds
    Supplicant: phone12, 00:22:22:00:04:0D
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentcation method: Radius
      Authenticated VLAN: sales_data_wired
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3312 seconds
```

Meaning Confirm that 802.1X has been configured and operating properly on devices.

Verifying Port Security on Access Devices

Purpose Verify that port security has been configured properly on access devices.

Action

- Verify that DHCP snooping has been configured and operating properly.

  The following example verification output is on an access device that is an EX4200.

```
root@cs-4200-ab1# run show dhcp snooping binding
DHCP Snooping Information:
MAC address        IP address       Lease (seconds)  Type     VLAN    Interface
00:10:94:00:04:41  10.16.0.52                670779  dynamic  sales_data_wired
 ge-5/0/42.0
00:10:94:00:04:42  10.16.0.51                669484  dynamic  sales_data_wired
 ge-6/0/42.0
00:10:94:00:04:43  10.17.0.51               670779  dynamic  finance_data_wired
 ge-7/0/42.0
00:10:94:00:04:45  10.17.64.51               669484  dynamic  legal_data_wired
 ge-9/0/42.0
00:10:94:00:04:44  10.18.0.51                 670779  dynamic
marketing_data_wired ge-8/0/42.0
00:10:94:00:04:3C  10.32.0.52                 669484  dynamic  eng1_data_wired
 ge-0/0/42.0
00:10:94:00:04:3D  10.32.0.56                 670779  dynamic  eng1_data_wired
 ge-2/0/42.0
00:10:94:00:04:3E  10.32.0.51                 670836  dynamic  eng1_data_wired
 ge-1/0/42.0
00:10:94:00:04:3F  10.32.0.53                 669484  dynamic  eng1_data_wired
 ge-3/0/42.0
00:10:94:00:04:40  10.32.0.54                 669484  dynamic  eng1_data_wired
 ge-4/0/42.0
00:22:22:00:04:01  10.32.16.251              669526  dynamic  eng1_voice_wired
 ge-0/0/42.0
00:22:22:00:04:02  10.32.17.10               669526  dynamic  eng1_voice_wired
 ge-2/0/42.0
00:22:22:00:04:03  10.32.17.13               669526  dynamic  eng1_voice_wired
 ge-1/0/42.0
00:22:22:00:04:04  10.32.17.21               670982  dynamic  eng1_voice_wired
 ge-3/0/42.0
00:22:22:00:04:05  10.32.17.15               669526  dynamic  eng1_voice_wired
 ge-4/0/42.0
00:22:22:00:04:06  10.32.17.12               669526  dynamic  eng1_voice_wired
 ge-5/0/42.0
00:22:22:00:04:07  10.32.17.11               669526  dynamic  eng1_voice_wired
 ge-6/0/42.0
00:22:22:00:04:08  10.32.17.22               669526  dynamic  eng1_voice_wired
 ge-7/0/42.0
00:22:22:00:04:09  10.32.17.17               669526  dynamic  eng1_voice_wired
 ge-8/0/42.0
00:22:22:00:04:0A  10.32.17.18               669526  dynamic  eng1_voice_wired
 ge-9/0/42.0
00:0C:29:8C:9E:A9  172.16.12.21             691033  dynamic  guest   ge-2/0/4.0
00:10:94:00:00:0B  172.16.12.18             428737  dynamic  guest   ge-0/0/0.0
00:10:94:00:00:0C  172.16.12.19             428737  dynamic  guest   ge-2/0/0.0
00:10:94:00:00:0D  172.16.12.20             428737  dynamic  guest   ge-1/0/0.0
00:10:94:00:00:0E  172.16.12.14             428737  dynamic  guest   ge-3/0/0.0
00:10:94:00:00:0F  172.16.12.15             428737  dynamic  guest   ge-4/0/0.0
00:10:94:00:00:10  172.16.12.17             428737  dynamic  guest   ge-5/0/0.0
00:10:94:00:00:11  172.16.12.16             428737  dynamic  guest   ge-6/0/0.0
00:10:94:00:00:12  172.16.12.13             428737  dynamic  guest   ge-7/0/0.0
```

```
00:10:94:00:00:13  172.16.12.12            428737  dynamic  guest   ge-8/0/0.0
00:10:94:00:00:14  172.16.12.11            428736  dynamic  guest   ge-9/0/0.0
```

The following example verification output is on an access device that is an EX4300.

```
root@cs-4300-ab3# run show dhcp-security binding
IP address        MAC address         Vlan     Expires State   Interface
10.32.0.57        00:10:94:00:04:47   eng1_data_wired 669330 BOUND ge-0/0/42.0
10.32.0.55        00:10:94:00:64:01   eng1_data_wired 669330 BOUND ge-3/0/42.0
10.32.17.23       00:22:22:00:04:0b   eng1_voice_wired 669432 BOUND ge-3/0/42.0
10.32.17.20       00:22:22:00:04:0c   eng1_voice_wired 669432 BOUND ge-0/0/42.0
10.32.17.19       00:22:22:00:04:0d   eng1_voice_wired 669432 BOUND ge-2/0/42.0
10.32.17.14       00:22:22:00:04:0e   eng1_voice_wired 669432 BOUND ge-1/0/42.0
10.32.17.16       00:22:22:00:04:0f   eng1_voice_wired 669432 BOUND ge-4/0/42.0
10.17.0.52       00:10:94:00:04:49   finance_data_wired 669330 BOUND ge-1/0/42.0
10.18.0.52        00:10:94:00:04:4a   marketing_data_wired 669330 BOUND
ge-4/0/42.0
10.16.0.53        00:10:94:00:04:48   sales_data_wired 669330 BOUND ge-2/0/42.0
```

- Verify IP source guard configuration on devices.

```
root@cs-4200-ab1# run show ip-source-guard
IP source guard information:
Interface    Tag   IP Address       MAC Address         VLAN
ge-3/0/42.0  0     10.32.0.53       00:10:94:00:04:3F   eng1_data_wired
ge-2/0/42.0  0     10.32.0.56       00:10:94:00:04:3D   eng1_data_wired
ge-4/0/42.0  0     10.32.0.54       00:10:94:00:04:40   eng1_data_wired
ge-0/0/42.0  0     10.32.0.52       00:10:94:00:04:3C   eng1_data_wired
ge-1/0/42.0  0     10.32.0.51       00:10:94:00:04:3E   eng1_data_wired
ge-5/0/0.0   61    *                *                   eng1_voice_wired
ge-5/0/42.0  61    *                *                   eng1_voice_wired
ge-6/0/0.0   61    *                *                   eng1_voice_wired
ge-6/0/42.0  61    *                *                   eng1_voice_wired
ge-3/0/0.0   61    *                *                   eng1_voice_wired
ge-3/0/42.0  61    *                *                   eng1_voice_wired
ge-2/0/0.0   61    *                *                   eng1_voice_wired
ge-2/0/42.0  61    *                *                   eng1_voice_wired
ge-8/0/0.0   61    *                *                   eng1_voice_wired
ge-8/0/42.0  61    *                *                   eng1_voice_wired
ge-4/0/0.0   61    *                *                   eng1_voice_wired
ge-4/0/42.0  61    *                *                   eng1_voice_wired
ge-0/0/0.0   61    *                *                   eng1_voice_wired
ge-0/0/42.0  61    *                *                   eng1_voice_wired
ge-9/0/0.0   61    *                *                   eng1_voice_wired
ge-9/0/42.0  61    *                *                   eng1_voice_wired
ge-7/0/0.0   61    *                *                   eng1_voice_wired
ge-7/0/42.0  61    *                *                   eng1_voice_wired
ge-1/0/0.0   61    *                *                   eng1_voice_wired
ge-1/0/42.0  61    *                *                   eng1_voice_wired
ge-7/0/42.0  0     10.17.0.51       00:10:94:00:04:43   finance_data_wired
ge-5/0/0.0   0     172.16.12.17     00:10:94:00:00:10   guest
ge-6/0/0.0   0     172.16.12.16     00:10:94:00:00:11   guest
ge-3/0/0.0   0     172.16.12.14     00:10:94:00:00:0E   guest
ge-2/0/0.0   0     172.16.12.19     00:10:94:00:00:0C   guest
ge-2/0/4.0   0     172.16.12.21     00:0C:29:8C:9E:A9   guest
ge-8/0/0.0   0     172.16.12.12     00:10:94:00:00:13   guest
ge-4/0/0.0   0     172.16.12.15     00:10:94:00:00:0F   guest
ge-0/0/0.0   0     172.16.12.18     00:10:94:00:00:0B   guest
ge-9/0/0.0   0     172.16.12.11     00:10:94:00:00:14   guest
ge-7/0/0.0   0     172.16.12.13     00:10:94:00:00:12   guest
ge-1/0/0.0   0     172.16.12.20     00:10:94:00:00:0D   guest
ge-9/0/42.0  0     10.17.64.51      00:10:94:00:04:45   legal_data_wired
```

```
ge-8/0/42.0  0     10.18.0.51      00:10:94:00:04:44   marketing_data_wired
ge-5/0/42.0  0     10.16.0.52      00:10:94:00:04:41   sales_data_wired
ge-6/0/42.0  0     10.16.0.51      00:10:94:00:04:42   sales_data_wired
```

Verifying Security Zone Configuration

Purpose Verify that the security zones have been properly configured.

Action

- Verify security policies from the trust zone to the untrust zone.

```
root@cs-edge-fw01-node0# show security policiies from-zone trust to-zone untrust
node0:
--------------------------------------------------------------------------
From zone: trust, To zone: untrust
  Policy: trust-untrust, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1
    Source addresses: any
    Destination addresses: any
    Applications: junos-http, junos-https, junos-dns-udp, junos-dns-tcp,
    junos-ntp, junos-icmp-ping, junos-udp-any, udp3min
    Action: permit
```

- Verify security policies from the untrust zone to the trust zone.

```
root@cs-edge-fw01-node0# show security policies from-zone untrust to-zone trust
node0:
--------------------------------------------------------------------------
From zone: untrust, To zone: trust
  Policy: Remote-SA, State: enabled, Index: 5, Scope Policy: 0, Sequence number:
 1
    Source addresses: any
    Destination addresses: SA-Address
    Applications: junos-https, junos-http
    Action: permit
  Policy: untrust-trust, State: enabled, Index: 6, Scope Policy: 0, Sequence
number: 2
    Source addresses: any
    Destination addresses: any
    Applications: junos-http, junos-https, junos-udp-any
    Action: permit
```

Meaning Confirm that the security zones were configured properly on the security device.

Verifying Source NAT Security

Purpose Verify that the source NAT security configuration on the security devices is set up and operating properly.

Action Show the source NAT summary on the security device.

```
root@cs-edge-fw01-node0# run show security nat source summary
node0:
--------------------------------------------------------------------------
Total port number usage for port translation pool: 1106954
Maximum port number for port translation pool: 67108864
Total pools: 7
```

```
Pool                Address                 Routing             PAT  Total
Name                Range                   Instance                 Address
SNATguestPool       10.92.84.12-10.92.84.12 default             yes  1
Source-NAT1         10.92.84.60-10.92.84.60 default             yes  1
Source-NAT2         10.92.84.61-10.92.84.61 default             yes  1
Source-NAT3         10.92.84.62-10.92.84.62 default             yes  1
Source-NAT4         10.92.84.63-10.92.84.63 default             yes  1
Source-NAT5         10.92.84.64-10.92.84.64 default             yes  1
Source-NAT6         10.92.84.65-10.92.84.80 default             yes  16

Total rules: 7
Rule name          Rule set       From             To                  Action
R2                 SNATguest      DMZ              untrust
SNATguestPool
Ru1                SNAT1          trust            untrust
Source-NAT1
Ru2                SNAT1          trust            untrust
Source-NAT2
Ru3                SNAT1          trust            untrust
Source-NAT3
Ru4                SNAT1          trust            untrust
Source-NAT4
Ru5                SNAT1          trust            untrust
Source-NAT5
Ru7                SNAT1          trust            untrust
Source-NAT6

node1:
--------------------------------------------------------------------------
Total port number usage for port translation pool: 1106954
Maximum port number for port translation pool: 67108864
Total pools: 7
Pool                Address                 Routing             PAT  Total
Name                Range                   Instance                 Address
SNATguestPool       10.92.84.12-10.92.84.12 default             yes  1
Source-NAT1         10.92.84.60-10.92.84.60 default             yes  1
Source-NAT2         10.92.84.61-10.92.84.61 default             yes  1
Source-NAT3         10.92.84.62-10.92.84.62 default             yes  1
Source-NAT4         10.92.84.63-10.92.84.63 default             yes  1
Source-NAT5         10.92.84.64-10.92.84.64 default             yes  1
Source-NAT6         10.92.84.65-10.92.84.80 default             yes  16

Total rules: 7
Rule name          Rule set       From             To                  Action
R2                 SNATguest      DMZ              untrust
SNATguestPool
Ru1                SNAT1          trust            untrust
Source-NAT1
Ru2                SNAT1          trust            untrust
Source-NAT2
Ru3                SNAT1          trust            untrust
Source-NAT3
Ru4                SNAT1          trust            untrust
Source-NAT4
Ru5                SNAT1          trust            untrust
Source-NAT5
Ru7                SNAT1          trust            untrust
Source-NAT6
```

Meaning Confirm that the configuration is working properly.

Related Documentation

- Understanding the Benefits of the Midsize Enterprise Campus Solution on page 6
- Example: Configuring High Availability for the Midsize Enterprise Campus on page 39
- Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus on page 85
- Example: Configuring Class of Service for the Midsize Enterprise Campus on page 137

Example: Configuring Class of Service for the Midsize Enterprise Campus

This example provides detailed steps for configuring class of service (CoS) on the switches in the access, aggregation, and core layers. The CoS parameters used in this example are designed to provide high quality of service to voice, video, and critical data applications by giving the application traffic priority over other traffic.

This example covers:

Requirements

Table 21 on page 137 shows the hardware and software requirements for this example. Table 22 on page 138 shows the scaling and performance targets used for this example.

Table 21: Hardware and Software Requirements

Hardware	Device Name	Software
MX240	cs-edge-r01, cs-edge-r02	13.2 R2.4
SRX650	cs-edge-fw-01, cs-edge-fw02	12.1 X44-D39.4
EX9214	cs-core-sw01, cs-core-sw02	13.2 R3.7
EX4550	cs-agg-01	12.3 R3.4
EX2200	cs-2200-ab5	12.3 R3.4
EX3300	cs-3300-ab4	12.3 R3.4
EX4200	cs-4200-ab1	12.3 R3.4
EX4300	cs-4300-ab2, cs-4300-ab3	13.2 X51-D21.1

Table 22: Node Features and Performance/Scalability

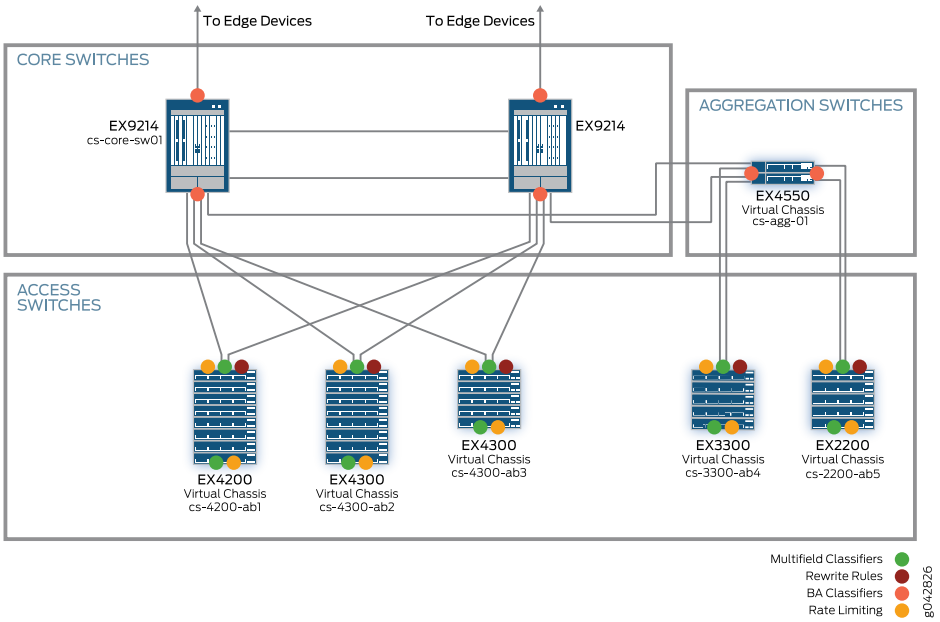
Node	Features	Performance/Scalability Target Value
Edge (MX240, SRX650)	MC-LAG, OSPF, BGP, IRB	3k IPv4
Core (EX9214)	VLANs, MC-LAG, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, IRB	3k IPv4 routes 128k MAC table entries 16k ARP entries
Aggregation (EX4550)	VLANs, LAG, IGMP snooping, OSPF, PIM-SM, IGMP, DHCP relay, RVI	3k IPv4 routes 5 IGMP groups
Access (EX3300, EX4300, EX4200)	VLANs, LAG, 802.1X, IGMP snooping, DHCP snooping, ARP inspection, IP source guard	55k MAC table entries 13k 8021.x users 5 IGMP groups

The configuration procedures that follow assume that the devices and device interfaces have been configured as described in "Example: Configuring High Availability for the Midsize Enterprise Campus" on page 39 and "Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus" on page 85.

Overview and Topology

As described in "Understanding the Design of the Midsize Enterprise Campus Solution" on page 6, a CoS configuration consists of multiple components, such as forwarding classes, schedulers, rewrite rules, and classifiers, that are configured on a per-hop basis. Figure 16 on page 139 shows where different components are configured in this solution.

Figure 16: Class-of-Service Components in the LAN



Configuring CoS in the Access Layer

This section describes how to configure CoS on the Virtual Chassis in the access layer. Table 23 on page 139 summarizes the CoS parameters used in the configuration.

Table 23: CoS Parameters for Access Virtual Chassis

Forwarding Class		Queue Number		DSCP Code Point	Queue Priority	Buffer Size	Transmit Rate	Rate Limiting	
EX4200, EX3300, EX2200	EX4300	EX4200, EX3300, EX2200	EX4300					Network Ports	Access Ports
Network-Control	Network-Control	7	3	NC1	Strict-high	5%	—	5%	1%
Voice	Voice	5	1	EF	Strict-high	5%	—	5%	1%
Video	mcast-be	3	8	AF21	Low	20%	20%	—	—
Mission-Critical	Mission-Critical	1	2	AF11	Low	40%	40%	—	—
Best-Effort	Best-Effort	0	0	BE	Low	Remainder	Remainder	—	—

As shown in Table 23 on page 139, the forwarding classes and queues used on the EX2200, EX3300, and EX4200 Virtual Chassis differ from the default forwarding classes and queues used on the EX4300 Virtual Chassis. Because of this, two sets of configuration

statements are shown for each step in the following procedures: one for the EX2200, EX3300, and EX4200 Virtual Chassis and one for the EX4300 Virtual Chassis.

To configure CoS on the Virtual Chassis in the access layer, perform these tasks:

Configure the Forwarding Classes

Step-by-Step Procedure

To configure the forwarding classes and associated queues shown in Table 23 on page 139:

- Enter the following commands:

  EX2200, EX3300, and EX4200 Virtual Chassis:

  ```
  [edit class-of-service]
  user@cs4200-ab1# set forwarding-classes class Network-Control queue-num 7
  user@cs-4200-ab1# set forwarding-classes class Voice queue-num 5
  user@cs-4200-ab1# set forwarding-classes class Video queue-num 3
  user@cs-4200-ab1# set forwarding-classes class Mission-Critical queue-num 1
  user@cs-4200-ab1# set forwarding-classes class Best-Effort queue-num 0
  ```

  EX4300 Virtual Chassis:

  ```
  [edit class-of-service]
  user@cs-4300-ab2# set forwarding-classes class Network-Control queue-num
  3
  user@cs-4300-ab2# set forwarding-classes class Voice queue-num 1
  user@cs-4300-ab2# set forwarding-classes class mcast-be queue-num 8
  user@cs-4300-ab2# set forwarding-classes class Mission-Critical queue-num 2
  user@cs-4300-ab2# set forwarding-classes class Best-Effort queue-num 0
  ```

Configure Schedulers and Scheduler Maps

Step-by-Step Procedure

Schedulers define buffer sizes, queue priorities, transmit rates, drop profiles, and queue shaping. Scheduler maps associate specific schedulers with specific forwarding classes, or queues.

To configure the schedulers and scheduler maps:

1. Configure the schedulers.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4200-ab1# set schedulers control-network-sched shaping-rate percent
    5
   user@cs-4200-ab1# set schedulers control-network-sched buffer-size percent 5
   user@cs-4200-ab1# set schedulers control-network-sched priority strict-high
   user@cs-4200-ab1# set schedulers control-user-sched shaping-rate percent 1
   user@cs-4200-ab1# set schedulers control-user-sched buffer-size percent 5
   user@cs-4200-ab1# set schedulers control-user-sched priority strict-high
   user@cs-4200-ab1# set schedulers voice-network-sched shaping-rate percent 5
   ```

```
user@cs-4200-ab1# set schedulers voice-network-sched buffer-size percent 5
user@cs-4200-ab1# set schedulers voice-network-sched buffer-size exact
user@cs-4200-ab1# set schedulers voice-network-sched priority strict-high
user@cs-4200-ab1# set schedulers voice-user-sched shaping-rate percent 1
user@cs-4200-ab1# set schedulers voice-user-sched buffer-size percent 5
user@cs-4200-ab1# set schedulers voice-user-sched buffer-size exact
user@cs-4200-ab1# set schedulers voice-user-sched priority strict-high
user@cs-4200-ab1# set schedulers video-sched transmit-rate percent 20
user@cs-4200-ab1# set schedulers video-sched buffer-size percent 20
user@cs-4200-ab1# set schedulers video-sched priority low
user@cs-4200-ab1# set schedulers mission-critical-sched transmit-rate percent
 40
user@cs-4200-ab1# set schedulers mission-critical-sched buffer-size percent 40
user@cs-4200-ab1# set schedulers mission-critical-sched priority low
user@cs-4200-ab1# set schedulers be-sched transmit-rate remainder
user@cs-4200-ab1# set schedulers be-sched buffer-size remainder
user@cs-4200-ab1# set schedulers be-sched priority low
```

EX4300 Virtual Chassis:

```
[edit class-of-service]
user@cs-4300-ab2# set schedulers control-network-sched shaping-rate percent
 5
user@cs-4300-ab2# set schedulers control-network-sched buffer-size percent
5
user@cs-4300-ab2# set schedulers control-network-sched priority strict-high
user@cs-4300-ab2#  set schedulers control-user-sched shaping-rate percent 1
user@cs-4300-ab2# set schedulers control-user-sched buffer-size percent 5
user@cs-4300-ab2# set schedulers control-user-sched priority strict-high
user@cs-4300-ab2# set schedulers voice-network-sched shaping-rate percent
5
user@cs-4300-ab2# set schedulers voice-network-sched buffer-size percent 5
user@cs-4300-ab2#  set schedulers voice-network-sched priority strict-high
user@cs-4300-ab2# set schedulers voice-user-sched shaping-rate percent 1
user@cs-4300-ab2# set schedulers voice-user-sched buffer-size percent 5
user@cs-4300-ab2# set schedulers voice-user-sched priority strict-high
user@cs-4300-ab2# set schedulers mcast-be-sched transmit-rate percent 20
user@cs-4300-ab2# set schedulers mcast-be-sched buffer-size percent 20
user@cs-4300-ab2# set schedulers mcast-be-sched priority low
user@cs-4300-ab2# set schedulers Mission-Critical-sched transmit-rate percent
 40
user@cs-4300-ab2# set schedulers Mission-Critical-sched buffer-size percent
40
user@cs-4300-ab2# set schedulers Mission-Critical-sched priority low
user@cs-4300-ab2# set schedulers be-sched transmit-rate remainder
user@cs-4300-ab2# set schedulers be-sched buffer-size remainder
user@cs-4300-ab2# set schedulers be-sched priority low
```

2. Create scheduler maps that map the schedulers to forwarding classes.

   Two scheduler maps are created: one for use with access ports (access-port-sched) and the other for the uplink ports (network-port-sched).

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit class-of-service]
   ```

```
user@cs-4200-ab1# set scheduler-maps access-port-sched forwarding-class
Network-Control scheduler control-user-sched
user@cs-4200-ab1# set scheduler-maps access-port-sched forwarding-class
Voice scheduler voice-user-sched
user@cs-4200-ab1# set scheduler-maps access-port-sched forwarding-class
Video scheduler video-sched
user@cs-4200-ab1# set scheduler-maps access-port-sched forwarding-class
Mission-Critical scheduler mission-critical-sched
user@cs-4200-ab1# set scheduler-maps access-port-sched forwarding-class
Best-Effort scheduler be-sched
user@cs-4200-ab1# set scheduler-maps network-port-sched forwarding-class
Network-Control scheduler control-network-sched
user@cs-4200-ab1# set scheduler-maps network-port-sched forwarding-class
Voice scheduler voice-network-sched
user@cs-4200-ab1# set scheduler-maps network-port-sched forwarding-class
Video scheduler video-sched
user@cs-4200-ab1# set scheduler-maps network-port-sched forwarding-class
Mission-Critical scheduler mission-critical-sched
user@cs-4200-ab1# set scheduler-maps network-port-sched forwarding-class
Best-Effort scheduler be-sched
```

EX4300 Virtual Chassis:

```
[edit class-of-service]
user@cs-4300-ab2# set scheduler-maps access-port-sched forwarding-class
Network-Control scheduler control-user-sched
user@cs-4300-ab2# set scheduler-maps access-port-sched forwarding-class
Voice scheduler voice-user-sched
user@cs-4300-ab2# set scheduler-maps access-port-sched forwarding-class
mcast-be scheduler mcast-be-sched
user@cs-4300-ab2# set scheduler-maps access-port-sched forwarding-class
Mission-Critical scheduler Mission-Critical-sched
user@cs-4300-ab2# set scheduler-maps access-port-sched forwarding-class
Best-Effort scheduler be-sched
user@cs-4300-ab2# set scheduler-maps network-port-sched forwarding-class
Network-Control scheduler control-network-sched
user@cs-4300-ab2# set scheduler-maps network-port-sched forwarding-class
Voice scheduler voice-network-sched
user@cs-4300-ab2# set scheduler-maps network-port-sched forwarding-class
mcast-be scheduler mcast-be-sched
user@cs-4300-ab2# set scheduler-maps network-port-sched forwarding-class
Mission-Critical scheduler Mission-Critical-sched
user@cs-4300-ab2# set scheduler-maps network-port-sched forwarding-class
Best-Effort scheduler be-sched
```

3. Assign the scheduler maps to the interfaces on the access switches.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4200-ab1# set interfaces ge-* scheduler-map access-port-sched
   user@cs-4200-ab1# set interfaces ae* scheduler-map network-port-sched
   ```

   EX4300 Virtual Chassis:

```
[edit class-of-service]
user@cs-4300-ab2# set interfaces ge-* scheduler-map access-port-sched
user@cs-4300-ab2# set interfaces ae* scheduler-map network-port-sched
```

Configure Rewrite Rules

Step-by-Step Procedure

The rewrite rules mark packets with the DSCP code points shown in Table 23 on page 139.

To configure the rewrite rules:

1. Create the rewrite rules.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4200-ab1# set rewrite-rules dscp rewrite-dscp forwarding-class
   Network-Control loss-priority low code-point nc1
   user@cs-4200-ab1# set rewrite-rules dscp rewrite-dscp forwarding-class Voice
   loss-priority low code-point ef
   user@cs-4200-ab1# set rewrite-rules dscp rewrite-dscp forwarding-class Video
   loss-priority low code-point af21
   user@cs-4200-ab1# set rewrite-rules dscp rewrite-dscp forwarding-class
   Mission-Critical loss-priority low code-point af11
   user@cs-4200-ab1# set rewrite-rules dscp rewrite-dscp forwarding-class
   Best-Effort loss-priority low code-point be
   ```

   EX4300 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4300-ab2# set rewrite-rules dscp rewrite-dscp forwarding-class
   Network-Control loss-priority low code-point nc1
   user@cs-4300-ab2# set rewrite-rules dscp rewrite-dscp forwarding-class Voice
    loss-priority low code-point ef
   user@cs-4300-ab2# set rewrite-rules dscp rewrite-dscp forwarding-class
   mcast-be loss-priority low code-point af21
   user@cs-4300-ab2# set rewrite-rules dscp rewrite-dscp forwarding-class
   Mission-Critical loss-priority low code-point af11
   user@cs-4300-ab2# set rewrite-rules dscp rewrite-dscp forwarding-class
   Best-Effort loss-priority low code-point be
   ```

2. Assign the rewrite rules to the logical interfaces on the aggregated Ethernet interfaces leading to the aggregation layer.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4200-ab1# set interfaces ae* unit * rewrite-rules dscp rewrite-dscp
   ```

   EX4300 Virtual Chassis:

   ```
   [edit class-of-service]
   user@cs-4300-ab2# set interfaces ae* unit * rewrite-rules dscp rewrite-dscp
   ```

Configure Multifield Classifiers

Step-by-Step Procedure

The multifield classifiers are implemented as firewall filters that classify traffic into the forwarding classes shown in Table 23 on page 139.

To configure the multifield classifiers:

1. Create the multifield classifier for classifying voice traffic.

   In this example, traffic arriving on port 5060, the standard port for SIP traffic, is classified as voice traffic.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit]
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf from destination-port 5060
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then accept
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then forwarding-class Voice
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then loss-priority low
   ```

   EX4300 Virtual Chassis:

   ```
   [edit]
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf from destination-port 5060
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then accept
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then forwarding-class Voice
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term voice-mf then loss-priority low
   ```

2. Create the multifield classifier for classifying video or multicast traffic.

   This multifield classifier matches traffic with the multicast destination address or with the DSCP value equaling af21.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit]
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mcast from destination-address 230.0.0.0/8
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mcast from dscp af21
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mcast then accept
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mcast then forwarding-class Video
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mcast then loss-priority low
   ```

   EX4300 Virtual Chassis:

   ```
   [edit]
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
   ```

```
term mcast-af-mf from dscp af21
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term mcast-af-mf from ip-destination-address 230.0.0.0/8
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term mcast-af-mf then accept
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term mcast-af-mf then forwarding-class mcast-be
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term mcast-af-mf then loss-priority low
```

3. Create the multifield classifier for classifying mission-critical traffic arriving at the access ports.

   In this example, traffic on port 80 (HTTP traffic) and port 25 (SMTP traffic) is classified as mission-critical traffic.

   EX2200, EX3300, and EX4200 Virtual Chassis:

```
[edit]
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-http-mf from destination-port 80
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-http-mf then accept
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-http-mf then forwarding-class Mission-Critical
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-http-mf then loss-priority low
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-smtp-mf from destination-port 25
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-smtp-mf then accept
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-smtp-mf then forwarding-class Mission-Critical
user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
term Mission-critical-smtp-mf then loss-priority low
```

   EX4300 Virtual Chassis:

```
[edit]
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-http-mf from destination-port 80
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-http-mf then accept
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-http-mf then forwarding-class Mission-Critical
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-http-mf then loss-priority low
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-smtp-mf from destination-port 25
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-smtp-mf then accept
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-smtp-mf then forwarding-class Mission-Critical
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
term Mission-Critical-smtp-mf then loss-priority low
```

4. Create the multifield classifier for classifying mission-critical traffic returning from the HTTP and SMTP servers.

   This classifier matches on source address matching the IP addresses of the servers or the DSCP value equaling af11.

   BA classification cannot be used for the return traffic on the Layer 2 interfaces from the aggregation layers because the multifield classifiers used on the VLANs take precedence.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit ]
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from source-address 172.16.34.2/32
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from source-address 172.16.34.18/32
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from dscp af11
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then accept
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then forwarding-class Mission-Critical
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then loss-priority low
   ```

   EX4300 Virtual Chassis:

   ```
   [edit]
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from dscp af11
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from ip-source-address 172.16.34.2/32
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret from ip-source-address 172.16.34.18/32
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then accept
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then forwarding-class Mission-Critical
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term Mission-critical-httpsmtp-ret then loss-priority low
   ```

5. Create the multifield classifier for classifying best-effort traffic.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit]
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term default then accept
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term default then forwarding-class Best-Effort
   user@cs-4200-ab1# set firewall family ethernet-switching filter mf-class-classifier
    term default then loss-priority high
   ```

   EX4300 Virtual Chassis:

   ```
   [edit]
   user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
    term default then accept
   ```

```
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
 term default then forwarding-class Best-Effort
user@cs-4300-ab2# set firewall family ethernet-switching filter mf-class-classifier
 term default then loss-priority low
```

6. Assign the multifield classifiers to the VLANs carrying user traffic.

   Examples of doing so for the VLANs eng1_data_wired and eng1_voice_wired are shown.

   EX2200, EX3300, and EX4200 Virtual Chassis:

   ```
   [edit]
   user@cs-4200-ab1# set vlans eng1_data_wired filter input mf-class-classifier
   user@cs-4200-ab1#  set vlans eng1_voice_wired filter input mf-class-classifier
   ```

   EX4300 Virtual Chassis:

   ```
   user@cs-4300-ab2# set vlans eng1_data_wired forwarding-options filter input
   mf-class-classifier
   user@cs-4300-ab2# set vlans eng1_voice_wired forwarding-options filter input
   mf-class-classifier
   ```

Configuring CoS in the Aggregation Layer

This section describes how to configure CoS on the EX4550 Virtual Chassis in location B. Table 24 on page 147 summarizes the CoS parameters used in the configuration.

Table 24: CoS Parameters for Aggregation Virtual Chassis

Forwarding Class	Queue Number	DSCP Code Point	Queue Priority	Buffer Size	Transmit Rate
Network-Control	7	NC1	Strict-high	5%	—
Voice	5	EF	Strict-high	5%	—
Video	3	AF21	Low	20%	20%
Mission-Critical	1	AF11	Low	40%	40%
Best-Effort	0	BE	Low	Remainder	Remainder

To configure CoS on the EX4550 Virtual Chassis, perform these tasks:

- Configure Forwarding Classes on page 147
- Configure Schedulers and Scheduler Maps on page 148
- Configure the Behavior Aggregate Classifier on page 149

Configure Forwarding Classes

Step-by-Step Procedure

To configure the forwarding classes and associated queues shown in Table 24 on page 147:

- Enter the following commands:

```
[edit class-of-service]
user@cs-agg-01# set forwarding-classes class Network-Control queue-num 7
user@cs-agg-01# set forwarding-classes class Voice queue-num 5
user@cs-agg-01# set forwarding-classes class Video queue-num 3
user@cs-agg-01# set forwarding-classes class Mission-Critical queue-num 1
user@cs-agg-01# set forwarding-classes class Best-Effort queue-num 0
```

Configure Schedulers and Scheduler Maps

Step-by-Step Procedure

Schedulers define buffer sizes, queue priorities, transmit rates, drop profiles, and queue shaping. Scheduler maps associate specific schedulers with specific forwarding classes, or queues.

For the aggregation switch, you create one scheduler per forwarding class, configuring the scheduler with the queue priority, buffer size, and transmit rate shown in Table 24 on page 147.

To configure the schedulers and scheduler maps:

1. Configure the schedulers.

```
[edit class-of-service]
user@cs-agg-01# set schedulers control-network-sched buffer-size percent 5
user@cs-agg-01# set schedulers control-network-sched priority strict-high
user@cs-agg-01# set schedulers voice-network-sched buffer-size percent 5
user@cs-agg-01# set schedulers voice-network-sched priority strict-high
user@cs-agg-01# set schedulers video-sched transmit-rate percent 20
user@cs-agg-01# set schedulers video-sched buffer-size percent 20
user@cs-agg-01# set schedulers video-sched priority low
user@cs-agg-01# set schedulers mission-critical-sched transmit-rate percent 40
user@cs-agg-01# set schedulers mission-critical-sched buffer-size percent 40
user@cs-agg-01# set schedulers mission-critical-sched priority low
user@cs-agg-01# set schedulers be-sched transmit-rate remainder
user@cs-agg-01# set schedulers be-sched buffer-size remainder
user@cs-agg-01# set schedulers be-sched priority low
```

2. Configure the scheduler map.

```
[edit class-of-service]
user@cs-agg-01# set scheduler-maps network-port-sched forwarding-class
Network-Control scheduler control-network-sched
user@cs-agg-01# set scheduler-maps network-port-sched forwarding-class Voice
 scheduler voice-network-sched
user@cs-agg-01# set scheduler-maps network-port-sched forwarding-class Video
 scheduler video-sched
user@cs-agg-01# set scheduler-maps network-port-sched forwarding-class
Mission-Critical scheduler mission-critical-sched
user@cs-agg-01# set scheduler-maps network-port-sched forwarding-class
Best-Effort scheduler be-sched
```

3. Assign the scheduler map to the interfaces leading to the core switches and to all aggregated Ethernet interfaces.

```
[edit class-of-service]
user@cs-agg-01# set interfaces xe-0/0/0 scheduler-map network-port-sched
```

```
user@cs-agg-01# set interfaces xe-1/0/0 scheduler-map network-port-sched
user@cs-agg-01# set interfaces ae* scheduler-map network-port-sched
```

Configure the Behavior Aggregate Classifier

Step-by-Step Procedure

In this procedure, you create the behavior aggregate (BA) classifier, using the code points shown in Table 24 on page 147 to map traffic to forwarding classes. You then assign the classifier to interfaces.

To configure the BA classifier:

1. Create the BA classifier.

```
[edit class-of-service]
user@cs-agg-01# set classifiers dscp dscp_ba forwarding-class Network-Control
 loss-priority low code-points nc1
user@cs-agg-01# set classifiers dscp dscp_ba forwarding-class Voice loss-priority
 low code-points ef
user@cs-agg-01# set classifiers dscp dscp_ba forwarding-class Video loss-priority
 low code-points af21
user@cs-agg-01# set classifiers dscp dscp_ba forwarding-class Mission-Critical
loss-priority low code-points af11
user@cs-agg-01# set classifiers dscp dscp_ba forwarding-class Best-Effort
loss-priority low code-points be
```

2. Assign the BA classifier to interfaces.

   For the example topology, the classifier is assigned to the logical interfaces leading to the core switches and to the logical aggregated Ethernet interfaces.

```
[edit class-of-service]
user@cs-agg-01# set interfaces xe-0/0/0 unit * classifiers dscp dscp_ba
user@cs-agg-01# set interfaces xe-1/0/0 unit * classifiers dscp dscp_ba
user@cs-agg-01# set interfaces ae* unit * classifiers dscp dscp_ba
```

Configuring CoS in the Core Layer

This section describes how to configure CoS on the EX9214 core switches. Table 25 on page 149 summarizes the CoS parameters used in the configuration.

Table 25: CoS Parameters for Core Switches

Forwarding Class	Queue Number	DSCP Code Point	Queue Priority	Buffer Size	Transmit Rate
Network-Control	7	NC1	Low	5%	5%
Voice	5	EF	Strict-high	5%	—
Video	3	AF21	Low	20%	20%
Mission-Critical	1	AF11	Low	40%	40%
Best-Effort	0	BE	Low	Remainder	Remainder

To configure CoS in the core layer, perform these tasks on both cs-core-sw01 and cs-core-sw02:

Configure Forwarding Classes

Step-by-Step Procedure

To configure the forwarding classes and their associated queues, as shown in Table 25 on page 149:

- Enter the following commands:

```
[edit class-of-service]
user@cs-core-sw01# set forwarding-classes class Network-Control queue-num
7
user@cs-core-sw01# set forwarding-classes class Voice queue-num 5
user@cs-core-sw01# set forwarding-classes class Video queue-num 3
user@cs-core-sw01# set forwarding-classes class Mission-Critical queue-num 1
user@cs-core-sw01# set forwarding-classes class Best-Effort queue-num 0
```

Configure Schedulers and Scheduler Maps

Step-by-Step Procedure

Schedulers define buffer sizes, queue priorities, transmit rates, drop profiles, and queue shaping. Scheduler maps associate specific schedulers with specific forwarding classes, or queues.

For the core switches, you create one scheduler per forwarding class, configuring the scheduler with the queue priority, buffer size, and transmit rate shown in Table 25 on page 149.

To configure the schedulers and scheduler maps:

1. Configure the schedulers.

```
[edit class-of-service]
user@cs-core-sw01# set schedulers control-network-sched transmit-rate percent
 5
user@cs-core-sw01# set schedulers control-network-sched buffer-size percent
5
user@cs-core-sw01# set schedulers control-network-sched priority low
user@cs-core-sw01# set schedulers voice-network-sched buffer-size percent 5
user@cs-core-sw01# set schedulers voice-network-sched priority strict-high
user@cs-core-sw01# set schedulers video-sched transmit-rate percent 20
user@cs-core-sw01# set schedulers video-sched buffer-size percent 20
user@cs-core-sw01# set schedulers video-sched priority low
user@cs-core-sw01# set schedulers mission-critical-sched transmit-rate percent
 40
user@cs-core-sw01# set schedulers mission-critical-sched buffer-size percent
40
user@cs-core-sw01# set schedulers mission-critical-sched priority low
user@cs-core-sw01# set schedulers be-sched transmit-rate remainder
```

```
user@cs-core-sw01# set schedulers be-sched buffer-size remainder
user@cs-core-sw01# set schedulers be-sched priority low
```

2. Configure the scheduler map.

```
[edit class-of-service]
user@cs-core-sw01# set scheduler-maps network-port-sched forwarding-class
Network-Control scheduler control-network-sched
user@cs-core-sw01# set scheduler-maps network-port-sched forwarding-class
Voice scheduler voice-network-sched
user@cs-core-sw01# set scheduler-maps network-port-sched forwarding-class
Video scheduler video-sched
user@cs-core-sw01# set scheduler-maps network-port-sched forwarding-class
Mission-Critical scheduler mission-critical-sched
user@cs-core-sw01# set scheduler-maps network-port-sched forwarding-class
Best-Effort scheduler be-sched
```

3. Assign the scheduler map to the interface leading to the aggregation switch and to all aggregated Ethernet interfaces.

```
[edit class-of-service]
user@cs-core-sw01# set interfaces xe-0/1/0 scheduler-map network-port-sched
user@cs-core-sw01# set interfaces ae* scheduler-map network-port-sched
```

Configure the Behavior Aggregate Classifier

Step-by-Step Procedure

In this procedure, you create the behavior aggregate (BA) classifier, using the code points shown in Table 25 on page 149 to map traffic to forwarding classes. You then assign the classifier to interfaces.

To configure the BA classifier:

1. Create the BA classifier.

```
[edit class-of-service]
user@cs-core-sw01# set classifiers dscp dscp_ba forwarding-class
Network-Control loss-priority low code-points nc1
user@cs-core-sw01# set classifiers dscp dscp_ba forwarding-class Voice
loss-priority low code-points ef
user@cs-core-sw01# set classifiers dscp dscp_ba forwarding-class Video
loss-priority low code-points af21
user@cs-core-sw01# set classifiers dscp dscp_ba forwarding-class Mission-Critical
 loss-priority low code-points af11
user@cs-core-sw01# set classifiers dscp dscp_ba forwarding-class Best-Effort
loss-priority low code-points be
```

2. Assign the BA classifier to logical interfaces.

   For the example topology, the classifier is assigned to the interface leading to the aggregation switch, to all aggregated Ethernet interfaces, and to all IRB interfaces.

```
[edit class-of-service]
user@cs-core-sw01# set interfaces xe-0/1/0 unit 0 classifiers dscp dscp_ba
user@cs-core-sw01# set interfaces ae* unit * classifiers dscp dscp_ba
user@cs-core-sw01# set interfaces irb unit * classifiers dscp dscp_ba
```

Verifying the Configuration

Confirm that the configuration is working properly.

Verifying the CoS Configuration in the Access Layer

Purpose Verify that CoS is configured correctly on the Virtual Chassis in the access layer.

Action Perform the following steps on the switches in the access layer:

1. Verify that the rewrite rules are properly configured.

   - On EX2200, EX3300, and EX4200 switches, enter:

```
user@cs-4200-ab1> show class-of-service rewrite-rule name rewrite-dscp
Rewrite rule: rewrite-dscp, Code point type: dscp, Index: 5066
  Forwarding class                Loss priority       Code point
  Best-Effort                     low                 000000
  Voice                           low                 101110
  Mission-Critical                low                 001010
  Network-Control                 low                 110000
  Video                           low                 010010
```

   - On EX4300 switches, enter:

```
user@cs-4300-ab3> show class-of-service rewrite-rule name rewrite-dscp
Rewrite rule: rewrite-dscp, Code point type: dscp, Index: 5066
  Forwarding class                Loss priority       Code point
  Best-Effort                     low                 000000
  Voice                           low                 101110
  Mission-Critical                low                 001010
  Network-Control                 low                 110000
  mcast-be                        low                 010010
```

   The DSCP code points are displayed in binary. Table Table 26 on page 152 shows the binary representation of the DSCP code points used in this configuration example.

Table 26: Binary Representation of Code Points

Forwarding Class	DSCP Code Point	Binary Representation
Network-Control	NC1	110000
Voice	EF	101110
Video mcast-be	AF21	010010
Mission-Critical	AF11	001010
Best-Effort	BE	000000

2. Verify that the class-of-service queues on the uplink interfaces—that is, an interface facing the core switch—are correct and that the queues are forwarding traffic.

NOTE: On the access switches used in this network configuration example, queue information is not available for aggregated Ethernet interfaces. To verify the class-of-service queues for an aggregated Ethernet interface, you must display the queues for the member interfaces themselves.

- On EX2200, EX3300, and EX4200 switches, enter:

```
user@cs-4200-ab1> show interfaces queue xe-2/1/0
Physical interface: xe-2/1/0, Enabled, Physical link is Up
  Interface index: 326, SNMP ifIndex: 648
Forwarding classes: 16 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :              1913991
    Bytes                :            995273072
    Tail-dropped packets :                    0
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets              :              5741958
    Bytes                :           2985818928
    Tail-dropped packets :                    0
Queue: 3, Forwarding classes: Video
  Queued:
  Transmitted:
    Packets              :                    0
    Bytes                :                    0
    Tail-dropped packets :                    0
Queue: 5, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets              :              7655940
    Bytes                :           1010584080
    Tail-dropped packets :                    0
Queue: 7, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                16940
    Bytes                :              1354260
    Tail-dropped packets :                    0
```

- On EX4300 switches, enter:

```
user@cs-4300-ab3> show interfaces queue xe-0/2/0
Physical interface: xe-0/2/0, Enabled, Physical link is Up
  Interface index: 1362, SNMP ifIndex: 811
Forwarding classes: 16 supported, 8 in use
Egress queues: 12 supported, 8 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :               775426
```

```
    Bytes               :             400084208
    Tail-dropped packets :                     0
Queue: 1, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets             :               3797507
    Bytes               :             486080896
    Tail-dropped packets :                     0
Queue: 2, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets             :               1562469
    Bytes               :            1010800788
    Tail-dropped packets :                     0
Queue: 3, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets             :                  1519
    Bytes               :                114950
    Tail-dropped packets :                     0
Queue: 8, Forwarding classes: mcast-be, mcast-be
  Queued:
  Transmitted:
    Packets             :                     0
    Bytes               :                     0
    Tail-dropped packets :                     0
Queue: 9, Forwarding classes: mcast-ef
  Queued:
```

3. Verify that the class-of-service queues on an access interface—that is, an interface facing a client—are correct and that the queues are forwarding traffic.

   - On EX2200, EX3300, and EX4200 switches, enter:

```
user@cs-4200-ab1> show interfaces queue ge-3/0/42
Physical interface: ge-3/0/42, Enabled, Physical link is Up
  Interface index: 369, SNMP ifIndex: 741
Forwarding classes: 16 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets             :              10380662
    Bytes               :            5394656270
    Tail-dropped packets :                     0
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets             :              31128850
    Bytes               :           24158391696
    Tail-dropped packets :                     0
Queue: 3, Forwarding classes: Video
  Queued:
  Transmitted:
    Packets             :              10372551
    Bytes               :            5393726520
    Tail-dropped packets :                     0
Queue: 5, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets             :               8298040
    Bytes               :            1095341280
```

```
    Tail-dropped packets :                      0
Queue: 7, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                     38
    Bytes                :                  12616
    Tail-dropped packets :                      0
```

- On EX4300 switches, enter:

```
user@cs-4300-ab3> show interfaces queue ge-4/0/42
Physical interface: ge-4/0/42, Enabled, Physical link is Up
  Interface index: 1558, SNMP ifIndex: 804
Forwarding classes: 16 supported, 8 in use
Egress queues: 12 supported, 8 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :               1155014
    Bytes                :             591367168
    Tail-dropped packets :                      0
Queue: 1, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets              :                923956
    Bytes                :             118266368
    Tail-dropped packets :                      0
Queue: 2, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets              :               3468606
    Bytes                :            2664801792
    Tail-dropped packets :                      0
Queue: 3, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                     4
    Bytes                :                  1408
    Tail-dropped packets :                      0
Queue: 8, Forwarding classes: mcast-be, mcast-be
  Queued:
  Transmitted:
    Packets              :               1155541
    Bytes                :             591378902
    Tail-dropped packets :                      0
Queue: 9, Forwarding classes: mcast-ef
  Queued:
```

Verifying the CoS Configuration in the Aggregation Layer

Purpose Verify that CoS is configured correctly on the EX4550 Virtual Chassis in the aggregation layer.

Action Perform the following steps on the EX4550 Virtual Chassis:

1. Verify that the correct DSCP code points have been configured.

```
user@cs-agg-01> show class-of-service classifier name dscp_ba
rClassifier: dscp_ba, Code point type: dscp, Index: 12806
  Code point         Forwarding class                  Loss priority
  000000             Best-Effort                       low
  001010             Mission-Critical                  low
  010010             Video                             low
  101110             Voice                             low
  110000             Network-Control                   low
```

   The DSCP code points are displayed in binary. Table 27 on page 156 shows the binary representation of the DSCP code points used in this configuration example.

Table 27: Binary Representation of Code Points

Forwarding Class	DSCP Code Point	Binary Representation
Network-Control	NC1	110000
Voice	EF	101110
Video mcast-be	AF21	010010
Mission-Critical	AF11	001010
Best-Effort	BE	000000

2. Verify that the class-of-service queues on the aggregated Ethernet interfaces connecting the access switches are correct and that the queues are forwarding traffic.

NOTE: On the EX4550 switches, queue information is not directly available for aggregated Ethernet interfaces. To verify the class-of-service queues for an aggregated Ethernet interface, you must display the queues for the member interfaces themselves.

```
user@cs-agg-01> show interfaces queue xe-1/0/30
Physical interface: xe-1/0/30, Enabled, Physical link is Up
  Interface index: 157, SNMP ifIndex: 524
Forwarding classes: 16 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :             20885472
    Bytes                :          10749056256
    Tail-dropped packets :                    0
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
```

```
    Packets              :              41783554
    Bytes                :           32260131848
    Tail-dropped packets :                     0
Queue: 3, Forwarding classes: Video
  Queued:
  Transmitted:
    Packets              :              12530559
    Bytes                :            6515890680
    Tail-dropped packets :                     0
Queue: 5, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets              :               5569137
    Bytes                :             690572988
    Tail-dropped packets :                     0
Queue: 7, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                  1201
    Bytes                :                140129
    Tail-dropped packets :                     0
```

3. Verify that the class-of-service queues on the interfaces going to the core switches (xe-0/0/0 and xe-1/0/0) are correct and that the queues are forwarding traffic.

```
user@cs-agg-01> show interfaces queue xe-0/0/0
Physical interface: xe-0/0/0, Enabled, Physical link is Up
  Interface index: 167, SNMP ifIndex: 502
  Description: L3 link to core-sw1 (xe-0/1/0),ospf area 0
Forwarding classes: 16 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :               7961906
    Bytes                :            4124743780
    Tail-dropped packets :                     0
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets              :              15917818
    Bytes                :           10282911964
    Tail-dropped packets :                     0
Queue: 3, Forwarding classes: Video
  Queued:
  Transmitted:
    Packets              :                     0
    Bytes                :                     0
    Tail-dropped packets :                     0
Queue: 5, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets              :                     0
    Bytes                :                     0
    Tail-dropped packets :                     0
Queue: 7, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                 20811
    Bytes                :               1639950
    Tail-dropped packets :                     0
```

```
user@cs-agg-01> show interfaces queue xe-1/0/0

Physical interface: xe-1/0/0, Enabled, Physical link is Up
  Interface index: 156, SNMP ifIndex: 522
  Description: L3 link to core-sw2 (xe-0/1/0),ospf area 0
Forwarding classes: 16 supported, 5 in use
Egress queues: 8 supported, 5 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
  Transmitted:
    Packets              :                 2972
    Bytes                :               245303
    Tail-dropped packets :                    0
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
  Transmitted:
    Packets              :                    0
    Bytes                :                    0
    Tail-dropped packets :                    0
Queue: 3, Forwarding classes: Video
  Queued:
  Transmitted:
    Packets              :                    0
    Bytes                :                    0
    Tail-dropped packets :                    0
Queue: 5, Forwarding classes: Voice
  Queued:
  Transmitted:
    Packets              :             21322481
    Bytes                :           2786137520
    Tail-dropped packets :                    0
Queue: 7, Forwarding classes: Network-Control
  Queued:
  Transmitted:
    Packets              :                20911
    Bytes                :              1645559
    Tail-dropped packets :                    0
```

4. Verify the network scheduler map configuration.

```
user@cs-agg-01> show class-of-service scheduler-map network-port-sched
Scheduler map: network-port-sched, Index: 47308

  Scheduler: be-sched, Forwarding class: Best-Effort, Index: 13005
    Transmit rate: remainder, Rate Limit: none, Buffer size: remainder, Buffer
 Limit: none,
    Priority: low
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      High            non-TCP         1    <default-drop-profile>
      High            TCP             1    <default-drop-profile>

  Scheduler: voice-network-sched, Forwarding class: Voice, Index: 14983
    Transmit rate: remainder, Rate Limit: none, Buffer size: 5 percent, Buffer
 Limit: none,
    Priority: strict-high
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      High            non-TCP         1    <default-drop-profile>
      High            TCP             1    <default-drop-profile>
```

```
 Scheduler: mission-critical-sched, Forwarding class: Mission-Critical, Index:
49903
   Transmit rate: 40 percent, Rate Limit: none, Buffer size: 40 percent,
Buffer Limit: none,
   Priority: low
   Excess Priority: unspecified
   Drop profiles:
     Loss priority   Protocol    Index    Name
     High            non-TCP         1    <default-drop-profile>
     High            TCP             1    <default-drop-profile>

 Scheduler: control-network-sched, Forwarding class: Network-Control, Index:
48571
   Transmit rate: remainder, Rate Limit: none, Buffer size: 5 percent, Buffer
Limit: none,
   Priority: strict-high
   Excess Priority: unspecified
   Drop profiles:
     Loss priority   Protocol    Index    Name
     High            non-TCP         1    <default-drop-profile>
     High            TCP             1    <default-drop-profile>

 Scheduler: video-sched, Forwarding class: Video, Index: 63266
   Transmit rate: 20 percent, Rate Limit: none, Buffer size: 20 percent,
Buffer Limit: none,
   Priority: low
   Excess Priority: unspecified
   Drop profiles:
     Loss priority   Protocol    Index    Name
     High            non-TCP         1    <default-drop-profile>
     High            TCP             1    <default-drop-profile>
```

5. Verify the forwarding classes configured on the aggregation switch.

```
user@cs-agg-01> show class-of-service forwarding-class
root@# run show class-of-service forwarding-class
Forwarding class                  ID                      Queue  Policing
priority    SPU priority
  Best-Effort                             0                       0
 normal           low
  Voice                                   1                       5
 normal           low
  Mission-Critical                        2                       1
 normal           low
  Network-Control                         3                       7
 normal           low
  Video                                   4                       3
 normal           low
```

Verifying the CoS Configuration on the Core Switches

Purpose Verify that CoS is configured correctly on the EX9214 switches in the core layer.

Action Perform the following steps on the EX9214 switches:

1. Verify that the correct DSCP code points have been configured.

```
user@cs-core-sw01-1> show class-of-service classifier name dscp_ba

root@cs-core-sw01-1# run show class-of-service classifier name dscp_ba
Classifier: dscp_ba, Code point type: dscp, Index: 12806
  Code point         Forwarding class                  Loss priority
  000000             Best-Effort                       low
  001010             Mission-Critical                  low
  010010             Video                             low
  101110             Voice                             low
  110000             Network-Control                   low
```

   The DSCP code points are displayed in binary. Table 28 on page 160 shows the binary representation of the DSCP code points used in this configuration example.

Table 28: Binary Representation of Code Points

Forwarding Class	DSCP Code Point	Binary Representation
Network-Control	NC1	110000
Voice	EF	101110
Video mcast-be	AF21	010010
Mission-Critical	AF11	001010
Best-Effort	BE	000000

2. Verify that the network-port-sched scheduler map and the dscp_ba classifier are active on interfaces.

   - An example of doing so for an aggregated Ethernet interface:

```
user@cs-core-sw01-1> show class-of-service interface ae1
Physical interface: ae1, Index: 129
Queues supported: 8, Queues in use: 6
  Scheduler map: network-port-sched, Index: 47308
  Congestion-notification: Disabled

  Logical interface: ae1.0, Index: 328
Object                 Name                 Type                 Index
Classifier             dscp_ba              dscp                 12806
```

   - An example of doing so for a physical interface:

```
user@cs-core-sw01-1> show class-of-service interface xe-0/1/0
Physical interface: xe-0/1/0, Index: 276
Queues supported: 8, Queues in use: 6
  Scheduler map: network-port-sched, Index: 47308
  Congestion-notification: Disabled

  Logical interface: xe-0/1/0.0, Index: 437
```



```
Object                  Name                    Type                    Index
Classifier              dscp_ba                 dscp                    12806
```

- An example of doing so for an IRB interface:

```
user@cs-core-sw01-1> show class-of-service interface irb.60
  Logical interface: irb.60, Index: 363
Object                  Name                    Type                    Index
Classifier              dscp_ba                 dscp                    12806
```

3. Verify the network scheduler map configuration.

```
user@cs-core-sw01-1> show class-of-service scheduler-map network-port-sched
Scheduler map: network-port-sched, Index: 47308

  Scheduler: be-sched, Forwarding class: Best-Effort, Index: 13005
    Transmit rate: remainder, Rate Limit: none, Buffer size: remainder, Buffer
 Limit: none,
    Priority: low
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium low      any             1    <default-drop-profile>
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>

  Scheduler: mission-critical-sched, Forwarding class: Mission-Critical, Index:
 49903
    Transmit rate: 40 percent, Rate Limit: none, Buffer size: 40 percent,
Buffer Limit: none,
    Priority: low
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium low      any             1    <default-drop-profile>
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>

  Scheduler: video-sched, Forwarding class: Video, Index: 63266
    Transmit rate: 20 percent, Rate Limit: none, Buffer size: 20 percent,
Buffer Limit: none,
    Priority: low
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium low      any             1    <default-drop-profile>
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>

  Scheduler: control-network-sched, Forwarding class: Network-Control, Index:
 48571
    Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent, Buffer
 Limit: none,
    Priority: low
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium low      any             1    <default-drop-profile>
```

```
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>

  Scheduler: voice-network-sched, Forwarding class: Voice, Index: 14983
    Transmit rate: unspecified, Rate Limit: none, Buffer size: 5 percent,
Buffer Limit: none,
    Priority: strict-high
    Excess Priority: unspecified
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium low      any             1    <default-drop-profile>
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>
```

4. Verify the forwarding classes configured on the core switch.

```
user@cs-core-sw01-1> show class-of-service forwarding-class
Forwarding class                          ID      Queue  Restricted queue  Fabric
 priority  Policing priority   SPU priority
  Best-Effort                              0       0          0             low
              normal            low
  Mission-Critical                         1       1          1             low
              normal            low
  assured-forwarding                       2       2          2             low
              normal            low
  Video                                    3       3          3             low
              normal            low
  Network-Control                          4       7          3             low
              normal            low
  Voice                                    5       5          1             high
              normal            low
```

5. Verify that the class-of-service queues the MC-LAG interfaces going to the access switches are correct and that the queues are forwarding traffic.

```
user@cs-core-sw01-1> show interfaces queue ae1 egress
Physical interface: ae1 (MC-AE-1, active), Enabled, Physical link is Up
  Interface index: 129, SNMP ifIndex: 710
  Description: Layer 2 MCLAG between core & AB1,xe-0/0/0,1/0/0
Forwarding classes: 16 supported, 6 in use
Egress queues: 8 supported, 6 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
    Packets              :             12682705                30081 pps
    Bytes                :           6786600578             128781152 bps
  Transmitted:
    Packets              :             12682705                30081 pps
    Bytes                :           6786600578             128781152 bps
    Tail-dropped packets :                    0                    0 pps
    RL-dropped packets   :                    0                    0 pps
    RL-dropped bytes     :                    0                    0 bps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
```

```
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
    Packets              :              71755144               170223 pps
    Bytes                :           65477965504            1242662496 bps
  Transmitted:
    Packets              :              71755144               170223 pps
    Bytes                :           65477965504            1242662496 bps
    Tail-dropped packets :                     0                    0 pps
    RL-dropped packets   :                     0                    0 pps
    RL-dropped bytes     :                     0                    0 bps
    RED-dropped packets  :                     0                    0 pps
     Low                 :                     0                    0 pps
     Medium-low          :                     0                    0 pps
     Medium-high         :                     0                    0 pps
     High                :                     0                    0 pps
    RED-dropped bytes    :                     0                    0 bps
     Low                 :                     0                    0 bps
     Medium-low          :                     0                    0 bps
     Medium-high         :                     0                    0 bps
     High                :                     0                    0 bps
Queue: 2, Forwarding classes: assured-forwarding
  Queued:
    Packets              :                     0                    0 pps
    Bytes                :                     0                    0 bps
  Transmitted:
    Packets              :                     0                    0 pps
    Bytes                :                     0                    0 bps
    Tail-dropped packets :                     0                    0 pps
    RL-dropped packets   :                     0                    0 pps
    RL-dropped bytes     :                     0                    0 bps
    RED-dropped packets  :                     0                    0 pps
     Low                 :                     0                    0 pps
     Medium-low          :                     0                    0 pps
     Medium-high         :                     0                    0 pps
     High                :                     0                    0 pps
    RED-dropped bytes    :                     0                    0 bps
     Low                 :                     0                    0 bps
     Medium-low          :                     0                    0 bps
     Medium-high         :                     0                    0 bps
     High                :                     0                    0 bps
Queue: 3, Forwarding classes: Video
  Queued:
    Packets              :              21137103                50135 pps
    Bytes                :           11311148184            214642528 bps
  Transmitted:
    Packets              :              21137103                50135 pps
    Bytes                :           11311148184            214642528 bps
    Tail-dropped packets :                     0                    0 pps
    RL-dropped packets   :                     0                    0 pps
    RL-dropped bytes     :                     0                    0 bps
    RED-dropped packets  :                     0                    0 pps
     Low                 :                     0                    0 pps
     Medium-low          :                     0                    0 pps
     Medium-high         :                     0                    0 pps
     High                :                     0                    0 pps
    RED-dropped bytes    :                     0                    0 bps
     Low                 :                     0                    0 bps
     Medium-low          :                     0                    0 bps
     Medium-high         :                     0                    0 bps
     High                :                     0                    0 bps
Queue: 5, Forwarding classes: Voice
```

```
  Queued:
    Packets              :             10126420                24028 pps
    Bytes                :           1498710160             28449600 bps
  Transmitted:
    Packets              :             10126420                24028 pps
    Bytes                :           1498710160             28449600 bps
    Tail-dropped packets :                    0                    0 pps
    RL-dropped packets   :                    0                    0 pps
    RL-dropped bytes     :                    0                    0 bps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
Queue: 7, Forwarding classes: Network-Control
  Queued:
    Packets              :                   93                    0 pps
    Bytes                :                13742                  672 bps
  Transmitted:
    Packets              :                   93                    0 pps
    Bytes                :                13742                  672 bps
    Tail-dropped packets :                    0                    0 pps
    RL-dropped packets   :                    0                    0 pps
    RL-dropped bytes     :                    0                    0 bps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
     Medium-low          :                    0                    0 pps
     Medium-high         :                    0                    0 pps
     High                :                    0                    0 pps
    RED-dropped bytes    :                    0                    0 bps
     Low                 :                    0                    0 bps
     Medium-low          :                    0                    0 bps
     Medium-high         :                    0                    0 bps
     High                :                    0                    0 bps
```

6. Verify that the class-of-service queues on the interfaces going to the aggregation switch are correct and that the queues are forwarding traffic.

```
user@cs-core-sw01-1> show interfaces queue xe-0/1/0 egress
Physical interface: xe-0/1/0, Enabled, Physical link is Up
  Interface index: 276, SNMP ifIndex: 681
  Description: L3 link to agg (xe-0/0/0),ospf area 0
Forwarding classes: 16 supported, 6 in use
Egress queues: 8 supported, 6 in use
Queue: 0, Forwarding classes: Best-Effort
  Queued:
    Packets              :             24873844                49973 pps
    Bytes                :          13232672656             212681696 bps
  Transmitted:
    Packets              :             24873844                49973 pps
    Bytes                :          13232672656             212681696 bps
    Tail-dropped packets :                    0                    0 pps
    RL-dropped packets   :                    0                    0 pps
    RL-dropped bytes     :                    0                    0 bps
    RED-dropped packets  :                    0                    0 pps
     Low                 :                    0                    0 pps
```

```
      Medium-low          :                    0                    0 pps
      Medium-high         :                    0                    0 pps
      High                :                    0                    0 pps
     RED-dropped bytes    :                    0                    0 bps
      Low                 :                    0                    0 bps
      Medium-low          :                    0                    0 bps
      Medium-high         :                    0                    0 bps
      High                :                    0                    0 bps
Queue: 1, Forwarding classes: Mission-Critical
  Queued:
    Packets               :             64688790               129965 pps
    Bytes                 :          48432345528            778435680 bps
  Transmitted:
    Packets               :             64688790               129965 pps
    Bytes                 :          48432345528            778435680 bps
    Tail-dropped packets  :                    0                    0 pps
    RL-dropped packets    :                    0                    0 pps
    RL-dropped bytes      :                    0                    0 bps
    RED-dropped packets   :                    0                    0 pps
     Low                  :                    0                    0 pps
     Medium-low           :                    0                    0 pps
     Medium-high          :                    0                    0 pps
     High                 :                    0                    0 pps
    RED-dropped bytes     :                    0                    0 bps
     Low                  :                    0                    0 bps
     Medium-low           :                    0                    0 bps
     Medium-high          :                    0                    0 bps
     High                 :                    0                    0 bps
Queue: 2, Forwarding classes: assured-forwarding
  Queued:
    Packets               :                    0                    0 pps
    Bytes                 :                    0                    0 bps
  Transmitted:
    Packets               :                    0                    0 pps
    Bytes                 :                    0                    0 bps
    Tail-dropped packets  :                    0                    0 pps
    RL-dropped packets    :                    0                    0 pps
    RL-dropped bytes      :                    0                    0 bps
    RED-dropped packets   :                    0                    0 pps
     Low                  :                    0                    0 pps
     Medium-low           :                    0                    0 pps
     Medium-high          :                    0                    0 pps
     High                 :                    0                    0 pps
    RED-dropped bytes     :                    0                    0 bps
     Low                  :                    0                    0 bps
     Medium-low           :                    0                    0 bps
     Medium-high          :                    0                    0 bps
     High                 :                    0                    0 bps
Queue: 3, Forwarding classes: Video
  Queued:
    Packets               :              5374296                10759 pps
    Bytes                 :           3188679882             50845920 bps
  Transmitted:
    Packets               :              5374296                10759 pps
    Bytes                 :           3188679882             50845920 bps
    Tail-dropped packets  :                    0                    0 pps
    RL-dropped packets    :                    0                    0 pps
    RL-dropped bytes      :                    0                    0 bps
    RED-dropped packets   :                    0                    0 pps
     Low                  :                    0                    0 pps
     Medium-low           :                    0                    0 pps
```

```
      Medium-high         :                    0                    0 pps
      High                :                    0                    0 pps
     RED-dropped bytes    :                    0                    0 bps
      Low                 :                    0                    0 bps
      Medium-low          :                    0                    0 bps
      Medium-high         :                    0                    0 bps
      High                :                    0                    0 bps
Queue: 5, Forwarding classes: Voice
  Queued:
    Packets               :              7959018                15990 pps
    Bytes                 :           1146098592             18421408 bps
  Transmitted:
    Packets               :              7959018                15990 pps
    Bytes                 :           1146098592             18421408 bps
    Tail-dropped packets  :                    0                    0 pps
    RL-dropped packets    :                    0                    0 pps
    RL-dropped bytes      :                    0                    0 bps
    RED-dropped packets   :                    0                    0 pps
     Low                  :                    0                    0 pps
     Medium-low           :                    0                    0 pps
     Medium-high          :                    0                    0 pps
     High                 :                    0                    0 pps
    RED-dropped bytes     :                    0                    0 bps
     Low                  :                    0                    0 bps
     Medium-low           :                    0                    0 bps
     Medium-high          :                    0                    0 bps
     High                 :                    0                    0 bps
Queue: 7, Forwarding classes: Network-Control
  Queued:
    Packets               :                    0                    0 pps
    Bytes                 :                    0                    0 bps
  Transmitted:
    Packets               :                    0                    0 pps
    Bytes                 :                    0                    0 bps
    Tail-dropped packets  :                    0                    0 pps
    RL-dropped packets    :                    0                    0 pps
    RL-dropped bytes      :                    0                    0 bps
    RED-dropped packets   :                    0                    0 pps
     Low                  :                    0                    0 pps
     Medium-low           :                    0                    0 pps
     Medium-high          :                    0                    0 pps
     High                 :                    0                    0 pps
    RED-dropped bytes     :                    0                    0 bps
     Low                  :                    0                    0 bps
     Medium-low           :                    0                    0 bps
     Medium-high          :                    0                    0 bps
     High                 :                    0                    0 bps
```

Related Documentation

- Understanding the Benefits of the Midsize Enterprise Campus Solution on page 6
- Example: Configuring High Availability for the Midsize Enterprise Campus on page 39
- Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus on page 85
- Example: Configuring Access Policy and Security for the Midsize Enterprise Campus on page 114

Known Issues

There were several persistent issues in testing that caused the test results to fall outside of the solution requirements. These issues include:

- On EX4300 switches, enabling IP source guard on data VLANs causes traffic on the voice VLAN to not be sent to other ports. Disabling IP source guard on the data VLANs resolves this issue. (PR 1001232)
- On EX4300 switches, when the 802.1X supplicant mode is multiple mode, DHCP messages are sent to the VLAN assigned to the port rather than to the VLAN dynamically assigned through 802.1X authentication. (PR 1005276)
- On EX4300 switches, the multifield classifier that is applied to the client VLANs sometimes stops classifying traffic after you reboot the switch. To correct this issue if it occurs, delete the multifield classifier and then recreate it. (PR 1008646).
- On the EX4550 Virtual Chassis, when the master is powered down, packets are dropped for 3 seconds, even when there are a low number of routes. (PR 1009531)
- On the SRX650 gateways, when a link on which BFD is configured goes down, BFD sessions on all links can go down. This happens when the BFD timer is configured for a short duration (for example, 1000 ms). The problem does not occur with longer BFD timers (for example, 7.5 seconds.) (PR 1010748)
- Although EX4300 switches support four multicast queues, traffic is always sent to the mcast-be queue regardless of the CoS configuration on the switch. For this reason, this solution configured all multicast traffic to be sent to the mcast-be queue on EX4300 switches. (PR 824525)

Related Documentation

- Understanding the Benefits of the Midsize Enterprise Campus Solution on page 6
- Example: Configuring High Availability for the Midsize Enterprise Campus on page 39
- Example: Configuring Layer 2 and Layer 3 Network Services for the Midsize Enterprise Campus on page 85
- Example: Configuring Access Policy and Security for the Midsize Enterprise Campus on page 114
- Example: Configuring Class of Service for the Midsize Enterprise Campus on page 137