Junos® OS

Multichassis Link Aggregation Feature Guide for EX Series, MX Series, and QFX Series Devices

Release
13.2

Modified: 2016-06-08

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

Junos® OS Multichassis Link Aggregation Feature Guide for EX Series, MX Series, and QFX Series Devices
13.2

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

Part 3 Troubleshooting

Part 4 Configuration Statements and Operational Commands

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series
- QFX Series standalone switches
- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```


2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   [edit]
   user@host# **edit system scripts**
   [edit system scripts]

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   [edit system scripts]
   user@host# **load merge relative /var/tmp/ex-script-snippet.conf**
   load complete

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		    route default {
		      nexthop *address*;
		      retain;
		    }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Understanding Multichassis Link Aggregation Groups

Multichassis Link Aggregation Overview

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Layer 2 networks are increasing in scale mainly because of technologies such as virtualization. Protocol and control mechanisms that limit the disastrous effects of a topology loop in the network are necessary. The Spanning Tree Protocol (STP) is the primary solution to this problem because it provides a loop-free Layer 2 environment. STP has gone through a number of enhancements and extensions, and even though it scales to very large network environments, it still only provides one active path from one device to another, regardless of how many actual connections might exist in the network. Although STP is a robust and scalable solution to redundancy in a Layer 2 network, the single logical link creates two problems: At least half of the available system bandwidth is off-limits to data traffic, and network topology changes occur. Rapid Spanning Tree Protocol (RSTP) reduces the overhead of the rediscovery process and allows a Layer 2 network to reconverge faster, but the delay is still high.

Link aggregation (IEEE 802.3ad) solves some of these problems by enabling users to use more than one link connection between switches. All physical connections are considered one logical connection. The problem with standard link aggregation is that the connections are point to point.

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two MC-LAG peers. An MC-LAG provides redundancy and load balancing between the two MC-LAG peers, multihoming support, and a loop-free Layer 2 network without running STP.

On one end of an MC-LAG, there is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device uses the link as a LAG. On the other side of the MC-LAG, there are two MC-LAG peers. Each of the MC-LAG peers has one or more physical links connected to a single client device.

The MC-LAG peers use Inter-Chassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly.

Link Aggregation Control Protocol (LACP) is a subcomponent of the IEEE 802.3ad standard. LACP is used to discover multiple links from a client device connected to an MC-LAG peer. LACP must be configured on both MC-LAG peers for an MC-LAG to work correctly.

NOTE: You must specify a service identifier (service-id) for each multichassis aggregated Ethernet interface that belongs to a LAG; otherwise, multichassis link aggregation will not work.

• Features Supported on the EX Series, MX Series, and QFX Series on page 4

Features Supported on the EX Series, MX Series, and QFX Series

Table 3 on page 4 lists the MC-LAG features supported on the EX Series, MX Series, and the QFX Series.

Table 3: Feature Support on the EX Series, MX Series, and QFX Series

Features	EX4300 Device	EX4600 Device	EX9200 Device	MX Series Devices	QFX Series Devices
Active-active bridging domain	Not supported	Not supported	Not supported	Supported	Not supported
Active-active mode	Supported	Supported	Supported	Supported	Supported
Active-standby mode	Not supported	Not supported	Supported	Supported	Not supported
Address Resolution Protocol (ARP) synchronization	Supported	Supported	Supported	Supported	Supported
Dynamic Host Control Protocol (DHCP) relay	Supported	Supported	Supported	Supported	Supported
Inter-Chassis Control Protocol (ICCP) and Inter-Chassis link (ICL)	Supported	Supported	Supported	Supported	Supported
Internet Group Management Protocol (IGMP)	Supported	Supported	Supported	Supported	Supported
IGMP snooping	Supported	Supported	Supported	Supported	Supported
Layer 2 circuit functions	Not supported	Not supported	Supported	Not supported	Supported
Link Aggregation Control Protocol (LACP)	Supported	Supported	Supported	Supported	Supported

Table 3: Feature Support on the EX Series, MX Series, and QFX Series *(continued)*

Features	EX4300 Device	EX4600 Device	EX9200 Device	MX Series Devices	QFX Series Devices
Media access control (MAC) management	Supported	Supported	Supported	Supported	Supported
MAC address synchronization	Supported	Supported	Not supported	Supported	Supported
Multichassis link protection	Supported	Supported	Supported	Supported	Supported
Protocol Independent Multicast (PIM)	Supported	Supported	Supported	Supported	Supported
Pseudowire status type	Not supported	Not supported	Not supported	Not supported	Supported
Virtual private LAN service (VPLS)	Not supported	Not supported	Supported in active-standby mode only	Supported in active-standby mode only	Not supported
Virtual Router Redundancy Protocol (VRRP)	Supported	Supported	Supported	Supported	Supported

Related Documentation

- Configuring Multichassis Link Aggregation for EX Series on page 32
- Configuring Multichassis Link Aggregation for MX Series on page 27
- Configuring Multichassis Link Aggregation for QFX Series on page 35

Multichassis Link Aggregation Guidelines

Supported Platforms EX Series, MX Series, QFX Series standalone switches

This topic provides configuration guidelines and information regarding the functional behavior of multichassis link aggregation.

MC-LAG Configuration Guidelines and Functional Behavior

When you configure MC-LAGs, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from the MC-LAG feature.

Table 4 on page 6 provides best practice configuration guidelines for MC-LAGs, and Table 5 on page 7 describes important functional behavior for MC-LAGs.

Table 4: MC-LAG Configuration Guidelines

We recommend that you use separate ports and choose different FPCs for the interchassis link (ICL) and Inter-Chassis Control Protocol (ICCP) interfaces.
On QFX Series switches and EX9200 switches, we recommend that you configure the backup liveness detection feature to implement faster failover of data traffic during an MC-LAG peer reboot. Configure the backup-liveness-detection statement on the management interface (fxp0) only. The backup liveness detection should be set to greater than or equal to 1 second on a QFX5100 switch. NOTE: On EX9200 switches, the backup-liveness-detection statement was added in Junos OS Release 13.2R1.
The following two methods can be used to enable Layer 3 functionality across an MC-LAG. We recommend that you use the Virtual Router Redundancy Protocol (VRRP) over integrated routing and bridging (IRB) interfaces method. Use media access control (MAC) address synchronization only when you cannot configure VRRP over IRB. NOTE: On QFX Series switches, you cannot configure both VRRP over IRB and MAC synchronization, because processing MAC addresses might not work. • Configure different IP addresses on IRB interfaces and run VRRP over the IRB interfaces. The virtual IP address is the gateway IP address for the MC-LAG clients. • Configure the MAC address synchronization feature using either the **set vlans *vlan-name* mcae-mac-synchronize** or **set bridge-domains *name* mcae-mac-synchronize** command and configure the same IP address on each of the IRBs on the MC-LAG peers. This IP address is the gateway IP address for the MC-LAG clients.
You must configure the ICL interface as a router-facing interface (by configuring the *multicast-router-interface* statement) for multicast forwarding to work in an MC-LAG environment.
You must configure the **multichassis-lag-replicate-state** statement for Internet Group Management Protocol (IGMP) snooping to work properly in an MC-LAG environment.
You must enable Protocol Independent Multicast (PIM) on the IRB interface to avoid multicast duplication.
If you are using Layer 3 multicast, configure the IP address on the active MC-LAG peer with a high IP address or a high designated router priority.
NOTE: Use this configuration guideline only if you can ensure that the ICCP will not go down unless the router or switch is down. You can configure the **prefer-status-control-active** statement with the mc-ae **status-control standby** configuration to prevent the LACP MC-LAG system ID from reverting to the default Link Aggregation Control Protocol (LACP) system ID on ICCP failure. You must also configure the **hold-time down** value (at the **[edit interfaces *interface-name*]** hierarchy level) for the ICL with the mc-ae **status-control standby** configuration to be higher than the ICCP Bidirectional Forwarding Detection (BFD) timeout. This configuration prevents data traffic loss by ensuring that when the router or switch with the mc-ae **status-control active** configuration goes down, the router or switch with the mc-ae **status-control standby** configuration does not go into standby mode. To make the **prefer-status-control-active** configuration work with the mc-ae **status-control standby** configuration when an ICL logical interface is configured on an aggregated Ethernet interface, you must either configure the ***lacp* periodic interval** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level as slow or configure the **detection-time threshold** statement at the **[edit protocols iccp peer *liveness-detection*]** hierarchy level as less than 3 seconds. NOTE: On EX9200 switches, the **prefer-status-control-active** statement was added in Junos OS Release 13.2R1.

Table 4: MC-LAG Configuration Guidelines *(continued)*

We recommend that you configure the ICCP liveness-detection interval to be at least 8 seconds, to allow graceful Routing Engine switchover to work seamlessly. By default, ICCP liveness detection uses multihop BFD, which runs in centralized mode. If you have configured ICCP connectivity through a dedicated physical interface rather than through an IRB interface, then you can configure single-hop BFD, and the restriction on the the liveness-detection interval does not apply.
We recommend that you configure only one redundancy group between MC-LAG nodes. The redundancy group represents the domain of high availability between the MC-LAG nodes. One redundancy group is sufficient between a pair of MC-LAG nodes.

Table 5: MC-LAG Functional Behavior

STP is not supported on the ICL or MC-LAG interfaces.
Load balancing of network traffic between MC-LAG peers is 100 percent local bias.
Load balancing of network traffic between multiple LAG members in a local MC-LAG node is achieved through a standard LAG hashing algorithm.
MAC learning is disabled on the ICL. Consequently, source MAC addresses cannot be learned locally on the ICL. However, MAC addresses from a remote MC-LAG node can be installed on the ICL interface. For example, the MAC address for a single-homed client on a remote MC-LAG node can be installed on the ICL interface of the local MC-LAG node.
Dynamic Address Resolution Protocol (ARP) resolution over the ICL interface is not supported. Consequently, incoming address resolution protocol replies on the ICL are discarded. However, ARP entries can be populated on the ICL interface through ICCP exchanges from a remote MC-LAG peer.
For EX9200 switches, ARP entries that were learned remotely are purged and then learned again during GRES.
Usually, a VRRP backup node does not forward incoming packets. However, when VRRP over IRB is configured in an MC-LAG active-active environment, both the VRRP master and the VRRP backup forward Layer 3 traffic arriving on the multichassis aggregated Ethernet interface.
If you are using the MAC address synchronization method (by configuring either the **set vlans *vlan-name* mcae-mac-synchronize** or **set bridge-domains *name* mcae-mac-synchronize** command) to enable Layer 3 functionality, running routing protocols over the IRB interface is not supported, and gratuitous ARP requests are not sent when the MAC address on the IRB interface changes.
Access port security features (for example, DHCP snooping, dynamic ARP inspection (DAI), and IP source guard) are not supported on the ICL or MC-LAG interfaces.

Spanning Tree Protocol Guidelines

- Enable Spanning Tree Protocol globally.

  STP might detect local miswiring loops within the peer or across MC-LAG peers.

  STP might not detect network loops introduced by MC-LAG peers.
- Disable STP on ICL links; otherwise, STP might block ICL interfaces and disable protection.
- Do not enable bridge protocol data unit (BPDU) block on interfaces connected to aggregation switches.

For more information about BPDU block, see *Understanding BPDU Protection for STP, RSTP, and MSTP*.

MC-LAG Upgrade Guidelines

Upgrade the MC-LAG peers according to the following guidelines.

NOTE: After a reboot, the multichassis aggregated Ethernet interfaces come up immediately and might start receiving packets from the server. If routing protocols are enabled, and the routing adjacencies have not been formed, packets might be dropped.

To prevent this scenario, issue the **set interfaces *interface-name* aggregated-ether-options mc-ae init-delay-time *time*** command to set a time by which the routing adjacencies are formed. The **init-delay-time** should be set to greater than or equal to 240 seconds on a QFX5100 switch.

1. Make sure that both of the MC-LAG peers (node1 and node2) are in the active-active state using the following command on any one of the MC-LAG peers:

```
user@switch> show interfaces mc-ae id 1
Member Link                  : ae0
 Current State Machine's State: mcae active state
 Local Status                 : active<<<<<<<
 Local State                  : up
 Peer Status                  : active<<<<<<<
 Peer State                   : up
     Logical Interface        : ae0.0
     Topology Type            : bridge
     Local State              : up
     Peer State               : up
     Peer Ip/MCP/State        : 20.1.1.2 ae2.0 up
```

2. Upgrade node1 of the MC-LAG.

   When node1 is upgraded, it is rebooted, and all traffic is sent across the available LAG interfaces of node2, which is still up. The amount of traffic lost depends on how quickly the neighbor devices detect the link loss and rehash the flows of the LAG.

3. Verify that node1 is running the software you just installed by issuing the **show version** command.

4. Make sure that both nodes of the MC-LAG (node1 and node2) are in the active-active state after the reboot of node1.

5. Upgrade node2 of the MC-LAG.

   Repeat Step 1 through Step 3 to upgrade node2.

Related Documentation

- Configuring Multichassis Link Aggregation for EX Series on page 32
- Configuring Multichassis Link Aggregation for MX Series on page 27
- Configuring Multichassis Link Aggregation for QFX Series on page 35

Multichassis Link Aggregation Terms and Features

Supported Platforms EX Series, MX Series, QFX Series standalone switches

The following sections provide an overview of the terms and features associated with MC-LAG:

Active-Active and Active-Standby Modes

In active-active mode, all member links are active on the MC-LAG. In this mode, media access control (MAC) addresses learned on one MC-LAG peer are propagated to the other MC-LAG peer.

In active-standby mode, only one of the MC-LAG peers is active at any given time. The other MC-LAG peer is in backup (standby) mode. The active MC-LAG peer uses Link Aggregation Control Protocol (LACP) to advertise to client devices that its child link is available for forwarding data traffic.

NOTE: Active-standby mode is not supported on QFX Series switches and the EX4300 switch.

ICCP and ICL

The MC-LAG peers uses Inter-Chassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly. ICCP replicates control traffic and forwarding states across the MC-LAG peers and communicates the operational state of the MC-LAG members. Because ICCP uses TCP/IP to communicate between the peers, the two peers must be connected to each other. ICCP messages exchange MC-LAG configuration parameters and ensure that both peers use the correct LACP parameters.

The interchassis link (ICL), also known as the interchassis link-protection link (ICL-PL), is used to forward data traffic across the MC-LAG peers. This link provides redundancy when a link failure (for example, an MC-LAG trunk failure) occurs on one of the active links. The ICL can be a single physical Ethernet interface or an aggregated Ethernet interface. You can configure only one ICL between the two MC-LAG peers, although you can configure multiple MC-LAGs between them.

LACP

LACP is a subcomponent of the IEEE 802.3ad standard. LACP is used to discover multiple links from a client device connected to an MC-LAG peer. LACP must be configured on all member links for an MC-LAG to work correctly.

Data Traffic Forwarding Rules

In active-active MC-LAG topologies, network interfaces are categorized into three interface types, as follows:

- S-Links—Single-homed link (S-Link) terminating on an MC-LAG peer device
- MC-Links—MC-LAG links
- ICL—Inter-chassis link

Depending on the incoming and outgoing interface types, some constraints are added to the Layer 2 forwarding rules for MC-LAG configurations. The following data traffic forwarding rules apply.

NOTE: If only one MC-LAG member link is in the up state, it is considered an S-Link.

- When an MC-LAG network receives a packet from a local MC-Link or S-Link, the packet is forwarded to other local interfaces, including S-Links and MC-Links based on the normal Layer 2 forwarding rules and on the configuration of the **mesh-group** and **no-local-switching** statements. If MC-Links and S-Links are in the same mesh group and their **no-local-switching** statements are enabled, the received packets are only forwarded upstream and not sent to MC-Links and S-Links.

- The following circumstances determine whether or not an ICL receives a packet from a local MC-Link or S-Link:
  - If the peer MC-LAG network device has S-Links or MC-LAGs that do not reside on the local MC-LAG network device
  - Whether or not interfaces on two peering MC-LAG network devices are allowed to talk to each other
- When an MC-LAG network receives a packet from the ICL, the packet is forwarded to all local S-Links and active MC-LAGs that do not exist in the MC-LAG network from which the packet was sent.

Multichassis Link Protection

Multichassis link protection provides link protection between the two MC-LAG peers that host an MC-LAG. If the ICCP connection is up and the ICL comes up, the peer configured as standby brings up the multichassis aggregated Ethernet interfaces shared with the peer. Multichassis protection must be configured on each MC-LAG peer that is hosting an MC-LAG.

Failure Handling

Configuring ICCP adjacency over aggregated links with child links on multiple FPCs mitigates the possibility of a split-brain state. A split-brain occurs when ICCP adjacency is lost between the MC-LAG peers. To work around this problem, enable backup liveness detection. With backup liveness detection enabled, the MC-LAG peers establish an out-of-band channel through the management network in addition to the ICCP channel.

During a split-brain state, both active and standby peers change LACP system IDs. Because both MC-LAG peers change the LACP system ID, the customer edge (CE) device accepts the LACP system ID of the first link that comes up and brings down other links carrying different LACP system IDs. When the ICCP connection is active, both of the MC-LAG peers use the configured LACP system ID. If the LACP system ID is changed during failures, the server that is connected over the MC-LAG removes these links from the aggregated Ethernet bundle.

When the ICL is operationally down and the ICCP connection is active, the LACP state of the links with status control configured as standby is set to the standby state. When the LACP state of the links is changed to standby, the server that is connected over the MC-LAG makes these links inactive and does not use them for sending data.

Table 6 on page 12 describes the different ICCP failure scenarios. The dash means that the item is not applicable.

Table 6: ICCP Failure Scenarios

ICCP Connection Status	ICL Status	Backup Liveness Peer Status	Action on Multichassis Aggregated Ethernet Interface with Status Set to Standby
Down	Down or Up	Not configured	LACP system ID is changed to default value.
Down	Down or Up	Active	LACP system ID is changed to default value.
Down	Down or Up	Inactive	No change in LACP system ID.
Up	Down	–	LACP state is set to standby. MUX state moves to waiting state.

Configure the **master-only** statement on the IP address of the fxp0 interface for backup liveness detection, on both the master and backup Routing Engines, to ensure that the connection is not reset during GRES in the remote peer.

For example, on the master Routing Engine:

```
user@switch-re1 > show configuration interfaces fxp0 | display inheritance no-comments
unit 0 {
   family inet {
      address 10.8.2.31/24;
      address 10.8.2.33/24 {
         master-only;
      }
   }
}
```

For example, on the backup Routing Engine:

```
user@switch1-re1 > show configuration interfaces fxp0 | display inheritance no-comments
unit 0 {
   family inet {
      address 10.8.2.32/24;
      address 10.8.2.33/24 {
         master-only;
      }
   }
}
```

The master Routing Engine services both 10.8.2.31 and 10.8.2.33. Configure 10.8.2.33 in a backup-liveness-detection configuration on the peer node.

For example, on the backup Routing Engine:

```
user@switch2 > show configuration protocols iccp
local-ip-addr 2.2.2.2;
peer 1.1.1.1 {
   session-establishment-hold-time 50;
   redundancy-group-id-list 1;
   backup-liveness-detection {
      backup-peer-ip 10.8.2.33;
   }
```

```
    liveness-detection {
      minimum-interval 500;
      multiplier 3;
      single-hop;
    }
  }
```

Load Balancing

Load balancing of network traffic between MC-LAG peers is 100 percent local bias. Load balancing of network traffic between multiple LAG members in a local MC-LAG node is achieved through a standard LAG hashing algorithm.

Layer 2 Unicast Features Supported

The following Layer 2 unicast features are supported:

Learning and aging

- Learned MAC addresses are propagated across MC-LAG peers for all of the VLANs that are spawned across the peers.
- Aging of MAC addresses occurs when the MAC address is not seen on both of the peers.
- MAC addresses learned on single-homed links are propagated across all of the VLANs that have MC-LAG links as members.

NOTE: **MAC learning is disabled on the ICL. Consequently, source MAC addresses cannot be learned locally on the ICL. However, MAC addresses from a remote MC-LAG node can be installed on the ICL interface. For example, the MAC address for a single-homed client on a remote MC-LAG node can be installed on the ICL interface of the local MC-LAG node.**

Layer 2 Multicast Features Supported

The following Layer 2 multicast features are supported:

Unknown unicast and IGMP snooping

- Flooding happens on all links across peers if both peers have virtual LAN membership. Only one of the peers forwards traffic on a given MC-LAG link.
- Known and unknown multicast packets are forwarded across the peers by adding the ICL port as a multicast router port.
- IGMP membership learned on MC-LAG links is propagated across peers.
- During an MC-LAG peer reboot, known multicast traffic is flooded until the IGMP snooping state is synchronized with the peer.

IGMP Snooping on an Active-Active MC-LAG

Internet Group Management Protocol (IGMP) snooping controls multicast traffic in a switched network. When IGMP snooping is not enabled, the Layer 2 device broadcasts multicast traffic out of all of its ports, even if the hosts on the network do not want the multicast traffic. With IGMP snooping enabled, a Layer 2 device monitors the IGMP join and leave messages sent from each connected host to a multicast router. This enables the Layer 2 device to keep track of the multicast groups and associated member ports. The Layer 2 device uses this information to make intelligent decisions and to forward multicast traffic to only the intended destination hosts. IGMP uses Protocol Independent Multicast (PIM) to route the multicast traffic. PIM uses distribution trees to determine which traffic is forwarded.

In an active-active MC-LAG configuration, IGMP snooping replicates the Layer 2 multicast routes so that each MC-LAG peer has the same routes. If a device is connected to an MC-LAG peer by way of a single-homed interface, IGMP snooping replicates the join message to its IGMP snooping peer. If a multicast source is connected to an MC-LAG by way of a Layer 3 device, the Layer 3 device passes this information to the IRB or the routed VLAN interface (RVI) that is configured on the MC-LAG. The first hop designated router is responsible for sending the register and register-stop messages for the multicast group. The last hop designated router is responsible for sending PIM join and leave messages toward the rendezvous point and source for the multicast group. The routing device with the smallest preference metric forwards traffic on transit LANs.

You must configure the ICL interface as a router-facing interface (by configuring the **multicast-router-interface** statement) for multicast forwarding to work in an MC-LAG environment. For the scenario in which traffic arrives by way of a Layer 3 interface, PIM and IGMP must be enabled on the IRB or RVI interface configured on the MC-LAG peers. You must enable PIM on the IRB or RVI interface to avoid multicast duplication.

Layer 3 Unicast Features Supported

To provide Layer 3 routing functions to downstream clients, the MC-LAG network peers must be configured to provide the same gateway address to the downstream clients. To the upstream routers, the MC-LAG network peers could be viewed as either equal-cost multipath (ECMP) or two routes with different preference values.

The following two methods can be used to enable Layer 3 functionality across an MC-LAG. We recommend that you use the VRRP over IRB or RVI method. Use MAC address synchronization only when you cannot configure VRRP over an IRB or RVI.

- Configure different IP addresses on IRB or RVI interfaces, and run Virtual Router Redundancy Protocol (VRRP) over the IRB or RVI interfaces. The virtual IP address is the gateway IP address for the MC-LAG clients.
- Configure the MAC address synchronization feature using the **mcae-mac-synchronize** statement, and configure the same IP address on each of the IRB or RVI interfaces on the MC-LAG peers. This IP address is the gateway IP address for the MC-LAG clients.

Layer 3 unicast feature support includes the following:

- Address Resolution Protocol (ARP) synchronization enables ARP resolution on both of the MC-LAG peers.
- DHCP Relay with option 82 enables option 82 on the MC-LAG peers. Option 82 provides information about the network location of DHCP clients. The DHCP server uses this information to implement IP addresses or other parameters for the client.

VRRP Active-Standby Support

The Juniper Networks Junos operating system (Junos OS) supports active-active MC-LAGs by using VRRP in active-standby mode. VRRP in active-standby mode enables Layer 3 routing over the multichassis aggregated Ethernet interfaces on the MC-LAG peers. In this mode, the MC-LAG peers act as virtual routers. The peers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG. This virtual IP address (of the IRB or RVI interface) maps to either of the VRRP MAC addresses or to the logical interfaces of the MC-LAG peers. The host or server uses the VRRP MAC address to send any Layer 3 upstream packets. At any time, one of the VRRP devices is the master (active), and the other is a backup (standby). Usually, a VRRP backup node does not forward incoming packets. However, when VRRP over IRB or RVI is configured in an MC-LAG active-active environment, both the VRRP master and the VRRP backup forward Layer 3 traffic arriving on the interface. If the master fails, all the traffic shifts to the multichassis aggregated Ethernet interface on the backup.

NOTE: **You must configure VRRP on both MC-LAG peers for both the active and standby members to accept and route packets. Additionally, you must configure the VRRP backup device to send and receive ARP requests.**

Routing protocols run on the primary IP address of the IRB or RVI interface, and both of the MC-LAG peers run routing protocols independently. The routing protocols use the primary IP address of the IRB or RVI interface and the IRB or RVI MAC address to communicate with the MC-LAG peers. The IRB or RVI MAC address of each MC-LAG peer is replicated on the other MC-LAG peer and is installed as a MAC address that has been learned on the ICL.

NOTE: **If you are using the VRRP over IRB or RVI method to enable Layer 3 functionality, you must configure static ARP entries for the IRB or RVI interface of the remote MC-LAG peer to allow routing protocols to run over the IRB or RVI interfaces.**

MAC Address Management

If an MC-LAG is configured to be active-active, upstream and downstream traffic could go through different MC-LAG peer devices. Because the MAC address is learned only on one of the MC-LAG peers, traffic in the reverse direction could be going through the other MC-LAG peer and flooding the network unnecessarily. Also, a single-homed client's MAC address is learned only on the MC-LAG peer that it is attached to. If a client attached to the peer MC-LAG network device needs to communicate with that single-homed client, then traffic would be flooded on the peer MC-LAG network device. To avoid unnecessary flooding, whenever a MAC address is learned on one of the MC-LAG peers, the address is replicated to the other MC-LAG peer. The following conditions are applied when MAC address replication is performed:

- MAC addresses learned on an MC-LAG of one MC-LAG peer must be replicated as learned on the same MC-LAG of the other MC-LAG peer.
- MAC addresses learned on single-homed customer edge (CE) clients of one MC-LAG peer must be replicated as learned on the ICL interface of the other MC-LAG peer.
- MAC address learning on an ICL is disabled from the data path. It depends on software to install MAC addresses replicated through ICCP.

MAC Aging

MAC aging support in Junos OS extends aggregated Ethernet logic for a specified MC-LAG. A MAC address in software is not deleted until all Packet Forwarding Engines have deleted the MAC address.

MAC Address Synchronization and Replication

MAC address synchronization enables MC-LAG peers to forward Layer 3 packets arriving on multichassis aggregated Ethernet interfaces with either their own IRB or RVI MAC address or their peer's IRB or RVI MAC address. Each MC-LAG peer installs its own IRB or RVI MAC address as well as the peer's IRB or RVI MAC address in the hardware. Each MC-LAG peer treats the packet as if it were its own packet. If MAC address synchronization is not enabled, the IRB or RVI MAC address is installed on the MC-LAG peer as if it was learned on the ICL.

NOTE: **If you are using MAC address synchronization to enable Layer 3 functionality, running routing protocols over the IRB or RVI interface is not supported. If you need routing capability, configure both VRRP and routing protocols on each MC-LAG peer.**

MAC address replication, however, provides the ability to exchange learned Layer 2 MAC address information. If you have a VLAN without an IRB or RVI configured, MAC address replication will synchronize the MAC addresses.

Control packets destined for a particular MC-LAG peer that arrive on an multichassis aggregated Ethernet interface of its MC-LAG peer are not forwarded on the ICL interface.

Additionally, using the gateway IP address as a source address when you issue either a ping, traceroute, telnet, or FTP request is not supported.

NOTE: Gratuitous ARP requests are not sent when the MAC address on the IRB or RVI interface changes.

In a VLAN that requires Layer 3 functionality and MAC address synchronization, you can configure either VRRP over an IRB or RVI interface or configure MAC address synchronization. MAC address synchronization requires you to configure the same IP address on the IRB interface in the VLAN on both MC-LAG peers. To enable the MAC address synchronization feature using the standard CLI, issue the **set vlan *vlan-name* mcae-mac-synchronize** command on each MC-LAG peer. If you are using the Enhanced Layer 2 CLI, issue the **set bridge-domains *name* mcae-mac-synchronize** command on each MC-LAG peer. Configure the same IP address on both MC-LAG peers. This IP address is used as the default gateway for the MC-LAG servers or hosts.

Address Resolution Protocol Active-Active MC-LAG Support Methodology

Address Resolution Protocol (ARP) maps IP addresses to MAC addresses. Junos OS uses ARP response packet snooping to support active-active MC-LAGs, providing easy synchronization without the need to maintain any specific state. Without synchronization, if one MC-LAG peer sends an ARP request, and the other MC-LAG peer receives the response, ARP resolution is not successful. With synchronization, the MC-LAG peers synchronize the ARP resolutions by sniffing the packet at the MC-LAG peer receiving the ARP response and replicating this to the other MC-LAG peer. This ensures that the entries in ARP tables on the MC-LAG peers are consistent.

When one of the MC-LAG peers restarts, the ARP destinations on its MC-LAG peer are synchronized. Because the ARP destinations are already resolved, its MC-LAG peer can forward Layer 3 packets out of the multichassis aggregated Ethernet interface.

NOTE: In some cases, ARP messages received by one MC-LAG peer are replicated to the other MC-LAG peer through ICCP. This optimization feature is applicable only for ARP replies, not ARP requests, received by the MC-LAG peers.

NOTE: Dynamic ARP resolution over the ICL interface is not supported. Consequently, incoming ARP replies on the ICL are discarded. However, ARP entries can be populated on the ICL interface through ICCP exchanges from a remote MC-LAG peer.

NOTE: During graceful Routing Engine switchover (GRES), ARP entries that were learned remotely are purged and then learned again.

DHCP Relay with Option 82

NOTE: **DHCP relay is not supported with MAC address synchronization. If DHCP relay is required, configure VRRP over IRB or RVI for Layer 3 functionality.**

DHCP relay with option 82 provides information about the network location of DHCP clients. The DHCP server uses this information to implement IP addresses or other parameters for the client. With DHCP relay enabled, DHCP request packets might take the path to the DHCP server through either of the MC-LAG peers. Because the MC-LAG peers have different host names, chassis MAC addresses, and interface names, you need to observe these requirements when you configure DHCP relay with option 82:

- Use the interface description instead of the interface name.
- Do not use the hostname as part of the circuit ID or remote ID string.
- Do not use the chassis MAC address as part of the remote ID string.
- Do not enable the vendor ID.
- If the ICL interface receives DHCP request packets, the packets are dropped to avoid duplicate packets in the network.

  A counter called *Due to received on ICL interface* has been added to the **show helper statistics** command, which tracks the packets that the ICL interface drops.

  An example of the CLI output follows:

  ```
  user@switch> show helper statistics
  BOOTP:
    Received packets: 6
    Forwarded packets: 0
    Dropped packets: 6
      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
      Due to received on ICL interface: 6
  ```

  The output shows that six packets received on the ICL interface have been dropped.

Protocol Independent Multicast

Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) provide support for Layer 3 multicast. In addition to the standard mode of PIM operation, there is a special mode called PIM dual DR (designated router). PIM dual DR minimizes multicast traffic loss in case of failures.

PIM operation is discussed in the following sections:

PIM Operation with Normal Mode Designated Router Election

In normal mode designated router election, the IRB or RVI interfaces on both of the MC-LAG peers are configured with PIM enabled. In this mode, one of the MC-LAG peers becomes the designated router through the PIM designated router election mechanism. The elected designated router maintains the rendezvous-point tree (RPT) and shortest-path tree (SPT) so it can receive data from the source device. The elected designated router participates in periodic PIM join and prune activities toward the rendezvous point (RP) or the source.

The trigger for initiating these join and prune activities is the IGMP membership reports that are received from interested receivers. IGMP reports received over multichassis aggregated Ethernet interfaces (potentially hashing on either of the MC-LAG peers) and single-homed links are synchronized to the MC-LAG peer through ICCP.

Both MC-LAG peers receive traffic on their incoming interface (IIF). The non-designated router receives traffic by way of the ICL interface, which acts as a multicast router (mrouter) interface.

If the designated router fails, the non-designated router has to build the entire forwarding tree (RPT and SPT), which can cause multicast traffic loss.

PIM Operation with Dual Designated Router Mode

In dual designated router (DR) mode, both of the MC-LAG peers act as designated routers (active and standby) and send periodic join and prune messages upstream toward the RP, or source, and eventually join the RPT or SPT.

The primary MC-LAG peer forwards the multicast traffic to the receiver devices even if the standby MC-LAG peer has a smaller preference metric.

The standby MC-LAG peer also joins the forwarding tree and receives the multicast data. The standby MC-LAG peer drops the data because it has an empty outgoing interface list (OIL). When the standby MC-LAG peer detects the primary MC-LAG peer failure, it adds the receiver VLAN to the OIL, and starts to forward the multicast traffic.

To enable a multicast dual DR, issue the **set protocols pim interface interface-name dual-dr** command on the VLAN interfaces of each MC-LAG peer.

MC-LAG Packet Forwarding

To prevent the server from receiving multiple copies from both of the MC-LAG peers, a block mask is used to prevent forwarding of traffic received on the ICL toward the multichassis aggregated Ethernet interface. Preventing forwarding of traffic received on the ICL interface toward the multichassis aggregated Ethernet interface ensures that traffic received on MC-LAG links is not forwarded back to the same link on the other peer. The forwarding block mask for a given MC-LAG link is cleared if all of the local members of the MC-LAG link go down on the peer. To achieve faster convergence, if all local members of the MC-LAG link are down, outbound traffic on the MC-LAG is redirected to the ICL interface on the data plane.

Layer 3 Unicast Features Supported

To provide Layer 3 routing functions to downstream clients, the MC-LAG network peers must be configured to provide the same gateway address to the downstream clients. To the upstream routers, the MC-LAG network peers could be viewed as either equal-cost multipath (ECMP) or two routes with different preference values.

The following two methods can be used to enable Layer 3 functionality across an MC-LAG. We recommend that you use the VRRP over IRB or RVI method. Use MAC address synchronization only when you cannot configure VRRP over the IRB or RVI interface.

- Configure different IP addresses on IRB or RVI interfaces, and run Virtual Router Redundancy Protocol (VRRP) over the IRB or RVI interfaces. The virtual IP address is the gateway IP address for the MC-LAG clients.
- Configure the MAC address synchronization feature using the **mcae-mac-synchronize** statement,and configure the same IP address on each of the IRBs or RVIs on the MC-LAG peers. This IP address is the gateway IP address for the MC-LAG clients.

If you are using the VRRP over IRB method to enable Layer 3 functionality, you must configure static ARP entries for the IRB interface of the remote MC-LAG peer to allow routing protocols to run over the IRB interfaces. This step is required so you can issue the **ping** command to reach both the physical IP addresses and virtual IP addresses of the MC-LAG peers.

For example, you can issue **set interfaces irb unit 18 family inet address 10.181.18.3/24 arp 10.181.18.2 mac 84:18:88:96:2f:f0** command.

When you issue the **show interfaces irb** command after you have configured VRRP over IRB, you will see that the static ARP entries are pointing to the IRB MAC addresses of the remote MC-LAG peer:

```
user@switch>show interfaces irb
Physical interface: irb, Enabled, Physical link is Up
  Interface index: 180, SNMP ifIndex: 532
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : None
  Current address: 84:18:88:96:2f:f0, Hardware address: 84:18:88:96:2f:f0
  Last flapped   : Never
    Input packets : 0
    Output packets: 0
```

Layer 3 unicast feature support includes the following:

- Address Resolution Protocol (ARP) synchronization enables ARP resolution on both of the MC-LAG peers.

- DHCP Relay with option 82 enables option 82 on the MC-LAG peers. Option 82 provides information about the network location of DHCP clients. The DHCP server uses this information to implement IP addresses or other parameters for the client.

Spanning Tree Protocol Guidelines

The Spanning Tree Protocol (STP) guidelines are as follows:

- Enable STP globally.

  STP might detect local miswiring loops within the peer or across MC-LAG peers.

  STP might not detect network loops introduced by MC-LAG peers.
- Disable STP on ICL links; otherwise, STP might block ICL interfaces and disable protection.
- Disable STP on interfaces that are connected to aggregation switches.
- Do not enable bridge protocol data unit (BPDU) block on interfaces connected to aggregation switches.

For more information about BPDU block, see *Understanding BPDU Protection for STP, RSTP, and MSTP* .

MC-LAG Upgrade

Upgrade the MC-LAG peers according to the following guidelines.

NOTE: After a reboot, the multichassis aggregated Ethernet interfaces come up immediately and might start receiving packets from the server. If routing protocols are enabled, and the routing adjacencies have not been formed, packets might be dropped.

To prevent this scenario, issue the **set interfaces** ***interface-name*** **aggregated-ether-options mc-ae init-delay-time** ***time*** command to set a time by which the routing adjacencies are formed.

1. Make sure that both of the MC-LAG peers (node1 and node2) are in the active-active state by using the following command on any one of the MC-LAG peers:

```
user@switch> show interfaces mc-ae id 1
Member Link                   : ae0
 Current State Machine's State: mcae active state
 Local Status                 : active<<<<<<<
 Local State                  : up
 Peer Status                  : active<<<<<<<
 Peer State                   : up
     Logical Interface        : ae0.0
     Topology Type            : bridge
     Local State              : up
     Peer State               : up
     Peer Ip/MCP/State        : 20.1.1.2 ae2.0 up
```

2. Upgrade node1 of the MC-LAG.

When node1 is upgraded, it is rebooted, and all traffic is sent across the available LAG interfaces of node2, which is still up. The amount of traffic lost depends on how quickly the neighbor devices detect the link loss and rehash the flows of the LAG.

3. Verify that node1 is running the software you just installed by issuing the **show version** command.

4. Make sure that both nodes of the MC-LAG (node1 and node2) are in the active-active state after the reboot of node1.

5. Upgrade node2 of the MC-LAG.

   Repeat Step 1 through Step 3 to upgrade node2.

Private VLANs

Private VLANs (P-VLANs) allow you to split a broadcast domain into multiple isolated broadcast subdomains, essentially putting a VLAN inside of a VLAN. A P-VLAN can span multiple peers on an MC-LAG.

When configuring a P-VLAN, you must configure the ICL interface as the P-VLAN trunk interface for the P-VLAN. This is essential for traffic to be switched to the required primary and secondary ports of the P-VLAN across the MC-LAG peers.

Related Documentation

- Configuring Multichassis Link Aggregation for EX Series on page 32
- Configuring Multichassis Link Aggregation for MX Series on page 27
- Configuring Multichassis Link Aggregation for QFX Series on page 35

PART 2

Configuring MC-LAG for Providing Redundancy, Load Balancing, and Multihoming Support

CHAPTER 2

Establishing Redundancy and Multihoming Using MC-LAG

Multichassis Link Aggregation Overview

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Layer 2 networks are increasing in scale mainly because of technologies such as virtualization. Protocol and control mechanisms that limit the disastrous effects of a topology loop in the network are necessary. The Spanning Tree Protocol (STP) is the primary solution to this problem because it provides a loop-free Layer 2 environment. STP has gone through a number of enhancements and extensions, and even though it scales to very large network environments, it still only provides one active path from one device to another, regardless of how many actual connections might exist in the network. Although STP is a robust and scalable solution to redundancy in a Layer 2 network, the single logical link creates two problems: At least half of the available system bandwidth is off-limits to data traffic, and network topology changes occur. Rapid Spanning Tree Protocol (RSTP) reduces the overhead of the rediscovery process and allows a Layer 2 network to reconverge faster, but the delay is still high.

Link aggregation (IEEE 802.3ad) solves some of these problems by enabling users to use more than one link connection between switches. All physical connections are considered one logical connection. The problem with standard link aggregation is that the connections are point to point.

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two MC-LAG peers. An MC-LAG provides redundancy and load balancing between the two MC-LAG peers, multihoming support, and a loop-free Layer 2 network without running STP.

On one end of an MC-LAG, there is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device uses the link as a LAG. On the other side of the MC-LAG, there are two MC-LAG peers. Each of the MC-LAG peers has one or more physical links connected to a single client device.

The MC-LAG peers use Inter-Chassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly.

Link Aggregation Control Protocol (LACP) is a subcomponent of the IEEE 802.3ad standard. LACP is used to discover multiple links from a client device connected to an MC-LAG peer. LACP must be configured on both MC-LAG peers for an MC-LAG to work correctly.

NOTE: **You must specify a service identifier (service-id) for each multichassis aggregated Ethernet interface that belongs to a LAG; otherwise, multichassis link aggregation will not work.**

- Features Supported on the EX Series, MX Series, and QFX Series on page 26

Features Supported on the EX Series, MX Series, and QFX Series

Table 3 on page 4 lists the MC-LAG features supported on the EX Series, MX Series, and the QFX Series.

Table 7: Feature Support on the EX Series, MX Series, and QFX Series

Features	EX4300 Device	EX4600 Device	EX9200 Device	MX Series Devices	QFX Series Devices
Active-active bridging domain	Not supported	Not supported	Not supported	Supported	Not supported
Active-active mode	Supported	Supported	Supported	Supported	Supported
Active-standby mode	Not supported	Not supported	Supported	Supported	Not supported
Address Resolution Protocol (ARP) synchronization	Supported	Supported	Supported	Supported	Supported
Dynamic Host Control Protocol (DHCP) relay	Supported	Supported	Supported	Supported	Supported
Inter-Chassis Control Protocol (ICCP) and Inter-Chassis link (ICL)	Supported	Supported	Supported	Supported	Supported
Internet Group Management Protocol (IGMP)	Supported	Supported	Supported	Supported	Supported
IGMP snooping	Supported	Supported	Supported	Supported	Supported
Layer 2 circuit functions	Not supported	Not supported	Supported	Not supported	Supported

Table 7: Feature Support on the EX Series, MX Series, and QFX Series *(continued)*

Features	EX4300 Device	EX4600 Device	EX9200 Device	MX Series Devices	QFX Series Devices
Link Aggregation Control Protocol (LACP)	Supported	Supported	Supported	Supported	Supported
Media access control (MAC) management	Supported	Supported	Supported	Supported	Supported
MAC address synchronization	Supported	Supported	Not supported	Supported	Supported
Multichassis link protection	Supported	Supported	Supported	Supported	Supported
Protocol Independent Multicast (PIM)	Supported	Supported	Supported	Supported	Supported
Pseudowire status type	Not supported	Not supported	Not supported	Not supported	Supported
Virtual private LAN service (VPLS)	Not supported	Not supported	Supported in active-standby mode only	Supported in active-standby mode only	Not supported
Virtual Router Redundancy Protocol (VRRP)	Supported	Supported	Supported	Supported	Supported

Related Documentation

- Configuring Multichassis Link Aggregation for EX Series on page 32
- Configuring Multichassis Link Aggregation for MX Series on page 27
- Configuring Multichassis Link Aggregation for QFX Series on page 35

Configuring Multichassis Link Aggregation on MX Series Routers

Supported Platforms MX Series

On MX Series routers, multichassis link aggregation (MC-LAG) enables a device to form a logical LAG interface with two or more other devices. MC-LAG provides additional benefits over traditional LAG in terms of node-level redundancy, multihoming support, and loop-free Layer 2 network without running the Spanning Tree Protocol (STP). MC-LAG can be configured for virtual private LAN service (VPLS) routing instance, circuit cross-connect (CCC) application, and Layer 2 circuit encapsulation types.

The MC-LAG devices use Inter-Chassis Control Protocol (ICCP) to exchange the control information between two MC-LAG network devices.

On one end of MC-LAG is an MC-LAG client device that has one or more physical links in a link aggregation group (LAG). This client device does not need to be aware of MC-LAG. On the other side of MC-LAG are two MC-LAG network devices. Each of these network devices has one or more physical links connected to a single client device. The network devices coordinate with each other to ensure that data traffic is forwarded properly.

MC-LAG includes the following functionality:

- Active-standby mode is supported using Link Aggregation Control Protocol (LACP).
- MC-LAG operates only between two chassis.
- Layer 2 circuit functions are supported with **ether-ccc** and **vlan-ccc** encapsulation.
- VPLS functions are supported with **ether-vpls** and **vlan-vpls**.

NOTE: Ethernet connectivity fault management (CFM) specified in the IEEE 802.1ag standard for Operation, Administration, and Management (OAM) is *not* supported on MC-LAG interfaces.

To enable MC-LAG, include the **mc-ae** statement at the **[edit interfaces ae*X* aggregated-ether-options]** hierarchy level along with either the **ethernet-bridge**, **encapsulation ethernet-ccc**, **encapsulation ethernet-vpls**, or **flexible-ethernet-services** statement at the **[edit interfaces ae*X*]** hierarchy level. You also need to configure the **lacp** statement and the **admin-key** and **system-id** statements at the **[edit interfaces ae*X* aggregated-ether-options]** hierarchy level:

```
[edit interfaces aeX]
encapsulation (ethernet-bridge | ethernet-ccc | ethernet-vpls | flexible-ethernet-services);
aggregated-ether-options {
  lacp {
    active;
    admin-key number;
    system-id mac-address;
    system-priority number;
  }
  mc-ae {
    chassis-id chassis-id;
    events {
      iccp-peer-down {
        force-icl-down;
        prefer-status-control-active;
      }
    }
    mc-ae-id mc-ae-id;
    mode (active-active | active-standby);
    redundancy-group group-id;
    status-control (active | standby);
  }
}
```

NOTE: When you configure the **prefer-status-control-active** statement, you must also configure the **status-control active** statement. If you configure the **status-control standby** statement with the **prefer-status-control-active** statement, the system issues a warning.

To delete an MC-LAG interface from the configuration, issue the **delete interfaces ae*X* aggregated-ether-options mc-ae** command at the **[edit]** hierarchy level in configuration mode:

```
[edit]
user@host# delete interfaces aeX aggregated-ether-options mc-ae
```

Preventing Loops in MC-LAG Topologies

To prevent loops in MC-LAG topologies, configure the two edge nodes with the same (STP) virtual root ID using Reverse Layer 2 Gateway Protocol (RL2GP). This root ID should be superior to all bridges in the downstream network because downstream bridges have to be capable of running STP. RL2GP should be configured on both MC-LAG nodes to prevent loops. A potential loop, such as one that can happen due to improper cabling at the core or the access switching layer, or due to a bug in server software, is broken by STP blocking one of the interfaces in the downstream network. Because both MC-LAG nodes are root bridges (virtual), the MC-LAG interface remains in the forwarding state. The downstream bridge receives bridge protocol data units (BPDUs) from both the nodes and thus receives twice the number of BPDUs on its ae interface. If both MC-LAG nodes use the same ae interface name, the STP port number is identical, which reduces the STP load on downstream bridge.

Configuring MC-LAG Devices

Perform the following steps on each router that is hosting an MC-LAG:

1. Specify the same multichassis aggregated Ethernet identification number for the MC-LAG that the aggregated Ethernet interface belongs to on each router.

   ```
   [edit interfaces]
   user@host# set aeX aggregated-ether-options mc-ae mc-ae-id mc-ae-id
   ```

   For example:

   ```
   [edit interfaces]
   user@host# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
   ```
2. Specify a unique chassis ID for the MC-LAG that the aggregated Ethernet interface belongs to on each router.

   ```
   [edit interfaces]
   user@host# set aeX aggregated-ether-options mc-ae chassis-id chassis-id
   ```

   For example:

   ```
   [edit interfaces]
   user@host# set ae1 aggregated-ether-options mc-ae chassis-id 0
   ```
3. Specify the mode of the MC-LAG the aggregated Ethernet interface belongs to.

   NOTE: Only active-active mode is supported for RL2GP at this time.

   ```
   [edit interfaces]
   user@host# set aeX aggregated-ether-options mc-ae mode mode
   ```

   For example:

   ```
   [edit interfaces]
   user@host# set ae1 aggregated-ether-options mc-ae mode active-active
   ```

4. Specify whether the aggregated Ethernet interface participating in the MC-LAG is primary or secondary.

   Primary is **active**, and secondary is **standby**.

   NOTE: You must configure status control on both routers hosting the MC-LAG. If one router is in active mode, the other must be in standby mode.

   [edit interfaces]
   user@host# **set *aeX* aggregated-ether-options mc-ae status-control (active | standby)**

   For example:

   [edit interfaces]
   user@host# **set *ae1* aggregated-ether-options mc-ae status-control active**

5. Specify the same LACP system ID on each router.

   [edit interfaces]
   user@host# **set *aeX* aggregated-ether-options lacp system-id *mac-address***

   For example:

   [edit interfaces]
   user@host# **set ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05**

6. Specify the same LACP administration key on each router.

   [edit interfaces]
   user@host# **set *aeX* aggregated-ether-options lacp admin-key *number***

   For example:

   [edit interfaces]
   user@host# **set ae1 aggregated-ether-options lacp admin-key 3**

7. Configure ICCP by doing the following on each router hosting the MC-LAG:

   a. Configure the local IP address to be used by all routers hosting the MC-LAG.

      [edit protocols]
      user@host# **set iccp local-ip-addr *local-ip-address***

      For example:

      [edit protocols]
      user@host# **set iccp local-ip-addr 3.3.3.1**

   b. (Optional) Configure the IP address of the router and the time during which an ICCP connection must succeed between the routers hosting the MC-LAG.

      Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

      [edit protocols]
      user@host# **set iccp peer *peer-ip-address* session-establishment-hold-time *seconds***

      For example:

      [edit protocols]
      user@host# **set iccp peer 3.3.3.2 session-establishment-hold-time 50**

   c. Configure the minimum interval at which the router must receive a reply from the other router with which it has established a Bidirectional Forwarding Detection (BFD) session.

NOTE: Configuring the minimum receive interval is required to enable BFD.

```
[edit protocols]
user@host# set iccp peer peer-ip-address liveness-detection minimum-receive-interval milliseconds
```

For example:

```
[edit protocols]
user@host# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 60
```

d. Configure the minimum transmit interval during which a router must receive a reply from a router with which it has established a BFD session.

```
[edit protocols]
user@host# set iccp peer peer-ip-address liveness-detection transmit-interval minimum-interval milliseconds
```

For example:

```
[edit protocols]
user@host# set iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 60
```

8. Configure a multichassis protection link between the routers.

```
[edit]
user@host# set multi-chassis multi-chassis-protection peer-ip-address interface interface-name
```

For example:

```
[edit protocols]
user@host# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

9. Enable Rapid Spanning Tree Protocol (RSTP).

```
[edit]
user@host# set protocols rstp interface ae1 mode point-to-point
```

10. Configure the MC-LAG interfaces as edge ports on both routers.

```
user@host# set protocols rstp interface interface-name edge
```

For example:

```
[edit]
user@host# set protocols rstp interface ae1 edge
```

11. Enable BPDU block on all interfaces except for the ICL-PL interfaces on both routers.

NOTE: MX routers set the MC LAG interfaces to STP blocking state if a superior BPDU is received on the MC-LAG. Do not configure block-on-edge or configure an inferior bridge ID for downstream devices.

```
[edit]
user@host# set protocols rstp bpdu-block-on-edge
```

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63

- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- *show interfaces mc-ae*
- *Ethernet Interfaces*

Configuring Multichassis Link Aggregation on EX Series Switches

Supported Platforms EX Series

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two MC-LAG peers (for example, EX9200 switches). An MC-LAG provides redundancy and load balancing between the two MC-LAG peers, multihoming support, and a loop-free Layer 2 network without running Spanning Tree Protocol (STP).

On one end of an MC-LAG, there is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device does not need to have an MC-LAG configured. On the other side of MC-LAG, there are two MC-LAG peers. Each of the MC-LAG peers has one or more physical links connected to a single client device.

The MC-LAG peers use Inter-Chassis Control Protocol (ICCP) to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly.

NOTE: An interface with an already configured IP address cannot form part of the aggregated Ethernet interface or multichassis aggregated Ethernet interface group.

For information about MC-LAG functional behaviors, see the “MC-LAG Configuration Guidelines and Functional Behavior” section in the topic *Understanding Multichassis Link Aggregation*. .

Perform the following steps on each switch that hosts an MC-LAG:

1. Specify the same multichassis aggregated Ethernet identification number for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.

   ```
   [edit interfaces]
   user@switch# set aex aggregated-ether-options mc-ae mc-ae-id number
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
   ```

2. Specify a unique chassis ID for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.

   ```
   [edit interfaces]
   user@switch# set aex aggregated-ether-options mc-ae chassis-id number
   ```

   For example:


```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 0
```

3. Specify the mode of the MC-LAG the aggregated Ethernet interface belongs to.

```
[edit interfaces]
user@switch# set aex aggregated-ether-options mc-ae mode mode
```

For example:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
```

4. Specify whether the aggregated Ethernet interface participating in the MC-LAG is primary or secondary.

Primary is **active**, and secondary is **standby**.

NOTE: You must configure status control on both switches that host the MC-LAG. If one switch is in active mode, the other must be in standby mode.

```
[edit interfaces]
user@switch# set aex aggregated-ether-options mc-ae status-control (active | standby)
```

For example:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae status-control active
```

NOTE: You can configure the **prefer-status-control-active** statement with the **mc-ae status-control standby** configuration to prevent the LACP MC-LAG system ID from reverting to the default LACP system ID on ICCP failure. Use this configuration only if you can ensure that ICCP will not go down unless the switch is down. You must also configure the **hold-time down** value (at the **[edit interfaces *interface-name*]** hierarchy level) for the ICL with the **mc-ae status-control standby** configuration to be higher than the ICCP BFD timeout. This configuration prevents data traffic loss by ensuring that when the switch with the **mc-ae status-control active** configuration goes down, the switch with the **mc-ae status-control standby** configuration does not go into standby mode.

To make the **prefer-status-control-active** configuration work with the **mc-ae status-control standby** configuration when an ICL logical interface is configured on an aggregated Ethernet interface, you must either configure the ***lacp* periodic interval** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level as slow or configure the **detection-time threshold** statement at the **[edit protocols iccp peer *liveness-detection*]** hierarchy level as less than 3 seconds.

On EX9200 switches, the **prefer-status-control-active** statement was added in Junos OS Release 13.2R1.

5. Specify the same LACP system ID on each switch.

```
[edit interfaces]
```

```
user@switch# set aex aggregated-ether-options lacp system-id mac-address
```

For example:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
```

6. Specify the same LACP administration key on each switch.

```
[edit interfaces]
user@switch# set aex aggregated-ether-options lacp admin-key number
```

For example:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp admin-key 3
```

7. Configure ICCP by performing the following steps on each switch that hosts the MC-LAG:

   a. Configure the local IP address to be used by the switches that host the MC-LAG.

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr local-ip-address
   ```

   For example:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.1
   ```

   b. (Optional) Configure the IP address of the switch and the time during which an ICCP connection must be established between the switches that host the MC-LAG.

   Configuring the session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

   ```
   [edit protocols]
   user@switch# set iccp peer peer-ip-address session-establishment-hold-time seconds
   ```

   For example:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
   ```

   c. (Optional) Configure the backup-liveness-detection statement on the management interface (fxp0) only.

   We recommend that you configure the backup liveness detection feature to implement faster failover of data traffic during an MC-LAG peer reboot.

   NOTE: On EX9200 switches, the backup-liveness-detection statement was added in Junos OS Release 13.2R1.

   ```
   [edit protocols]
   user@switch# set iccp peer peer-ip-address backup-liveness-detection backup-peer-ip
   ip-address
   ```

   For example:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
   10.207.64.232
   ```


d. Configure the minimum interval at which the switch must receive a reply from the other switch with which it has established a Bidirectional Forwarding Detection (BFD) session.

NOTE: Configuring the minimum receive interval is required to enable BFD. We recommend a minimum receive interval value of 60 seconds.

```
[edit protocols]
user@switch# set iccp peer peer-ip-address liveness-detection minimum-receive-interval seconds
```

For example:

```
[edit protocols]
user@switch# set iccppeer 3.3.3.2 liveness-detection minimum-receive-interval 60
```

e. Configure the minimum transmit interval during which a switch must receive a reply from a switch with which it has established a BFD session.

```
[edit protocols]
user@switch# set iccp peer peer-ip-address liveness-detection transmit-interval minimum-interval seconds
```

For example:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 60
```

8. Configure a multichassis protection link between the switches.

```
[edit]
user@switch# set multi-chassis multi-chassis-protection peer-ip-address interface interface-name
```

For example:

```
[edit protocols]
user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Related Documentation

- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on EX9200 Switches on page 152
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on EX9200 Switches on page 130

Configuring Multichassis Link Aggregation

Supported Platforms EX4600, QFX Series standalone switches

NOTE: **Multichassis link aggregation (MC-LAG) is supported on QFX3500 and QFX3600 standalone switches running the original CLI, and on QFX5100 switches running Enhanced Layer 2 Software.**

Multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two switches. An MC-LAG provides redundancy and load balancing between the two switches, multihoming support, and a loop-free Layer 2 network without running the Spanning Tree Protocol (STP).

The MC-LAG switches use the Inter-Chassis Control Protocol (ICCP) to exchange the control information between two MC-LAG switches.

On one end of an MC-LAG is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device does not need to detect the MC-LAG. On the other side of MC-LAG are two MC-LAG switches. Each of the switches has one or more physical links connected to a single client device. The switches coordinate with each other to ensure that data traffic is forwarded properly.

NOTE: **An interface with an already configured IP address cannot form part of the aggregated Ethernet interface or multichassis aggregated Ethernet interface group.**

Perform the following steps on each switch that is hosting an MC-LAG:

1. Specify the same multichassis aggregated Ethernet identification number for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options mc-ae mc-ae-id number
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
   ```

2. Specify a unique chassis ID for the MC-LAG that the aggregated Ethernet interface belongs to on each switch.

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options mc-ae chassis-id number
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 0
   ```

3. Specify the mode of the MC-LAG the aggregated Ethernet interface belongs to.

   NOTE: **Only active-active mode is supported at this time.**

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options mc-ae mode mode
   ```

   For example:


```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
```

4. Specify whether the aggregated Ethernet interface participating in the MC-LAG is primary or secondary.

   Primary is **active**, and secondary is **standby**.

   NOTE: You must configure status control on both switches hosting the MC-LAG. If one switch is in active mode, the other must be in standby mode.

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options mc-ae status-control (active | standby)
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae status-control active
   ```

5. Specify the same LACP system ID on each switch.

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options lacp system-id mac-address
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
   ```

6. Specify the same LACP administration key on each switch.

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options lacp admin-key number
   ```

   For example:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp admin-key 3
   ```

7. Configure ICCP by doing the following on each switch hosting the MC-LAG:

   a. Configure the local IP address to be used by all switches hosting the MC-LAG.

      ```
      [edit protocols]
      user@switch# set iccp local-ip-addr local-ip-address
      ```

      For example:

      ```
      [edit protocols]
      user@switch# set iccp local-ip-addr 3.3.3.1
      ```

   b. (Optional) Configure the IP address of the switch and the time during which an ICCP connection must succeed between the switches hosting the MC-LAG.

      Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

      ```
      [edit protocols]
      user@switch# set iccp peer peer-ip-address session-establishment-hold-time seconds
      ```

      For example:

      ```
      [edit protocols]
      user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
      ```

   c. (Optional) Configure the IP address to be used for backup liveness detection.

NOTE: By default, backup liveness detection is not enabled. Configure backup liveness detection if you require minimal traffic loss during a reboot. Backup liveness detection helps achieve sub-second traffic loss during an MC-LAG reboot.

```
[edit protocols]
user@switch# set iccp peer peer-ip-address backup-liveness-detection backup-peer-ip
ip-address
```

For example:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
10.207.64.232
```

d. Configure the minimum interval at which the switch must receive a reply from the other switch with which it has established a Bidirectional Forwarding Detection (BFD) session.

NOTE: Configuring the minimum receive interval is required to enable BFD.

```
[edit protocols]
user@switch# set iccp peer peer-ip-address liveness-detection minimum-receive-interval
seconds
```

For example:

```
[edit protocols]
user@switch# set iccppeer 3.3.3.2 liveness-detection minimum-receive-interval 1000
```

e. Configure the minimum transmit interval during which a switch must receive a reply from a switch with which it has established a BFD session.

```
[edit protocols]
user@switch# set iccp peer peer-ip-address liveness-detection transmit-interval
minimum-interval seconds
```

For example:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval
1000
```

8. Configure a multichassis protection link between the switches.

```
[edit]
user@switch# set multi-chassis multi-chassis-protection peer-ip-address interface
interface-name
```

For example:

```
[edit protocols]
user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

9. If you are using ELS, configure the **service-id** on both switches.

The **service-id** must be the same number on both switches.

```
[edit]
```

```
user@switch# set switch-options service-id number
```

For example:

```
[edit]
user@switch# set switch-options service-id 10
```

10. Configure the MC-LAG interfaces as edge ports on both switches.

```
user@switch# set protocols rstp interface interface-name edge
```

For example:

```
[edit]
user@switch# set protocols rstp interface ae1 edge
```

11. Enable BPDU block on all interfaces except for the ICL-PL interfaces on both switches.

```
[edit]
user@switch# set protocols rstp bpdu-block-on-edge
```

Related Documentation

- Example: Configuring Multichassis Link Aggregation on page 39
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast using MAC Address Synchronization on page 193
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on page 208
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on page 235

Example: Configuring Multichassis Link Aggregation

Supported Platforms EX4600, QFX Series standalone switches

NOTE: Multichassis link aggregation (MC-LAG) is supported on QFX3500 and QFX3600 standalone switches running the original CLI and QFX5100 standalone switches and EX4600 switches running Enhanced Layer 2 Software. (This example has not been tested on all devices that support MC-LAG. See Feature Explorer for a full listing of devices that support MC-LAG, and see "Multichassis Link Aggregation Overview" on page 3 for some specifics on which MC-LAG subfeatures are available per device.)

This example shows how multichassis link aggregation groups (MC-LAGs) enable a client device to form a logical LAG interface between two switches to provide redundancy and load balancing between the two switches, multihoming support, and a loop-free Layer 2 network without running Spanning Tree Protocol (STP).

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2 or later for the QFX3500 and QFX3600 standalone switches and Junos OS Release 13.2X51-D10 or later for the QFX5100 standalone switches, or Junos OS Release 13.2X51-D25 or later for EX4600 switches.
- Two QFX3500 or QFX3600 standalone switches, two QFX5100 standalone switches, or two EX4600 switches.

Before you configure an MC-LAG, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch*.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch*.

Overview

In this example, you configure an MC-LAG across two switches, consisting of two aggregated Ethernet interfaces, an interchassis control link-protection link (ICL-PL), multichassis protection link for the ICL-PL, the Inter-Chassis Control Protocol for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers. Layer 3 connectivity is required for ICCP.

Topology

The topology used in this example consists of two switches hosting an MC-LAG. The two switches are connected to a server. Figure 1 on page 40 shows the topology used in this example.

Figure 1: Configuring a Multichassis LAG Between Switch A and Switch B

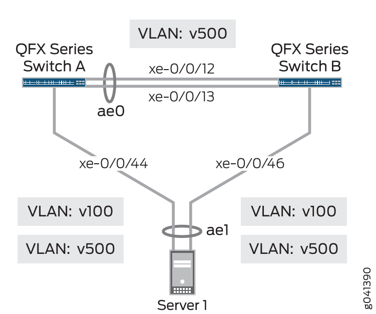


Table 8 on page 41 details the topology used in this configuration example.

Table 8: Components of the Topology for Configuring a Multichassis LAG Between Two Switches

Hostname	Base Hardware	Multichassis Link Aggregation Group
Switch A Switch B	QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch	ae0 is configured as an aggregated Ethernet interface, and is used as an ICL-PL. The following interfaces are part of ae0: xe-0/0/12 and xe-0/0/13 Switch A and xe-0/0/12 and xe-0/0/13 on Switch B. ae1 is configured as an MC-LAG, and the following two interfaces are part of ae1: xe-0/0/44 on Switch A and xe-0/0/46 on Switch B. .

Configuration

CLI Quick Configuration

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

NOTE: This example shows how to configure MC-LAG using both the original CLI and Enhanced Layer 2 Software (ELS).

In ELS, there are three statements and one additional statement that are different grom the original CLI:

- The **port-mode** statement in the **[edit interfaces *interface-name* unit *number* family ethernet-switching]** hierarchy is not supported. Use the **interface-mode** statement instead.
- The **vlan** statement in the **[edit interfaces *interface-name*]** hierarchy is not supported. Use the **irb** statement instead.
- The **vlan.*logical-interface-number*** option in the **[edit vlans *vlan-name* l3-interface]** hierarchy is not supported. Use the **irb.*logical-interface-number*** option instead.
- The **service-id** statement in the **[edit switch-options]** hierarchy is required in the ELS CLI.

Switch A—Original CLI

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
```

```
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch A—ELS

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
set switch-options service-id 10
```

Switch B—Original CLI

```
set chassis aggregated-devices ethernet device-count 2
```



```
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Switch B—ELS

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
```

set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
set switch-options service-id 10

Configuring MC-LAG on Two Switches

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable multichassis protection link between MC-LAG peers:

1. Configure the number of LAGs on both Switch A and Switch B.

   [edit chassis]
   user@switch# **set aggregated-devices ethernet device-count 2**

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   Switch A and Switch B:

   [edit interfaces]
   user@switch# **set xe-0/0/12 ether-options 802.3ad ae0**
   [edit interfaces]
   user@switch# **set xe-0/0/13 ether-options 802.3ad ae0**

   Switch A:

   [edit interfaces]
   user@switch# **set xe-0/0/44 ether-options 802.3ad ae1**

   Switch B:

   [edit interfaces]
   user@switch# **set xe-0/0/46 ether-options 802.3ad ae1**

3. Configure a trunk interface between Switch A and Switch B.

   NOTE: The **port-mode** statement is not supported on Enhanced Layer 2 Software (ELS). If you are running ELS, use the **interface-mode** statement.

   Orignal CLI:

   [edit interfaces]
   user@switch# **set ae0 unit 0 family ethernet-switching port-mode trunk**

   or

   ELS:

   [edit interfaces]
   user@switch# **set ae0 unit 0 family ethernet-switching interface-mode trunk**

4. Configure a multichassis protection link between Switch A and Switch B.

   Switch A:

   ```
   [edit]
     user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
   ```

   Switch B:

   ```
   [edit]
     user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
   ```

Step-by-Step Procedure

To enable ICCP:

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address and minimum receive interval for a BFD session for ICCP on Switch A and Switch B.

   NOTE: Configure at least 1000 ms as the minimum receive interval.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval
     1000
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
     1000
   ```

3. Configure the peer IP address and minimum transmit interval for BFD session for ICCP on Switch A and Switch B.

   NOTE: Configure at least 1000 ms as the transmit interval minimum interval.

Switch A:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
  minimum-interval 1000
```

Switch B:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
  minimum-interval 1000
```

4. (Optional) Configure the time during which an ICCP connection must succeed between MC-LAG peers on Switch A and Switch B.

   NOTE: Configuring session establishment hold time helps in faster ICCP connection establishment. The recommended value is 50 seconds.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
   ```

5. (Optional) Configure the backup IP address to be used for backup liveness detection on both Switch A and Switch B.

   NOTE: By default, backup liveness detection is not enabled. Configuring a backup IP address helps achieve sub-second traffic loss during a MC-LAG peer reboot.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip
     10.207.64.233
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
     10.207.64.234
   ```

6. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B.

   ```
   [edit vlans]
     user@switch# set v500 vlan-id 500
   ```

Original CLI:

[edit vlans]
user@switch# **set v500 l3-interface vlan.500**

ELS:

[edit vlans]
user@switch# **set v500 l3-interface irb.500**

NOTE: The **port-mode** statement is not supported on Enhanced Layer 2 Software (ELS). If you are running ELS, use the **interface-mode** statement.

Original CLI:

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching port-mode trunk vlan members v500**

Original CLI:

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching port-mode trunk vlan members v100**

or

ELS:

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching interface-mode trunk vlan members v500**

ELS:

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching interface-mode trunk vlan members v100**

Step-by-Step Procedure

To enable the MC-LAG interface:

1. Enable LACP on the MC-LAG interface on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options lacp active**

2. Specify the same multichassis aggregated Ethernet identification number on both MC-LAG peers on Switch A and Switch B.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
```

3. Specify the same service ID on Switch A and Switch B.

   ELS:

   ```
   [edit]
     user@switch# set switch-options service-id 10
   ```

4. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A:

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 0
   ```

   Switch B:

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 1
   ```

5. Specify the operating mode of the MC-LAG on both Switch A and Switch B.

   NOTE: Only active-active mode is supported at this time.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
   ```

6. Specify the status control for MC-LAG on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAG. If one peer is in active mode, the other must be in standby mode.

   Switch A:

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae status-control active
   ```

   Switch B:

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae status-control standby
   ```

7. Specify the number of seconds by which the bring-up of the multichassis aggregated Ethernet interface should be deferred after you reboot Switch A and Switch B.

NOTE: The recommended value for maximum VLAN configuration (for example, 4,000 VLANS) is 240 seconds. If IGMP snooping is enabled on all of the VLANs, the recommended value is 420 seconds.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae init-delay-time 240
```

8. Specify the same LACP system ID for the MC-LAG on Switch A and Switch B.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05
```

9. Specify the same LACP administration key on both Switch A and Switch B.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options lacp admin-key 3
```

10. Enable a VLAN on the MC-LAG on Switch A and Switch B.

NOTE: The **port-mode** statement is not supported on Enhanced Layer 2 Software (ELS). If you are running ELS, use the **interface-mode** statement.

Original CLI:

```
[edit interfaces]
  user@switch# set ae1 unit 0 family ethernet-switching port-mode trunk
```

or

ELS:

```
[edit interfaces]
  user@switch# set ae1 unit 0 family ethernet-switching interface-mode trunk
```

```
[edit]
  user@switch# set vlans v100 vlan-id 100
```

```
[edit interfaces]
  user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
```

11. (Optional) Enable a private VLAN on the MC-LAG on Switch A and Switch B.

```
[edit]
  user@switch# set vlans vlan100 pvlan isolation-vlan-id 200
  extend-secondary-vlan-id
[edit]
  user@switch# set vlans vlan100 interface ae0.0 pvlan-trunk
```

Step-by-Step Procedure

To enabled RSTP:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Enable RSTP globally on all interfaces on Switch A and Switch B.

   NOTE: The **all** option is not available on ELS, so you cannot issue this command on ELS.

   ```
   [edit]
     user@switch# set protocols rstp interface all mode point-to-point
   ```

   ELS:

   ```
   [edit]
     user@switch# set protocols rstp interface ae1.0 mode point-to-point
   ```

2. Disable RSTP on the ICL-PL interfaces on Switch A and Switch B:

   NOTE: This command is not needed on ELS.

   ```
   [edit]
     user@switch# set protocols rstp interface ae0.0 disable
   ```

3. Configure the MC-LAG interfaces as edge ports on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured. MC LAG switches are usually configured as root bridge. When downstream switches send superior BPDUs to the MC LAG switches, the MC LAG interfaces will be set as blocked by the downstream switches. The default behavior for the original CLI is to drop superior BPDUs.

   ```
   [edit]
     user@switch# set protocols rstp interface ae1.0 edge
   ```

4. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
   ```


user@switch# **set protocols rstp bpdu-block-on-edge**

Results

From configuration mode on Switch A using Original CLI, confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/44 {
  ether-options {
    802.3ad ae1;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members v500;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
      active;
      system-id 00:01:02:03:04:05;
      admin-key 3;
    }
    mc-ae {
      mc-ae-id 3;
      chassis-id 0;
      mode active-active;
      status-control active;
      init-delay-time 240
```

```
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 500 {
        family inet {
            address 3.3.3.2/24;
        }
    }
}
```

```
user@SwitchA# show protocols
iccp {
    local-ip-addr 3.3.3.2;
    peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
    interface ae0;
}
```

```
user@SwitchA# show vlans
v100 {
    vlan-id 100;
}
```



```
v500 {
  vlan-id 500;
  l3-interface vlan.500;
}
```

From configuration mode on Switch A using ELS, confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, **show switch-options**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/44 {
  ether-options {
    802.3ad ae1;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
      vlan {
        members v500;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
      active;
      system-id 00:01:02:03:04:05;
      admin-key 3;
    }
    mc-ae {
      mc-ae-id 3;
      chassis-id 0;
      mode active-active;
      status-control active;
      init-delay-time 240
```

```
        }
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 500 {
        family inet {
            address 3.3.3.2/24;
        }
    }
}
```

```
user@SwitchA# show protocols
iccp {
    local-ip-addr 3.3.3.2;
    peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae1.0 {
        edge;
    }
    mode point-to-point;
    }
    bpdu-block-on-edge;
    }
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
    interface ae0;
}
```

```
user@SwitchA# show switch-options
service-id 10;
```

```
user@SwitchA# show vlans
v100 {
    vlan-id 100;
}
v500 {
```



```
    vlan-id 500;
    l3-interface irb.500;
}
```

From configuration mode on Switch B using Original CLI, confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@SwitchB# show chassis
aggregated-devices {
    ethernet {
        device-count 2;
    }
}
user@SwitchB# show interfaces
xe-0/0/12 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/13 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/46 {
    ether-options {
        802.3ad ae1;
    }
}
ae0 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v500;
            }
        }
    }
}
ae1 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:05;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 3;
            chassis-id 1;
            mode active-active;
            status-control standby;
            init-delay-time 240
        }
```

```
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 500 {
        family inet {
            address 3.3.3.1/24;
        }
    }
}
```

```
user@SwitchB# show protocols
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
    interface ae0;
}
```

```
user@SwitchB# show vlans
v100 {
    vlan-id 100;
}
v500 {
```



```
    vlan-id 500;
    l3-interface vlan.500;
}
```

From configuration mode on Switch B using ELS, confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, **show switch-options**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@SwitchB# show chassis
aggregated-devices {
    ethernet {
        device-count 2;
    }
}
```

```
user@SwitchB# show interfaces
xe-0/0/12 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/13 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/46 {
    ether-options {
        802.3ad ae1;
    }
}
ae0 {
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v500;
            }
        }
    }
}
ae1 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:05;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 3;
            chassis-id 1;
            mode active-active;
            status-control standby;
            init-delay-time 240
        }
```

```
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 500 {
        family inet {
            address 3.3.3.1/24;
        }
    }
}
```

```
user@SwitchB# show protocols
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae1.0 {
        edge;
    }
    mode point-to-point;
    }
    bpdu-block-on-edge;
    }
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
    interface ae0;
}
```

```
user@SwitchB# show switch-options
service-id 10;
```

```
user@SwitchB# show vlans
v100 {
    vlan-id 100;
}
v500 {
    vlan-id 500;
```



```
    l3-interface irb.500;
  }
```

Verification

Verify that the configuration is working properly.

Verifying That ICCP Is Working on Switch A

Purpose Verify that ICCP is running on Switch A.

Action

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.1
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That ICCP Is Working on Switch B

Purpose Verify that ICCP is running on Switch B.

Action show iccp

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```


Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That LACP Is Active on Switch A

Purpose Verify that LACP is active on Switch A.

Action

```
[edit]
user@switch> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/46      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/46    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/46                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch A is participating in LACP negotiation.

Verifying That LACP Is Active on Switch B

Purpose Verify that LACP is active on Switch B

Action

```
[edit]
user@switch> show lacp interfaces

Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/44      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/44    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/44                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch B is participating in LACP negotiation.

Verifying That the multichassis aggregated Ethernet and ICL-PL Interfaces Are Up on Switch A

Purpose Verify that the multichassis aggregated Ethernet and ICL-PL interfaces are up on Switch A.

Action

```
[edit]
user@switch> 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         : 3.3.3.1 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet interface on Switch A is up and active.

Verifying That the multichassis aggregated Ethernet and ICL-PL Interfaces Are Up on Switch B

Purpose Verify that the multichassis aggregated Ethernet and ICL-PL interfaces are up on Switch B.

Action

```
[edit]
user@switch> 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         : 3.3.3.2 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet interface on Switch B is up and active.

Verifying That MAC Learning Is Occurring on Switch A

Purpose Verify that MAC learning is working on Switch A.

Action

```
[edit]
user@switch> show ethernet-switching table
Ethernet-switching table: 10 entries, 4 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  V100              *                 Flood          - All-members
  V100              00:10:94:00:00:05 Learn(L)      33 ae0.0 (MCAE)
```

Meaning The output shows four learned MAC addresses entries.

Verifying That MAC Learning Is Occurring on Switch B

Purpose Verify that MAC learning is working on Switch B.

Action

```
[edit]
user@switch> show ethernet-switching table
Ethernet-switching table: 10 entries, 4 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  V100              *                 Flood          - All-members
  V100              00:10:94:00:00:05 Learn(L)       33 ae0.0 (MCAE)
```

Meaning The output shows four learned MAC addresses entries.

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**.

Solution Check the following:

- Verify that there is no configuration mismatch.
- Verify that all member ports are up.
- Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
- Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- Configuring Multichassis Link Aggregation on page 35

CHAPTER 3

Enabling High Availability in Layer 2 Networks Using Active-Active Bridging for MC-LAG

Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview

Supported Platforms MX Series

MX Series routers support active-active bridging and Virtual Router Redundancy Protocol (VRRP) over integrated routing and bridging (IRB). This is a common scenario used in data centers. This section provides an overview of the supported functionality.

Active-active bridging and VRRP over IRB support extend multichassis link aggregation group (MC-LAG) by adding the following functionality:

- Interchassis link (ICL) pseudowire interface or Ethernet interface (ICL-PL field) for active-active bridging
- Active-active bridging
- VRRP over IRB for active-active bridging
- A single bridge domain not corresponding to two redundancy group IDs

The following functionalities are supported for MC-LAG in an active-active bridging domain:

- MC-LAG is supported only between two chassis, using an interchassis link (ICL) pseudowire interface or Ethernet interface (ICL-PL field) for **active-active bridging**, and **active-active bridging** VRRP over IRB for **active-active bridging**.
- For VPLS networks, you can configure the aggregated Ethernet (aeX) interfaces on MC-LAG devices with the **encapsulation ethernet-vpls** statement to use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values or the **encapsulation vlan-vpls** statement to use Ethernet VLAN encapsulation on VPLS circuits.
- Layer 2 circuit functionalities are supported with **ethernet-ccc** as the encapsulation mode.
- Network topologies in a triangular and square pattern are supported. In a triangular network design, with equal-cost paths to all redundant nodes, slower, timer-based convergence can possibly be prevented. Instead of indirect neighbor or route loss detection using hellos and dead timers, you can identify the physical link loss and denote a path as unusable and reroute all traffic to the alternate equal-cost path. In a square network design, depending on the location of the failure, the routing protocol might converge to identify a new path to the subnet or the VLAN, causing the convergence of the network to be slower.
- Interoperation of Link Aggregation Control Protocol (LACP) for MC-LAG devicess is supported. LACP is one method of bundling several physical interfaces to form one logical interface. When LACP is enabled, the local and remote sides of the aggregated Ethernet links exchange protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when the links receive the PDUs from another link. One side of the link must be configured as active for the link to be up.
- Active-standby mode is supported using LACP. When an MC-LAG operates in the active-standby mode, one of the router's ports only becomes active when failure is detected in the active links. In this mode, the provider edge (PE) routers perform an election to determine the active and standby routers.
- Configuration of the pseudowire status type length variable (TLV) is supported. The pseudowire status TLV is used to communicate the status of a pseudowire back and forth between two PE routers. The pseudowire status negotiation process ensures that a PE router reverts back to the label withdraw method for pseudowire status if its remote PE router neighbor does not support the pseudowire status TLV.
- The MC-LAG devices use Inter-Chassis Control Protocol (ICCP) to exchange the control information between two MC-LAG network devices.

Keep the following points in mind when you configure MC-LAG in an active-active bridging domain:

- A single bridge domain cannot be associated with two redundancy groups. You cannot configure a bridge domain to contain logical interfaces from two different multichassis aggregated Ethernet interfaces and associate them with different redundancy group IDs by using the **redundancy group group-id** statement at the **[edit interfaces ae*X* aggregated-ether-options]** hierarchy level.

- You must configure logical interfaces in a bridge domain from a single multichassis aggregated Ethernet interface and associate it with a redundancy group. You must configure a service ID by including the **service-id *vid*** statement at the **[edit bridge-domains *bd-name*]** hierarchy level for multichassis aggregated Ethernet interfaces if you configure logical interfaces on multichassis aggregated Ethernet interfaces that are part of the bridge domain.

For a multichassis link aggregation group (MC-LAG) configured in an active-active bridge domain and with VRRP configured over an IRB interface, you must include the **accept-data** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]** hierarchy level to enable the router that functions as the master router to accept all packets destined for the virtual IP address.

On an MC-LAG, if you modify the source MAC address to be the virtual MAC address, you must specify the virtual IP address as the source IP address instead of the physical IP address. In such a case, the **accept-data** option is required for VRRP to prevent ARP from performing an incorrect mapping between IP and MAC addresses for customer edge (CE) devices. The **accept-data** attribute is needed for VRRP over IRB interfaces in MC-LAG to enable OSPF or other Layer 3 protocols and applications to work properly over multichassis aggregated Ethernet (mc-aeX) interfaces.

NOTE: On an MC-LAG, the unit number associated with aggregated Ethernet interfaces on provider edge router PE1 must match the unit number associated with aggregated Ethernet interfaces on provider edge router PE2. If the unit numbers differ, MAC address synchronization does not happen. As a result, the status of the MAC address on the remote provider edge router remains in a pending state.

In an IPv6 network, you cannot configure an MC-LAG in an active-active bridge domain if you specified the **vlan-id none** statement at the **[edit bridge-domain *bd-name*]** hierarchy level. The **vlan-id none** statement that enables the removal of the incoming VLAN tags identifying a Layer 2 logical interface when packets are sent over VPLS pseudowires is not supported for IPv6 packets in an MC-LAG.

The topologies shown in Figure 2 on page 66 and Figure 3 on page 66 are supported. These figures use the following abbreviations:

- Aggregated Ethernet (AE)
- Interchassis link (ICL)
- Multichassis link (MCL)

Figure 2: Single Multichassis Link

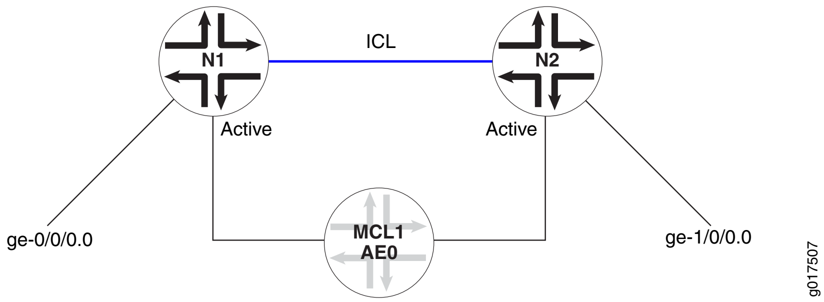
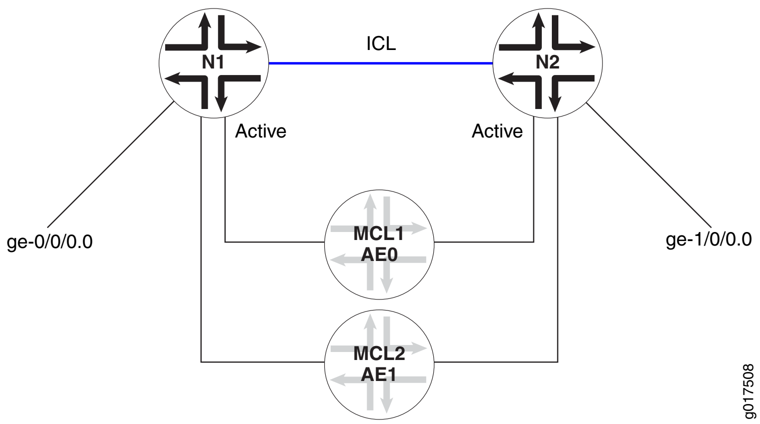


Figure 3: Dual Multichassis Link



The following functionality is *not* supported:

- Virtual private LAN service (VPLS) within the core
- Bridged core
- Topology as described in Rule 4 of “Data Traffic Forwarding Rules” on page 69
- Routed multichassis aggregated Ethernet interface, where the VRRP backup router is used in the edge of the network
- Track object, where in the case of an MC-LAG, the status of the uplinks from the provider edge can be monitored, and the MC-LAG can act on the status
- Mixed mode (active-active MC-LAG is supported on MX Series routers with MPC or MIC interfaces only). All interfaces in the bridge domain that are multichassis aggregated Ethernet active-active must be on MPC or MICs.

The topologies shown in Figure 4 on page 67, Figure 5 on page 67, and Figure 6 on page 67 are *not* supported:

Figure 4: Interchassis Data Link Between Active-Active Nodes

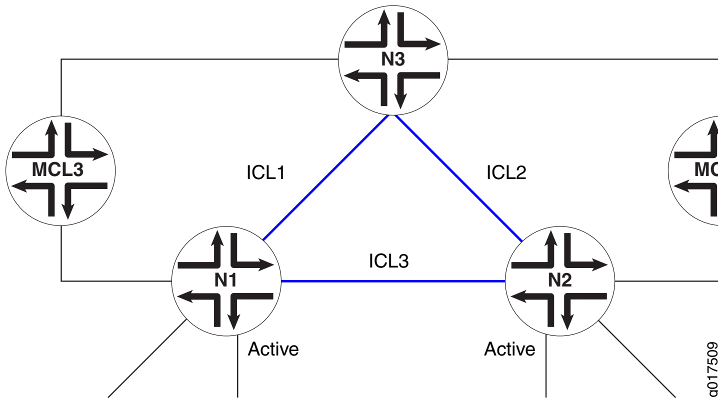


Figure 5: Active-Active MC-LAG with Single MC-LAG

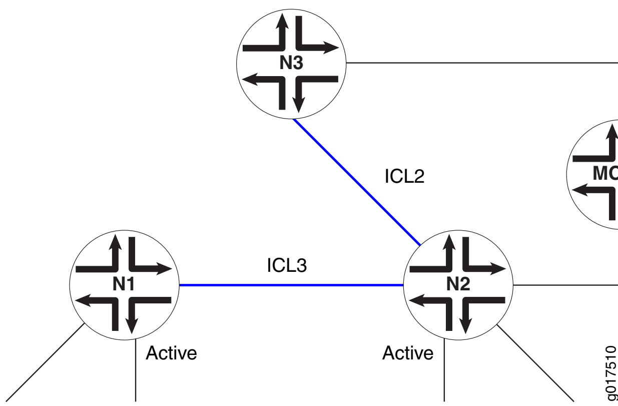
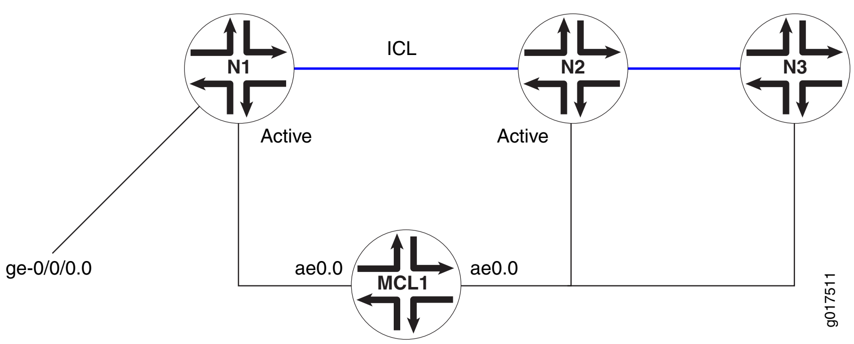


Figure 6: Active-Active MC-LAG with Multiple Nodes on a Single Multichassis Link



NOTE: A redundancy group cannot span more than two routers.

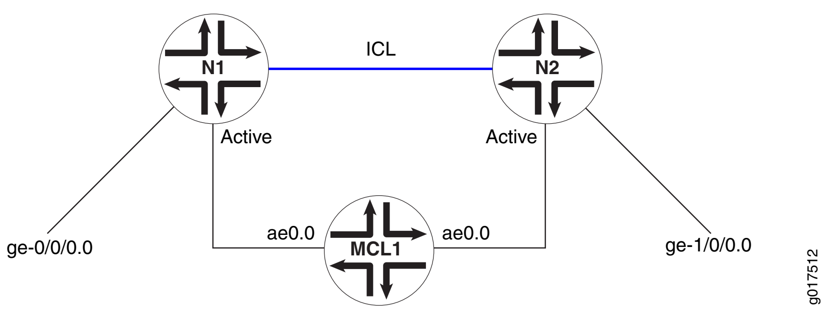
When configured to be active-active, the client device load-balances the traffic to the peering MC-LAG network devices. In a bridging environment, this could potentially cause the following problems:

- Traffic received on the MC-LAG from one MC-LAG network device could be looped back to the same MC-LAG on the other MC-LAG network device.
- Duplicated packets could be received by the MC-LAG client device.
- Traffic could be unnecessarily forwarded on the interchassis link.

To better illustrate the problems listed, consider Figure 7 on page 68, where an MC-LAG device MCL1 and single-homed clients ge-0/0/0.0 and ge-1/0/0.0 are allowed to talk to each other through an ICL.

- Traffic received on network routing instance N1 from MCL1 could be flooded to ICL to reach network routing instance N2. Once it reaches network routing instance N2, it could flood again to MCL1.
- Traffic received on interface ge-0/0/0.0 could be flooded to MCL1 and ICL on network routing instance N1. Once network routing instance N2 receives such traffic from ICL, it could again be flooded to MCL1.
- If interface ge-1/0/0.0 does not exist on network routing instance N2, traffic received from interface ge-0/0/0.0 or MCL1 on network routing instance N1 could be flooded to network routing instance N2 through ICL unnecessarily since interface ge-0/0/0.0 and MCL1 could reach each other through network routing instance N1.

Figure 7: MC-LAG Device and Single-Homed Client



Advantages of Using Multichassis Link Aggregation Groups

An MC-LAG reduces operational expenses by providing active-active links with a LAG, eliminates the need for Spanning Tree Protocol (STP), and provides faster Layer 2 convergence upon link and device failures.

An MC-LAG adds node-level redundancy to the normal link-level redundancy that a LAG provides. An MC-LAG improves network resiliency, which reduces network down time as well as expenses.

In data centers, it is desirable for servers to have redundant connections to the network. You probably want active-active connections along with links from any server to at least two separate routers.

An MC-LAG allows you to bond two or more physical links into a logical link between two routers or between a server and a router, which improves network efficiency. An MC-LAG enables you to load-balance traffic on multiple physical links. If a link fails, the traffic can be forwarded through the other available link, and the logical aggregated link remains in the UP state.

Data Traffic Forwarding Rules

In active-active bridging and VRRP over IRB topographies, network interfaces are categorized into three different interface types, as follows:

S-Links—Single-homed link (S-Link) terminating on MC-LAG-N device or MC-LAG in active-standby mode. In Figure 7 on page 68, interfaces ge-0/0/0.0 and ge-1/0/0.0 are S-Links.

MC-Links—MC-LAG links. In Figure 7 on page 68, interface ae0.0 is the MC-Link.

ICL—Interchassis link.

Based on incoming and outgoing interface types, some constraints are added to the Layer 2 forwarding rules for MC-LAG configurations, as described in the data traffic forwarding rules. Note that if only one of the MC-LAG member link is in the UP state, it is considered an S-Link.

The following data traffic forwarding rules apply:

1. When an MC-LAG network receives a packet from a local MC-Link or S-Link, the packet is forwarded to other local interfaces, including S-Links and MC-Links based on the normal Layer 2 forwarding rules and on the configuration of the **mesh-group** and **no-local-switching** statements. If MC-Links and S-Links are in the same mesh group and their **no-local-switching** statements are enabled, the received packets are only forwarded upstream and not sent to MC-Links and S-Links.

   NOTE: The functionality described in Rule 2 is *not* supported.

2. The following circumstances determine whether or not an ICL receives a packet from a local MC-Link or S-Link:

   a. If the peer MC-LAG network device has S-Links or MC-LAGs that do not reside on the local MC-LAG network device.

   b. Whether or not interfaces on two peering MC-LAG network devices are allowed to talk to each other only if both a. and b. are true. Traffic is always forwarded to the ICL.

3. When an MC-LAG network receives a packet from the ICL, the packet is forwarded to all local S-Links and active MC-LAGs that do not exist in the MC-LAG network that the packet comes from.

4. NOTE: The topology shown in Figure 8 on page 70 is *not* supported.

In certain cases, for example the topology shown in Figure 8 on page 70, there could be a loop caused by the ICL. To break the loop, one of the following mechanisms could be used:

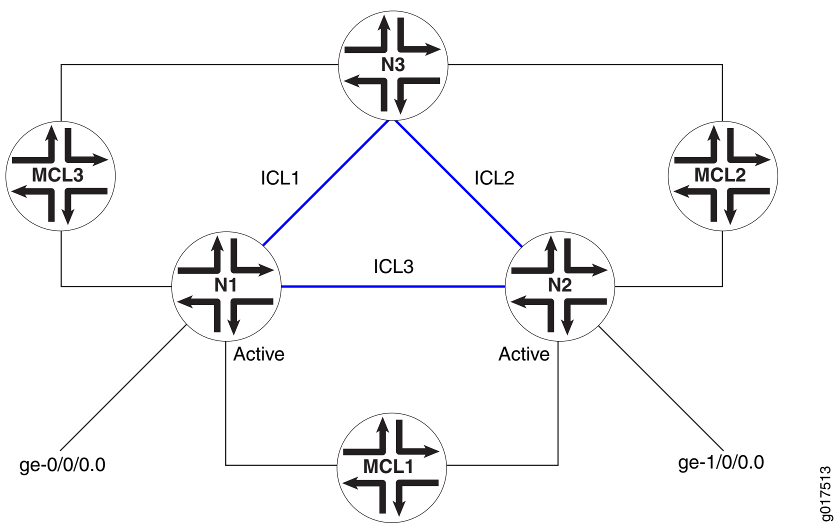
a. Run certain protocols, such as STP. In this case, whether packets received on one ICL are forwarded to other ICLs is determined by using Rule 3.

b. Configure the ICL to be fully meshed among the MC-LAG network devices. In this case, traffic received on the ICL would not be forwarded to any other ICLs.

In either case, duplicate packets could be forwarded to the MC-LAG clients. Consider the topology shown in Figure 8 on page 70, where if network routing instance N1 receives a packet from ge-0/0/0.0, it could be flooded to ICL1 and ICL3.

When receiving from ICL1 and ICL3, network routing instances N3 and N2 could flood the same packet to MCL2, as shown in Figure 8 on page 70. To prevent this from happening, the ICL designated forwarder should be elected between MC-LAG peers, and traffic received on an ICL could be forwarded to the active-active MC-LAG client by the designated forwarder only.

Figure 8: Loop Caused by the ICL Links



5. When received from an ICL, traffic should not be forwarded to the core-facing client link connection between two provider edge (PE) devices (MC-Link) if the peer chassis's (where the traffic is coming from) MC-Link is UP.

MAC Address Management

If an MC-LAG is configured to be active-active, upstream and downstream traffic could go through different MC-LAG network devices. Since the media access control (MAC) address is learned only on one of the MC-LAG network devices, the reverse direction's traffic could be going through the other MC-LAG network and be flooded unnecessarily. Also, a single-homed client's MAC address is only learned on the MC-LAG network device it is attached to. If a client attached to the peer MC-LAG network needs to communicate with that single-homed client, then traffic would be flooded on the peer MC-LAG network device. To avoid unnecessary flooding, whenever a MAC address is learned on one of the MC-LAG network devices, it gets replicated to the peer MC-LAG network device. The following conditions should be applied when MAC address replication is performed:

- MAC addresses learned on an MC-LAG of one MC-LAG network device should be replicated as learned on the same MC-LAG of the peer MC-LAG network device.
- MAC addresses learned on single-homed customer edge (CE) clients of one MC-LAG network device should be replicated as learned on the ICL-PL interface of the peer MC-LAG network device.
- MAC addresses learned on MC-LAG VE clients of one MC-LAG network device should be replicated as learned on the corresponding VE interface of the peer MC-LAG network device.
- MAC address learning on an ICL is disabled from the data path. It depends on software to install MAC addresses replicated through Inter-Chassis Control Protocol (ICCP).

MAC Aging

MAC aging support in Junos OS extends aggregated Ethernet logic for a specified MC-LAG. A MAC address in software is deleted until all Packet Forwarding Engines have deleted the MAC address. In the case of an MC-LAG, a remote provider edge is treated as a remote Packet Forwarding Engine and has a bit in the MAC data structure.

Layer 3 Routing

In general, when an MC-LAG is configured to provide Layer 3 routing functions to downstream clients, the MC-LAG network peers should be configured to provide the same gateway address to the downstream clients. To the upstream routers, the MC-LAG network peers could be viewed as either equal-cost multipath (ECMP) or two routes with different preference values.

Junos OS supports active-active MC-LAGs by using VRRP over IRB. Junos OS also supports active-active MC-LAGs by using IRB MAC address synchronization. You must configure IRB using the same IP address across MC-LAG peers. IRB MAC synchronization is supported on 32-bit interfaces and interoperates with earlier MPC and MIC releases.

To ensure that Layer 3 operates properly, instead of dropping the Layer 3 packet, the VRRP backup attempts to perform routing functions if the packet is received on an MC-LAG. A VRRP backup sends and responds to Address Resolution Protocol (ARP) requests.

For ARP, the same issue exists as with Layer 2 MAC addresses. Once ARP is learned, it must be replicated to the MC-LAG through ICCP. The peer must install an ARP route based on the ARP information received through ICCP.

For ARP aging, ARP requests on the MC-LAG peers can be aged out independently.

Address Resolution Protocol Active-Active MC-LAG Support Methodology

Suppose one of the PE routers issues an ARP request and another PE router gets the response and, because of the aggregated Ethernet distribution logic, the ARP resolution is not successful. Junos OS uses ARP response packet snooping to perform active-active multichassis link aggregation group support, providing easy synchronization without the need to maintain any specific state.

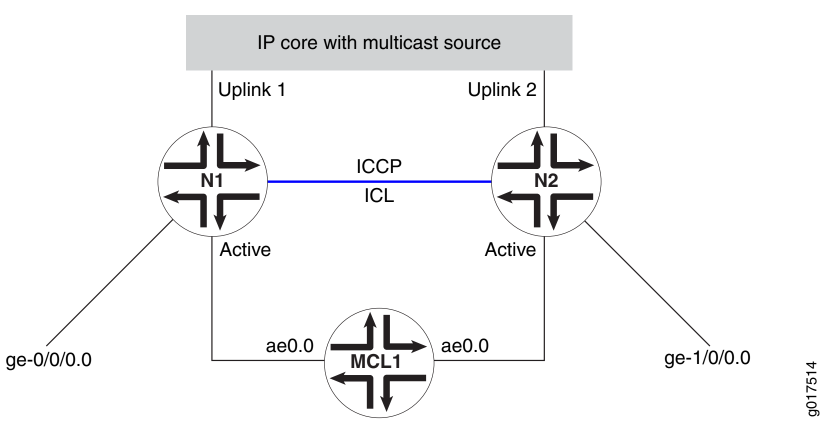
IGMP Snooping on Active-Active MC-LAG

For multicast to work in an active-active MC-LAG scenario, the typical topology is as shown in Figure 9 on page 72 and Figure 10 on page 73 with interested receivers over S-links and MC-Links. Starting in Junos OS Release 11.2, support is extended for sources connected over the Layer 2 interface.

If an MC-LAG is configured to be active-active, reports from MC-LAG clients could reach any of the MC-LAG network device peers. Therefore, the IGMP snooping module needs to replicate the states such that the Layer 2 multicast route state on both peers are the same. Additionally for S-Link clients, snooping needs to replicate these joins to its snooping peer, which in the case of Layer 3 connected source, passes this information to the PIM on IRB to enable the designated router to pull traffic for these groups,

The ICL should be configured as a router facing interface. For the scenario where traffic arrives through a Layer 3 interface, it is a requirement to have PIM and IGMP enabled on the IRB interface configured on the MC-LAG network device peers.

Figure 9: Multicast Topology with Source Connected Through Layer 3



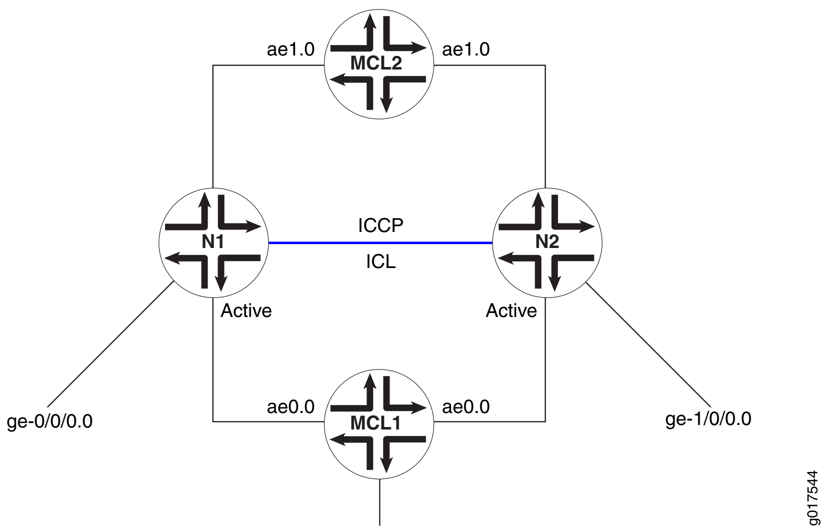
With reference to Figure 9 on page 72, either Device N1 or N2 becomes a designated router (for this example, N1 is the designated router). Router N1 therefore pulls the multicast traffic from the core. Once multicast data hits the network Device N1, the data is forwarded based on the snooping learned route.

For MC-Link clients, data is forwarded through N1. In the case of failover of the MC-Links, the data reaches the client through N2. For S-Link clients on N1, data would be forwarded through normal snooping routes.

For S-Link clients on N2, data is forwarded through the ICL interface. Layer 2 multicast routes on N1 do not show these groups unless there is interest for the same group over MC-Links or over S-Links on N1. For the IRB scenario, the IGMP membership and Layer 3 multicast route on N1 does however show these groups learned over the IRB interface.

Therefore, for a case where a specific group interest is only on the S-Link on N2, data arriving on N1 reaches N2 through the default route, and the Layer 2 multicast route on N2 has the S-Link in the outgoing interface list.

Figure 10: Multicast Topology with Source Connected Through MC-Link



In Figure 10 on page 73, MCL1 and MCL2 are on different devices, and the multicast source or IGMP querier is connected through MCL2. The data forwarding behavior seen is similar to that explained for multicast topology with source connected through Layer 3.

NOTE: **IGMP snooping should not be configured in proxy mode. There should be no IGMP hosts or IGMP or PIM routers sitting on the ICL interface.**

Up and Down Event Handling

The following conditions apply to up and down event handling:

- If the Inter-Chassis Control Protocol (ICCP) connection is UP but the ICL interface goes DOWN, the router configured as the backup brings down all the multichassis aggregated Ethernet interfaces shared with the peer that is connected to ICL. This ensures that there are no loops in the network. Otherwise, both PEs become PIM-designated routers and, hence, forward multiple copies of the same packet to the customer edge.
- If the ICCP connection is UP and the ICL comes UP, the router configured as the backup brings up the multichassis aggregated Ethernet interfaces shared with the peer.

- If both the ICCP connection and the ICL are DOWN, the router configured as the backup brings up the multichassis aggregated Ethernet interfaces shared with the peer.
- The Layer 2 address learn daemon (l2ald) does not store the information about a MAC address learned from a peer in the kernel. If l2ald restarts, and if the MAC address was not learned from the local multichassis aggregated Ethernet interface, l2ald clears the MAC addresses, which causes the router to flood the packets destined to this MAC address. This behavior is similar to that in a Routing Engine switchover. (Note that currently l2ald runs on a Routing Engine only when it is a master). Also, during the time l2ald is DOWN, ARP packets received from an ICCP peer are dropped. ARP retry takes care of this situation. This is the case with Routing Engine switchover, too.
- If ICCP restarts, l2ald does not identify that a MAC address was learned from a peer and, if the MAC address was learned only from the peer, that MAC address is deleted, and the packets destined to this MAC address are flooded.

VRRP Active-Standby Support

VRRP in active-standby mode enables Layer 3 routing over the multichassis aggregated Ethernet interfaces on the MC-LAG peers. In this mode, the MC-LAG peers act as virtual routers. The virtual routers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG. This virtual IP address, known as a routed VLAN interface (RVI), maps to either of the VRRP MAC addresses or the logical interfaces of the MC-LAG peers. The host or server uses the VRRP MAC address to send any Layer 3 upstream packets. At any time, one of the VRRP routers is the master (active), and the other is a backup (standby). Both VRRP active and VRRP backup routers forward Layer 3 traffic arriving on the multichassis aggregated Ethernet interface. If the master router fails, all the traffic shifts to the multichassis aggregated Ethernet link on the backup router.

NOTE: **You must configure VRRP on both MC-LAG peers for both the active and standby members to accept and route packets. Additionally, configure the VRRP backup router to send and receive ARP requests.**

Routing protocols run on the primary IP address of the RVI, and both of the MC-LAG peers run routing protocols independently. The routing protocols use the primary IP address of the RVI and the RVI MAC address to communicate with the MC-LAG peers. The RVI MAC address of each MC-LAG peer is replicated on the other MC-LAG peer and is installed as a MAC address that has been learned on the ICL-PL.

In many cases, MC-LAG devices are Layer 3 routing devices and perform the default gateway functionality for hosts that are part of the attached IP subnets. The MC-LAG device-pair can therefore share the default gateway routing functionality with the VRRP protocol. The VRRP active-standby operation can be optimized to be an active-active mode of processing because traffic flowing from an MC-LAG client to an MC-LAG device is always sent on one of the available links of an MC-LAG and reaches exactly one of the MC-LAG destination devices. Because of this behavior, both MC-LAG devices in the pair can be enabled as routers for IP traffic destined to the VRRP destination MAC address.

Both MC-LAG devices must be full members of the routing domain and have routing entries that allow them to reach the IP destination networks.

The active-active functionality works without changing any VRRP state machine and by activating the routing function in the forwarding plane of the VRRP backup system (similar to the VRRP master). The mechanism enables traffic forwarding in Layer 3 to be fully redundant, leveraging all available link bandwidth. All routers forward traffic and thereby load-share routed traffic.

Inter-Chassis Control Protocol

Inter-Chassis Control Protocol (ICCP) is used to synchronize configurations, states, and data.

ICCP supports the following types of state information:

- MC-LAG members and their operational states
- Single-homed members and their operational states

ICCP supports the following application database synchronization parameters:

- MAC addresses learned and to be aged
- ARP information learned over IRB

Inter-Chassis Control Protocol Message

ICCP messages and attribute-value pairs (AVPs) are used for synchronizing MAC address and ARP information.

Related Documentation

- Configuring Multichassis Link Aggregation on MX Series Routers on page 27
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers on page 87
- *multi-chassis-protection*
- *peer*
- *show interfaces mc-ae*
- *Ethernet Interfaces*

Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers

Supported Platforms MX Series

The following sections describe the configuration of active-active bridging and VRRP over IRB in multichassis link aggregation (MC-LAG) on MX Series routers:

Configuring MC-LAG

Supported Platforms MX Series

An MC-LAG is composed of logical link aggregation groups (LAGs) and is configured under the **[edit interfaces ae*X*]** hierarchy, as follows:

```
[edit]
interfaces {
  ae0 {
    encapsulation ethernet-bridge;
    multi-chassis-protection {
      peer 10.10.10.10 {
        interface ge-0/0/0;
        }
      }
    aggregated-ether-options {
      mc-ae {
        mode active-active; # see note below
      }
    }
  }
}
```

NOTE: **The mode active-active statement is valid only if encapsulation is an ethernet-bridge or extended-vlan-bridge.**

Use the **mode** statement to specify if an MC-LAG is **active-standby** or **active-active**. If the ICCP connection is UP and ICL comes UP, the router configured as standby brings up the multichassis aggregated Ethernet interfaces shared with the peer.

Using **multi-chassis-protection** at the physical interface level is a way to reduce the configuration at the logical interface level.

If there are n+1 logical interfaces under ae0, from ae0.0 through ae0.n, there are n+1 logical interfaces under ge-0/0/0 as well, from ge-0/0/0.0 through ge-0/0/0.n, each ge-0/0/0 logical interface is a protection link for the **ae0** logical interface.

NOTE: A bridge domain cannot have multichassis aggregated Ethernet logical interfaces that belong to different redundancy groups.

Configuring the Interchassis Link-Protection Link

Supported Platforms MX Series

The interchassis link-protection link (ICL-PL) provides redundancy when a link failure (for example, an MC-LAG trunk failure) occurs on one of the active links. The ICL-PL is an aggregated Ethernet interface. You can configure only one ICL-PL between the two peers, although you can configure multiple MC-LAGs between them.

The ICL-PL assumes interface ge-0/0/0.0 is used to protect interface ae0.0 of MC-LAG-1:

```
[edit]
interfaces {
  ae0 {
    ....
    unit 0 {
      multi-chassis-protection {
        peer 10.10.10.10 {
          interface ge-0/0/0.0;
        }
        ....
      }
      ...
    }
  }
}
```

The protection interface can be an Ethernet type interface such as ge, or xe, or an aggregated Ethernet (ae) interface.

Configuring Multiple Chassis

Supported Platforms MX Series

A top-level hierarchy is used to specify a multichassis-related configuration, as follows:

```
[edit]
multi-chassis {
  multi-chassis-protection {
    peer 10.10.10.10 {
      interface ge-0/0/0;
    }
  }
}
```

This example specifies interface ge-0/0/0 as the multichassis protection interface for all the multichassis aggregated Ethernet interfaces which are also part of the peer. This can be overridden by specifying protection at the physical interface level and the logical interface level.

Configuring the Service ID

Supported Platforms MX Series

You must configure the same unique network-wide configuration for a service in the set of PE routers providing the service. You can configure the service IDs under the level of the hierarchies shown in the following examples:

Global Configuration (Default Logical System)

```
switch-options {
  service-id 10;
}
bridge-domains {
  bd0 {
    service-id 2;
  }
}
routing-instances {
  r1 {
    switch-options {
      service-id 10;
    }
    bridge-domains {
      bd0 {
        service-id 2;
      }
    }
  }
}
```

Logical Systems

```
ls1 {
  switch-options {
    service-id 10;
  }
  routing-instances {
    r1 {
      switch-options {
        service-id 10;
      }
    }
  }
}
```

NOTE: Using a service name per bridge domain is not supported.

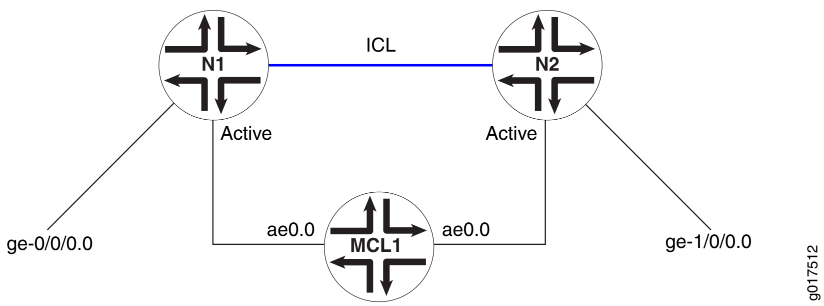
The bridge-level service ID is required to link related bridge domains across peers, and should be configured with the same value. The **service-id** values share the name space across all bridging and routing instances, and across peers. Thus, duplicate values for service IDs are not permitted across these entities.

The service ID at the bridge domain level is mandatory for type non-single VLAN bridge domains. The service ID is optional for bridge domains with a VID defined. If no service ID is defined in the latter case, it is picked up from the service ID configuration for that routing instance.

NOTE: When this default routing instance (or any other routing instance) which contains a bridge domain containing an multichassis aggregated Ethernet interface is configured, you must configure a global level **switch-options service-id** *number*, irrespective of whether the contained bridge domains have specific service IDs configured.

In the sample illustration shown in Figure 11 on page 79, network routing instances N1 and N2, both for the same service ID, are configured with same service-ID in both N1 and N2. Use of a name string instead of a number is not supported.

Figure 11: N1 and N2 for the Same Service with Same Service ID

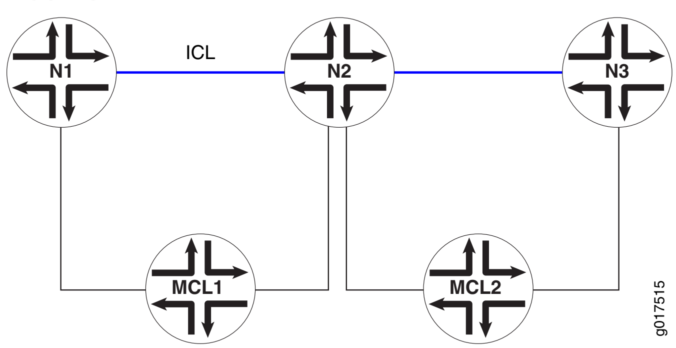


The following configuration restrictions apply:

- The service ID must be configured when the multichassis aggregated Ethernet interface is configured and a multichassis aggregated Ethernet logical interface is part of a bridge domain. This requirement is enforced.
- A single bridge domain cannot correspond to two redundancy group IDs.

  In Figure 12 on page 79, it is possible to configure a bridge domain consisting of logical interfaces from two multichassis aggregated Ethernet interfaces and map them to a separate redundancy group ID, which is not supported. A service must be mapped one-to-one with the redundancy group providing the service. This requirement is enforced.

Figure 12: Bridge Domain with Logical Interfaces from Two Multichassis Aggregated Ethernet Interfaces



To display the multichassis aggregated Ethernet configuration, use the **show interfaces *mc-ae*** command. For more information, see the CLI Explorer.

Configuring IGMP Snooping for Active-Active MC-LAG

Supported Platforms

For the multicast solution to work, the following must be configured:

- The multichassis protection link must be configured as a router-facing interface.

```
[edit bridge-domain bd-name]
protocols {
  igmp-snooping {
    interface ge-0/0/0.0 {
      multicast-router-interface;
    }
  }
}
```

  In this example, ge-0/0/0.0 is an ICL interface.

- The ***multichassis-lag-replicate-state*** statement options must be configured under the ***multicast-snooping-options*** statement for that bridge domain.

NOTE: Snooping with active-active MC-LAG is only supported in non-proxy mode.

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63
- Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers on page 87
- Configuring Multichassis Link Aggregation on MX Series Routers on page 27
- **mc-ae on page 363**
- *multi-chassis-protection*
- *peer*
- *show interfaces irb*
- *show interfaces mc-ae*
- *Ethernet Interfaces*

Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers

Supported Platforms MX240, MX480, MX960

You can use the **bridge-domain** statement's **service-id** option to specify the multichassis aggregated Ethernet configuration.

- The **service-id** statement is mandatory for non-single VLAN type bridge domains (**none**, **all** or **vlan-id-tags:dual**).
- The statement is optional for bridge domains with a VID defined.
- If no **service-id** is defined in the latter case, it is picked up from the round-trip time's (RTT's) **service-id** configuration.
- The bridge-level **service-id** is required to link related bridge domains across peers, and should be configured with the same value.
- The **service-id** values share the name space across all bridging and routing instances, and across peers. Thus, duplicate **service-id** values are not permitted across these entities.
- A change of bridge **service-id** is considered catastrophic, and the bridge domain is changed.

This procedure allows you to enable or disable the replication feature.

To configure IGMP snooping in active-standby mode:

- Use the **multichassis-lag-replicate-state** statement at the **multicast-snooping-options** hierarchy level in the master instance.

```
multicast-snooping-options {
  ...
  multichassis-lag-replicate-state; # REQUIRED
}
```

The interchassis link, **interface *icl-intf-name***, of the learning domain should be a router-facing interface.

- Use the **interface *icl-intf-name*** statement at the **protocols igmp-snooping** hierarchy level, as shown in the following example:

```
protocols {
  igmp-snooping {
    interface icl-intf-name {
      multicast-router-interface;
    }
  }
}
```

Related Documentation

- *IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview*
- *Example: Configuring IGMP Snooping*
- *igmp-snooping*
- *multicast-router-interface*
- *show l2-learning instance*
- *Ethernet Interfaces*

Example: Configuring DHCP Relay on MC- LAG with VRRP on an EX9200 Switch

Supported Platforms EX Series

This example shows how you can configure DHCP relay on EX9200 switches with the Multichassis Link Aggregation (MC-LAG) feature using the Virtual Router Redundancy Protocol (VRRP).

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.3 or later for EX Series
- Two EX9200 switches

Before you configure DHCP relay, be sure that you understand how to:

- Configure MC-LAG and verify that MC-LAG and ICCP is up and running

To complete the configuration, enable VRRP by completing the following steps for each MC-LAG:

- Create a Integrated Routing and Bridging (IRB) interface
- Create a VRRP group and assign a virtual IP address that is shared between each switch in the VRRP group
- Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group
- Configure Layer 3 connectivity between the VRRP groups

Overview

In this example, you configure DHCP relay with MC-LAG across two switches, consisting of two EX9200 switches, an interchassis control link-protection link (ICL-PL), multichassis protection link for the ICL-PL, ICCP for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers. Layer 3 connectivity is required for ICCP.

NOTE: On EX9200 switches, dynamic ARP resolution is not supported over inter-chassis control links (ICLs). As a workaround, you can configure static ARP on both ends of the ICL.

Topology

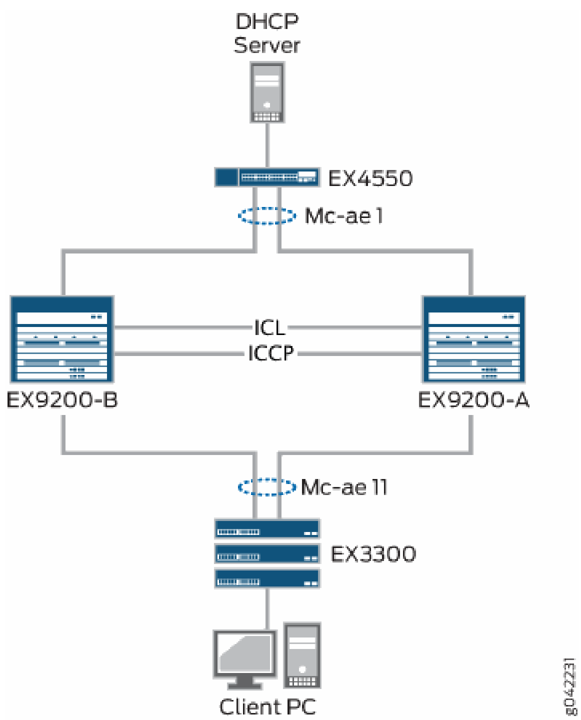


Table 9: Components of the topology for Configuring DHCP Relay

Hostname	Hardware
Swtich 9200-A	EX9200 switch
Switch 9200-B	EX9200 switch

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the [edit forwarding-options] hierarchy level of Switch A.

```
[edit]
set forwarding-options dhcp-relay forward-snooped-clients all-interfaces
set forwarding-options dhcp-relay server-group GVP-DHCP 10.168.61.5
set forwarding-options dhcp-relay overrides allow-snooped-clients
set forwarding-options dhcp-relay active-server-group GVP-DHCP
set forwarding-options dhcp-relay group Floor1 interface irb.2540
set forwarding-options dhcp-relay route-suppression destination
```

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the [edit forwarding-options] hierarchy level of Switch B.

```
[edit]
set forwarding-options dhcp-relay forward-snooped-clients all-interfaces
set forwarding-options dhcp-relay server-group GVP-DHCP 10.168.61.5
set forwarding-options dhcp-relay overrides allow-snooped-clients
set forwarding-options dhcp-relay active-server-group GVP-DHCP
set forwarding-options dhcp-relay group Floor1 interface irb.2540
set forwarding-options dhcp-relay route-suppression destination
```

Step-by-Step Procedure

To configure DHCP relay on Switch A :

1. Configure forward snooped (unicast) packets on interfaces.

   ```
   [edit]
   set forwarding-options dhcp-relay forward-snooped-clients all-interfaces
   ```
2. Create a DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

   ```
   set forwarding-options dhcp-relay server-group GVP-DHCP 10.168.61.5
   ```
3. Allow the creation of a binding entry using snooped (unicast) clients:

   ```
   set forwarding-options dhcp-relay overrides allow-snooped-clients
   ```
4. Apply a DHCP relay agent configuration to the named group of DHCP server addresses:

   ```
   set forwarding-options dhcp-relay active-server-group GVP-DHCP
   ```
5. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

   ```
   set forwarding-options dhcp-relay group Floor1 interface irb.2540
   ```
6. Configure the relay agent to suppress the installation of ARP and route entries for corresponding client binding:

   ```
   set forwarding-options dhcp-relay route-suppression destination
   ```

Step-by-Step Procedure

To configure DHCP relay on Switch B :

1. Configure forward snooped (unicast) packets on interfaces.

   ```
   [edit]
   set forwarding-options dhcp-relay forward-snooped-clients all-interfaces
   ```
2. Create a DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

   ```
   set forwarding-options dhcp-relay server-group GVP-DHCP 10.168.61.5
   ```
3. Allow the creation of a binding entry using snooped (unicast) clients:

   ```
   set forwarding-options dhcp-relay overrides allow-snooped-clients
   ```
4. Apply a DHCP relay agent configuration to the named group of DHCP server addresses:

   ```
   set forwarding-options dhcp-relay active-server-group GVP-DHCP
   ```
5. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

   ```
   set forwarding-options dhcp-relay group Floor1 interface irb.2540
   ```
6. Configure the relay agent to suppress the installation of ARP and route entries for corresponding client binding:

set forwarding-options dhcp-relay route-suppression destination

Results

Display the results of the configuration on Switch A.

```
root@CORE-A# show
dhcp-relay {
  forward-snooped-clients all-interfaces;
  overrides {
    allow-snooped-clients;
  }
  server-group {
    GVP-DHCP {
      10.168.61.5;
    }
active-server-group GVP-DHCP;
  group Floor1 {
    interface irb.2540;
  }
```

Display the results of the configuration on Switch B.

```
root@CORE-B# show
dhcp-relay {
  forward-snooped-clients all-interfaces;
  overrides {
    allow-snooped-clients;
  }
  server-group {
    GVP-DHCP {
      10.168.61.5;
    }
active-server-group GVP-DHCP;
  group Floor1 {
    interface irb.2540;
  }
```

Overwriting Address Information

Step-by-Step Procedure

We recommend that you configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server. To overwrite the address of every DHCP packet with the address of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the address of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

Verification

- Check whether DHCP Relay Binding is happening on page 86
- Check whether relay statistics are being displayed on page 86

Check whether DHCP Relay Binding is happening

Purpose To check whether address bindings in the Dynamic Host Configuration Protocol (DHCP) client table are being displayed.

Action On Switch A, run the following command:

```
root@CORE-A# run show dhcp relay binding detail
Client IP Address:  10.168.103.20
Hardware Address:             84:18:88:a8:ca:80
State:            BOUND(RELAY_STATE_BOUND)
Lease Expires:                2013-10-03 12:17:43 CEST
Lease Expires in:             85829 seconds
Lease Start:                  2013-10-02 10:48:34 CEST
Last Packet Received:         2013-10-02 12:17:43 CEST
Incoming Client Interface:    ae0.0(irb.2540)
Server Ip Address:            10.168.61.5
Server Interface:             none
Bootp Relay Address:          10.168.103.2
Session Id:                   29
```

On Switch B, run the following command:

```
root@CORE-A# run show dhcp relay binding detail
Client IP Address:  10.168.103.20
Hardware Address:             84:18:88:a8:ca:80
State:            BOUND(RELAY_STATE_BOUND)
Lease Expires:                2013-10-03 12:17:43 CEST
Lease Expires in:             86228 seconds
Lease Start:                  2013-10-02 10:48:34 CEST
Last Packet Received:         2013-10-02 10:48:34 CEST
Incoming Client Interface:    ae11.0(irb.2540)
Server Ip Address:            10.168.61.5
Server Interface:             none
Bootp Relay Address:          10.168.103.2
Session Id:                   16
```

Meaning The field State indicates the state of DHCP relay address binding table on the DHCP client. The state BOUND indicates that the client has an active IP address lease.

Check whether relay statistics are being displayed

Purpose To check whether DHCP relay statistics are being displayed.

Action On Switch A, run the following command:

```
root@CORE-A# run show dhcp relay statistics
Packets dropped:
 Total                      9
 dhcp-service total         9
Messages received:
    BOOTREQUEST                4
    DHCPDECLINE                0
    DHCPDISCOVER               1
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                3

Messages sent:
    BOOTREPLY                  0
    DHCPOFFER                  0
    DHCPACK                    0
    DHCPNAK                    0
    DHCPFORCERENEW             0
```

Meaning The field Total displays the total number of packets discarded by the extended DHCP relay agent application.

Related Documentation

- Configuring Multichassis Link Aggregation on EX Series Switches on page 32
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on EX9200 Switches on page 130

Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers

Supported Platforms MX240, MX480, MX960

This example shows how to configure a multichassis link aggregation group (MC-LAG) in an active-active scenario, which load balances traffic across the PEs.

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks MX Series routers
- Junos OS Release 11.2 or later running on all four routers

Overview

Consider a sample topology in which a customer edge router, CE, is connected to two provider edge (PE) routers, PE1 and PE2, respectively. The two PE devices each have a link aggregation group (LAG) connected to the CE device. The configured mode is active -active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time. PE1 and PE2 are connected to a single service provider router, P.

In this example, the CE router is not aware that its aggregated Ethernet links are connected to two separate PE devices. The two PE devices each have a LAG connected to the CE device. The configured mode is active-active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time.

In Figure 13 on page 89, from the perspective of Router CE, all four ports belonging to a LAG are connected to a single service provider device. Because the configured mode is active-active, all four ports are active, and the CE device load-balances the traffic to the peering PE devices. On the PE routers, a regular LAG is configured facing the CE device.

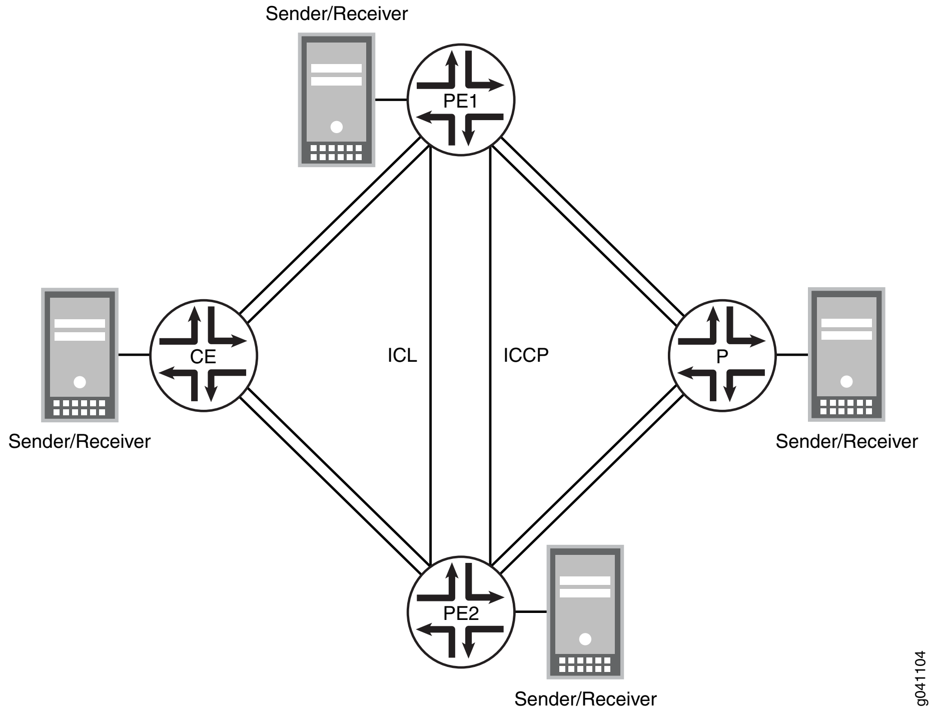
On one end of an MC-LAG is an MC-LAG client device, such as a server, that has one or more physical links in a LAG. This client device does not need to detect the MC-LAG. On the other side of an MC-LAG are two MC-LAG routers. Each of the routers has one or more physical links connected to a single client device. The routers coordinate with each other to ensure that data traffic is forwarded properly.

ICCP messages are sent between the two PE devices. In this example, you configure an MC-LAG across two routers, consisting of two aggregated Ethernet interfaces, an interchassis link-protection link (ICL-PL), multichassis protection link for the ICL-PL, and ICCP for the peers hosting the MC-LAG.

Topology Diagram

Figure 13 on page 89 shows the topology used in this example.

Figure 13: MC-LAG Active-Active on MX Series Routers



Configuring the PE Routers

CLI Quick Configuration

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

Router PE1

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/1 gigether-options 802.3ad ae1
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.1/30
set interfaces ge-1/0/6 gigether-options 802.3ad ae0
set interfaces ge-1/1/1 flexible-vlan-tagging
set interfaces ge-1/1/1 encapsulation flexible-ethernet-services
set interfaces ge-1/1/1 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/1 unit 0 vlan-id-range 100-110
set interfaces ge-1/1/4 flexible-vlan-tagging
set interfaces ge-1/1/4 encapsulation flexible-ethernet-services
set interfaces ge-1/1/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/4 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
```

```
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/1/1.0
set bridge-domains bd0 interface ge-1/1/4.0
set bridge-domains bd0 interface ae0.0
set protocols iccp local-ip-addr 100.100.100.1
set protocols iccp peer 100.100.100.2 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.2 liveness-detection minimum-interval 1000
set switch-options service-id 10
```

Router PE2

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.2/30
set interfaces ge-1/0/3 flexible-vlan-tagging
set interfaces ge-1/0/3 encapsulation flexible-ethernet-services
set interfaces ge-1/0/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/3 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/4 flexible-vlan-tagging
set interfaces ge-1/0/4 encapsulation flexible-ethernet-services
set interfaces ge-1/0/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/4 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/5 gigether-options 802.3ad ae0
set interfaces ge-1/1/0 gigether-options 802.3ad ae1
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
```



```
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/0/4.0
set bridge-domains bd0 interface ae0.0
set protocols iccp local-ip-addr 100.100.100.2
set protocols iccp peer 100.100.100.1 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.1 liveness-detection minimum-interval 1000
set switch-options service-id 10
```

Configuring the Router PE1

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router PE1:

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

   ```
   [edit chassis]
   user@PE1# set aggregated-devices ethernet device-count 5
   ```

2. Specify the members to be included within the aggregated Ethernet bundles.

   ```
   [edit interfaces]
   user@PE1# set ge-1/0/1 gigether-options 802.3ad ae1
   user@PE1# set ge-1/0/6 gigether-options 802.3ad ae0
   ```

3. Configure the interfaces that connect to senders or receivers, the ICL interfaces, and the ICCP interfaces.

   ```
   [edit interfaces]
   user@PE1# set ge-1/1/1 flexible-vlan-tagging
   user@PE1# set ge-1/1/1 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/1 unit 0 encapsulation vlan-bridge
   user@PE1# set ge-1/1/1 unit 0 vlan-id-range 100-110
   user@PE1# set ge-1/1/4 flexible-vlan-tagging
   user@PE1# set ge-1/1/4 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/4 unit 0 encapsulation vlan-bridge
   ```

```
user@PE1# set ge-1/1/4 unit 0 vlan-id-range 100-110
user@PE1# set ge-1/0/2 unit 0 family inet address 100.100.100.1/30
```

4. Configure parameters on the aggregated Ethernet bundles.

```
[edit interfaces ae0]
user@PE1# set flexible-vlan-tagging
user@PE1# set encapsulation flexible-ethernet-services
user@PE1# set unit 0 encapsulation vlan-bridge
user@PE1# set unit 0 vlan-id-range 100-110
user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0

[edit interfaces ae1]
user@PE1# set flexible-vlan-tagging
user@PE1# set encapsulation flexible-ethernet-services
user@PE1# set unit 0 encapsulation vlan-bridge
user@PE1# set unit 0 vlan-id-range 100-110
user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
```

5. Configure LACP on the aggregated Ethernet bundles.

```
[edit interfaces ae0 aggregated-ether-options]
user@PE1# set lacp active
user@PE1# set lacp system-priority 100
user@PE1# set lacp system-id 00:00:00:00:00:05
user@PE1# set lacp admin-key 1

[edit interfaces ae1 aggregated-ether-options]
user@PE1# set lacp active
user@PE1# set lacp system-priority 100
user@PE1# set lacp system-id 00:00:00:00:00:05
user@PE1# set lacp admin-key 1
```

6. Configure the MC-LAG interfaces.

```
[edit interfaces ae0 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 5
user@PE1# set mc-ae redundancy-group 10
user@PE1# set mc-ae chassis-id 1
user@PE1# set mc-ae mode active-active
user@PE1# set mc-ae status-control active

[edit interfaces ae1 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 10
user@PE1# set mc-ae redundancy-group 10
user@PE1# set mc-ae chassis-id 1
user@PE1# set mc-ae mode active-active
user@PE1# set mc-ae status-control active
```

The multichassis aggregated Ethernet identification number (**mc-ae-id**) specifies which link aggregation group the aggregated Ethernet interface belongs to. The ae0 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 5**. The ae1 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 10**. (To refer to the configuration on Router PE2, see “Router PE2” on page 90).

The **redundancy-group 10** statement is 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 ae0 and ae1 interfaces on Router PE1 and Router PE2 are configured with the same redundancy group, **redundancy-group 10**.

The **chassis-id** statement is used by LACP for calculating the port number of the MC-LAG's physical member links. Router PE1 uses **chassid-id 1** to identify both its ae0 and ae1 interfaces. Router PE2 (as shown in "Router PE2" on page 90) uses **chassis-id 0** to identify both its ae0 and ae1 interfaces.

The **mode** statement 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.

7. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@PE1# set domain-type bridge
user@PE1# set vlan-id all
user@PE1# set service-id 20
user@PE1# set interface ae0.0
user@PE1# set interface ae1.0
user@PE1# set interface ge-1/0/3.0
user@PE1# set interface ge-1/1/1.0
user@PE1# set interface ge-1/1/4.0
```

The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

The bridge-level **service-id** statement is required to link related bridge domains across peers (in this case Router PE1 and Router PE2), and must be configured with the same value.

8. Configure ICCP parameters.

```
[edit protocols iccp]
user@PE1# set local-ip-addr 100.100.100.1
user@PE1# set peer 100.100.100.2 redundancy-group-id-list 10
user@PE1# set peer 100.100.100.2 liveness-detection minimum-interval 1000
```

9. Configure the service ID at the global level.

```
[edit switch-options]
user@PE1# set service-id 10
```

You must configure the same unique network-wide configuration for a service in the set of PE routers providing the service. This service ID is required if the multichassis aggregated Ethernet interfaces are part of a bridge domain.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, **show interfaces**, **show protocols**, and **show switch-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show bridge-domains
bd0 {
    domain-type bridge;
    vlan-id all;
    service-id 20;
    interface ae1.0;
    interface ge-1/0/3.0;
    interface ge-1/1/1.0;
    interface ge-1/1/4.0;
    interface ae0.0;
}
```

```
user@PE1# show chassis
aggregated-devices {
    ethernet {
        device-count 5;
    }
}
```

```
user@PE1# show interfaces
ge-1/0/1 {
    gigether-options {
        802.3ad ae1;
    }
}
ge-1/0/6 {
    gigether-options {
        802.3ad ae0;
    }
}
ge-1/0/2 {
    unit 0 {
        family inet {
            address 100.100.100.1/30;
        }
    }
}
ge-1/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
    }
}
ge-1/1/4 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
    }
}
ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
```



```
        lacp {
            active;
            system-priority 100;
            system-id 00:00:00:00:00:05;
            admin-key 1;
        }
        mc-ae {
            mc-ae-id 5;
            redundancy-group 10;
            chassis-id 1;
            mode active-active;
            status-control active;
        }
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        lacp {
            active;
            system-priority 100;
            system-id 00:00:00:00:00:05;
            admin-key 1;
        }
        mc-ae {
            mc-ae-id 10;
            redundancy-group 10;
            chassis-id 1;
            mode active-active;
            status-control active;
        }
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
```

```
user@PE1# show protocols
iccp {
    local-ip-addr 100.100.100.1;
    peer 100.100.100.2 {
        redundancy-group-id-list 10;
        liveness-detection {
            minimum-interval 1000;
```

```
        }
      }
    }
```

user@PE1# **show switch-options**
service-id 10;

If you are done configuring the device, enter **commit** from configuration mode.

Repeat the procedure for Router PE2, using the appropriate interface names and addresses.

Configuring the CE Device

CLI Quick Configuration

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

Router CE

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-2/0/2 gigether-options 802.3ad ae0
set interfaces ge-2/0/3 gigether-options 802.3ad ae0
set interfaces ge-2/1/6 flexible-vlan-tagging
set interfaces ge-2/1/6 encapsulation flexible-ethernet-services
set interfaces ge-2/1/6 unit 0 encapsulation vlan-bridge
set interfaces ge-2/1/6 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-500
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 interface ge-2/1/6.0
set bridge-domains bd0 interface ae0.0
```

Configuring the CE Device

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the CE router:

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

   [edit chassis]
   user@CE# **set aggregated-devices ethernet device-count 2**

2. Specify the members to be included within the aggregated Ethernet bundle.

   [edit interfaces]
   user@CE# **set ge-2/0/2 gigether-options 802.3ad ae0**
   user@CE# **set ge-2/0/3 gigether-options 802.3ad ae0**

3. Configure an interface that connects to senders or receivers.

```
[edit interfaces ge-2/1/6]
user@CE# set flexible-vlan-tagging
user@CE# set encapsulation flexible-ethernet-services
user@CE# set unit 0 encapsulation vlan-bridge
user@CE# set unit 0 vlan-id-range 100-110
```

4. Configure parameters on the aggregated Ethernet bundle.

```
[edit interfaces ae0]
user@CE# set flexible-vlan-tagging
user@CE# set encapsulation flexible-ethernet-services
user@CE# set unit 0 encapsulation vlan-bridge
user@CE# set unit 0 vlan-id-range 100-500
```

5. Configure LACP on the aggregated Ethernet bundle.

```
[edit interfaces ae0 aggregated-ether-options]
user@CE# set lacp active
user@CE# set lacp system-priority 100
```

   The **active** statement initiates transmission of LACP packets.

   For the **system-priority** statement, a smaller value indicates a higher priority. The device with the lower system priority value determines which links between LACP partner devices are active and which are in standby mode for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

6. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@CE# set domain-type bridge
user@CE# set vlan-id all
user@CE# set interface ge-2/1/6.0
user@CE# set interface ae0.0
```

   The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@CE# show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  interface ge-2/1/6.0;
  interface ae0.0;
}
```

```
user@CE# show chassis
```

```
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

user@CE# **show interfaces**

```
ge-2/0/2 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/0/3 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/1/6 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-110;
  }
}
ae0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  aggregated-ether-options {
    lacp {
      active;
      system-priority 100;
    }
  }
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-500;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring the Provider Router

CLI Quick Configuration

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

Router P

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-1/0/5 gigether-options 802.3ad ae1
set interfaces ge-1/0/11 gigether-options 802.3ad ae1
set interfaces ge-1/1/3 flexible-vlan-tagging
set interfaces ge-1/1/3 encapsulation flexible-ethernet-services
set interfaces ge-1/1/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/3 unit 0 vlan-id-range 100-500
```

```
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 interface ge-1/1/3.0
set bridge-domains bd0 interface ae1.0
```

Configuring the Router P

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the router P:

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

   ```
   [edit chassis]
   user@P# set aggregated-devices ethernet device-count 2
   ```

2. Specify the members to be included within the aggregated Ethernet bundle.

   ```
   [edit interfaces]
   user@P# set ge-1/0/5 gigether-options 802.3ad ae1
   user@P# set ge-1/0/11 gigether-options 802.3ad ae1
   ```

3. Configure an interface that connects to senders or receivers.

   ```
   [edit interfaces ge-1/1/3]
   user@P# set flexible-vlan-tagging
   user@P# set encapsulation flexible-ethernet-services
   user@P# set unit 0 encapsulation vlan-bridge
   user@P# set unit 0 vlan-id-range 100-500
   ```

4. Configure parameters on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae1]
   user@P# set flexible-vlan-tagging
   user@P# set encapsulation flexible-ethernet-services
   user@P# set unit 0 encapsulation vlan-bridge
   user@P# set unit 0 vlan-id-range 100-110
   ```

5. Configure LACP on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae1 aggregated-ether-options]
   user@P# set lacp active
   user@P# set lacp system-priority 100
   ```

6. Configure a domain that includes the set of logical ports.

   ```
   [edit bridge-domains bd0]
   user@P# set vlan-id all
   user@P# set domain-type bridge
   user@P# set interface ge-1/1/3.0
   ```



```
user@P# set interface ae1.0
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@P#  show bridge-domains
bd0 {
   domain-type bridge;
   vlan-id all;
   interface ge-1/1/3.0;
   interface ae1.0;
}
```

```
user@P#  show chassis
aggregated-devices {
   ethernet {
      device-count 2;
   }
}
```

```
user@P#  show interfaces
ge-1/0/5 {
   gigether-options {
      802.3ad ae1;
   }
}
ge-1/0/11 {
   gigether-options {
      802.3ad ae1;
   }
}
ge-1/1/3 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-500;
   }
}
ae1 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   aggregated-ether-options {
      lacp {
         active;
         system-priority 100;
      }
   }
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
   }
}
```


If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly by running the following commands:

- **show iccp**
- **show interfaces ae0**
- **show interfaces ae1**
- **show interfaces mc-ae**
- ***show l2-learning instance* extensive**

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- *Configuring ICCP for MC-LAG*
- *show interfaces (Aggregated Ethernet)* in the CLI Explorer

CHAPTER 4

Enabling High Availability in Layer 3 Networks Using VRRP and MAC Synchronization for MC-LAG

Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview

Supported Platforms MX Series

MX Series routers support active-active bridging and Virtual Router Redundancy Protocol (VRRP) over integrated routing and bridging (IRB). This is a common scenario used in data centers. This section provides an overview of the supported functionality.

Active-active bridging and VRRP over IRB support extend multichassis link aggregation group (MC-LAG) by adding the following functionality:

- Interchassis link (ICL) pseudowire interface or Ethernet interface (ICL-PL field) for active-active bridging
- Active-active bridging
- VRRP over IRB for active-active bridging
- A single bridge domain not corresponding to two redundancy group IDs

The following functionalities are supported for MC-LAG in an active-active bridging domain:

- MC-LAG is supported only between two chassis, using an interchassis link (ICL) pseudowire interface or Ethernet interface (ICL-PL field) for **active-active bridging**, and **active-active bridging** VRRP over IRB for **active-active bridging**.
- For VPLS networks, you can configure the aggregated Ethernet (aeX) interfaces on MC-LAG devices with the **encapsulation ethernet-vpls** statement to use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values or the **encapsulation vlan-vpls** statement to use Ethernet VLAN encapsulation on VPLS circuits.
- Layer 2 circuit functionalities are supported with **ethernet-ccc** as the encapsulation mode.
- Network topologies in a triangular and square pattern are supported. In a triangular network design, with equal-cost paths to all redundant nodes, slower, timer-based convergence can possibly be prevented. Instead of indirect neighbor or route loss detection using hellos and dead timers, you can identify the physical link loss and denote a path as unusable and reroute all traffic to the alternate equal-cost path. In a square network design, depending on the location of the failure, the routing protocol might converge to identify a new path to the subnet or the VLAN, causing the convergence of the network to be slower.
- Interoperation of Link Aggregation Control Protocol (LACP) for MC-LAG devicess is supported. LACP is one method of bundling several physical interfaces to form one logical interface. When LACP is enabled, the local and remote sides of the aggregated Ethernet links exchange protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when the links receive the PDUs from another link. One side of the link must be configured as active for the link to be up.
- Active-standby mode is supported using LACP. When an MC-LAG operates in the active-standby mode, one of the router’s ports only becomes active when failure is detected in the active links. In this mode, the provider edge (PE) routers perform an election to determine the active and standby routers.
- Configuration of the pseudowire status type length variable (TLV) is supported. The pseudowire status TLV is used to communicate the status of a pseudowire back and forth between two PE routers. The pseudowire status negotiation process ensures that

a PE router reverts back to the label withdraw method for pseudowire status if its remote PE router neighbor does not support the pseudowire status TLV.

- The MC-LAG devices use Inter-Chassis Control Protocol (ICCP) to exchange the control information between two MC-LAG network devices.

Keep the following points in mind when you configure MC-LAG in an active-active bridging domain:

- A single bridge domain cannot be associated with two redundancy groups. You cannot configure a bridge domain to contain logical interfaces from two different multichassis aggregated Ethernet interfaces and associate them with different redundancy group IDs by using the **redundancy group group-id** statement at the **[edit interfaces ae*X* aggregated-ether-options]** hierarchy level.
- You must configure logical interfaces in a bridge domain from a single multichassis aggregated Ethernet interface and associate it with a redundancy group. You must configure a service ID by including the **service-id *vid*** statement at the **[edit bridge-domains *bd-name*]** hierarchy level for multichassis aggregated Ethernet interfaces if you configure logical interfaces on multichassis aggregated Ethernet interfaces that are part of the bridge domain.

For a multichassis link aggregation group (MC-LAG) configured in an active-active bridge domain and with VRRP configured over an IRB interface, you must include the **accept-data** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet address *address* vrrp-group *group-id*]** hierarchy level to enable the router that functions as the master router to accept all packets destined for the virtual IP address.

On an MC-LAG, if you modify the source MAC address to be the virtual MAC address, you must specify the virtual IP address as the source IP address instead of the physical IP address. In such a case, the **accept-data** option is required for VRRP to prevent ARP from performing an incorrect mapping between IP and MAC addresses for customer edge (CE) devices. The **accept-data** attribute is needed for VRRP over IRB interfaces in MC-LAG to enable OSPF or other Layer 3 protocols and applications to work properly over multichassis aggregated Ethernet (mc-aeX) interfaces.

NOTE: On an MC-LAG, the unit number associated with aggregated Ethernet interfaces on provider edge router PE1 must match the unit number associated with aggregated Ethernet interfaces on provider edge router PE2. If the unit numbers differ, MAC address synchronization does not happen. As a result, the status of the MAC address on the remote provider edge router remains in a pending state.

In an IPv6 network, you cannot configure an MC-LAG in an active-active bridge domain if you specified the **vlan-id none** statement at the **[edit bridge-domain *bd-name*]** hierarchy level. The **vlan-id none** statement that enables the removal of the incoming VLAN tags identifying a Layer 2 logical interface when packets are sent over VPLS pseudowires is not supported for IPv6 packets in an MC-LAG.

The topologies shown in Figure 2 on page 66 and Figure 3 on page 66 are supported. These figures use the following abbreviations:

- Aggregated Ethernet (AE)
- Interchassis link (ICL)
- Multichassis link (MCL)

Figure 14: Single Multichassis Link

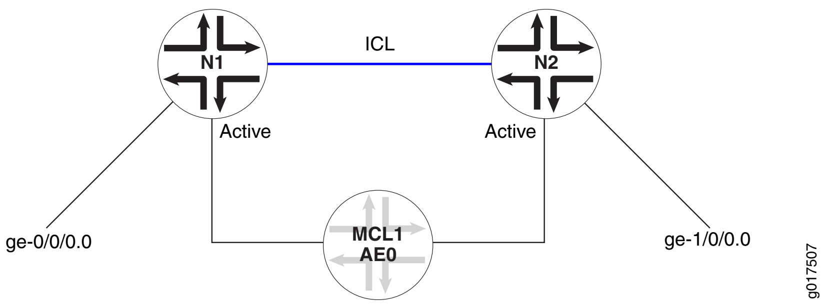
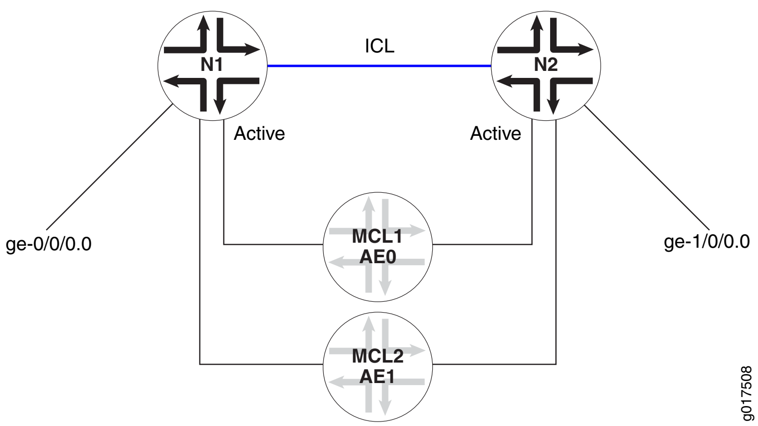


Figure 15: Dual Multichassis Link



The following functionality is *not* supported:

- Virtual private LAN service (VPLS) within the core
- Bridged core
- Topology as described in Rule 4 of "Data Traffic Forwarding Rules" on page 69
- Routed multichassis aggregated Ethernet interface, where the VRRP backup router is used in the edge of the network
- Track object, where in the case of an MC-LAG, the status of the uplinks from the provider edge can be monitored, and the MC-LAG can act on the status
- Mixed mode (active-active MC-LAG is supported on MX Series routers with MPC or MIC interfaces only). All interfaces in the bridge domain that are multichassis aggregated Ethernet active-active must be on MPC or MICs.

The topologies shown in Figure 4 on page 67, Figure 5 on page 67, and Figure 6 on page 67 are *not* supported:

Figure 16: Interchassis Data Link Between Active-Active Nodes

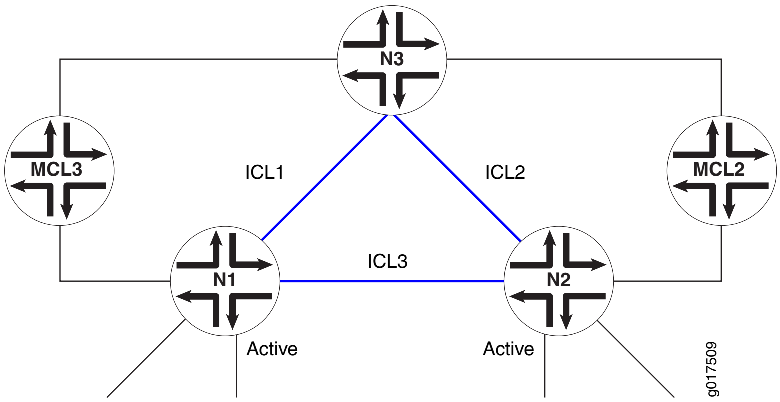


Figure 17: Active-Active MC-LAG with Single MC-LAG

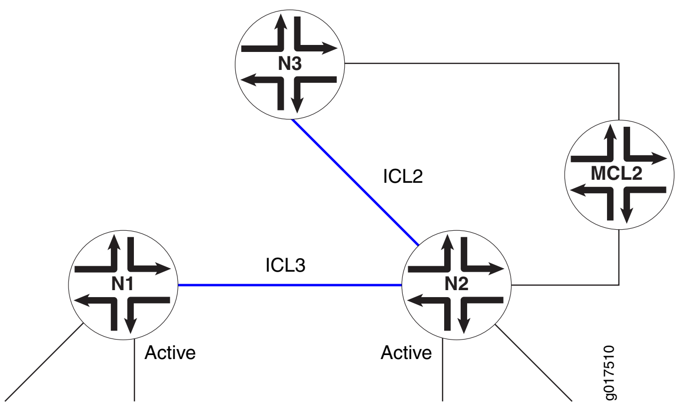
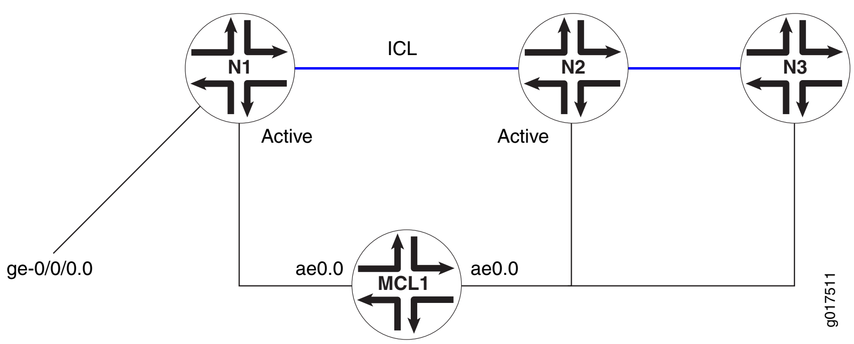


Figure 18: Active-Active MC-LAG with Multiple Nodes on a Single Multichassis Link



NOTE: A redundancy group cannot span more than two routers.

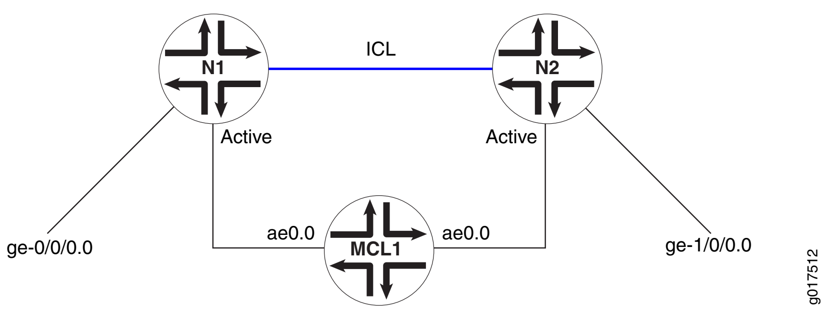
When configured to be active-active, the client device load-balances the traffic to the peering MC-LAG network devices. In a bridging environment, this could potentially cause the following problems:

- Traffic received on the MC-LAG from one MC-LAG network device could be looped back to the same MC-LAG on the other MC-LAG network device.
- Duplicated packets could be received by the MC-LAG client device.
- Traffic could be unnecessarily forwarded on the interchassis link.

To better illustrate the problems listed, consider Figure 7 on page 68, where an MC-LAG device MCL1 and single-homed clients ge-0/0/0.0 and ge-1/0/0.0 are allowed to talk to each other through an ICL.

- Traffic received on network routing instance N1 from MCL1 could be flooded to ICL to reach network routing instance N2. Once it reaches network routing instance N2, it could flood again to MCL1.
- Traffic received on interface ge-0/0/0.0 could be flooded to MCL1 and ICL on network routing instance N1. Once network routing instance N2 receives such traffic from ICL, it could again be flooded to MCL1.
- If interface ge-1/0/0.0 does not exist on network routing instance N2, traffic received from interface ge-0/0/0.0 or MCL1 on network routing instance N1 could be flooded to network routing instance N2 through ICL unnecessarily since interface ge-0/0/0.0 and MCL1 could reach each other through network routing instance N1.

Figure 19: MC-LAG Device and Single-Homed Client



Advantages of Using Multichassis Link Aggregation Groups

An MC-LAG reduces operational expenses by providing active-active links with a LAG, eliminates the need for Spanning Tree Protocol (STP), and provides faster Layer 2 convergence upon link and device failures.

An MC-LAG adds node-level redundancy to the normal link-level redundancy that a LAG provides. An MC-LAG improves network resiliency, which reduces network down time as well as expenses.

In data centers, it is desirable for servers to have redundant connections to the network. You probably want active-active connections along with links from any server to at least two separate routers.

An MC-LAG allows you to bond two or more physical links into a logical link between two routers or between a server and a router, which improves network efficiency. An MC-LAG enables you to load-balance traffic on multiple physical links. If a link fails, the traffic can be forwarded through the other available link, and the logical aggregated link remains in the UP state.

Data Traffic Forwarding Rules

In active-active bridging and VRRP over IRB topographies, network interfaces are categorized into three different interface types, as follows:

S-Links—Single-homed link (S-Link) terminating on MC-LAG-N device or MC-LAG in active-standby mode. In Figure 7 on page 68, interfaces ge-0/0/0.0 and ge-1/0/0.0 are S-Links.

MC-Links—MC-LAG links. In Figure 7 on page 68, interface ae0.0 is the MC-Link.

ICL—Interchassis link.

Based on incoming and outgoing interface types, some constraints are added to the Layer 2 forwarding rules for MC-LAG configurations, as described in the data traffic forwarding rules. Note that if only one of the MC-LAG member link is in the UP state, it is considered an S-Link.

The following data traffic forwarding rules apply:

1. When an MC-LAG network receives a packet from a local MC-Link or S-Link, the packet is forwarded to other local interfaces, including S-Links and MC-Links based on the normal Layer 2 forwarding rules and on the configuration of the **mesh-group** and **no-local-switching** statements. If MC-Links and S-Links are in the same mesh group and their **no-local-switching** statements are enabled, the received packets are only forwarded upstream and not sent to MC-Links and S-Links.

   NOTE: The functionality described in Rule 2 is *not* supported.

2. The following circumstances determine whether or not an ICL receives a packet from a local MC-Link or S-Link:

   a. If the peer MC-LAG network device has S-Links or MC-LAGs that do not reside on the local MC-LAG network device.

   b. Whether or not interfaces on two peering MC-LAG network devices are allowed to talk to each other only if both a. and b. are true. Traffic is always forwarded to the ICL.

3. When an MC-LAG network receives a packet from the ICL, the packet is forwarded to all local S-Links and active MC-LAGs that do not exist in the MC-LAG network that the packet comes from.

4. NOTE: The topology shown in Figure 8 on page 70 is *not* supported.

In certain cases, for example the topology shown in Figure 8 on page 70, there could be a loop caused by the ICL. To break the loop, one of the following mechanisms could be used:

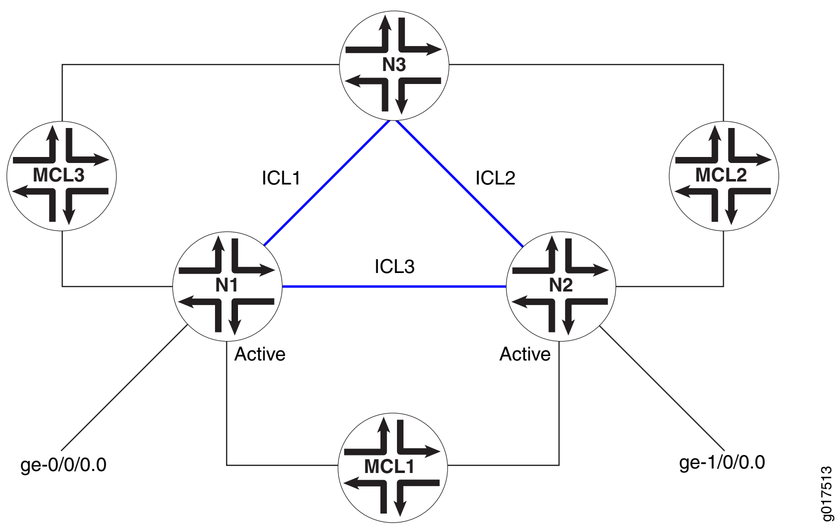
a. Run certain protocols, such as STP. In this case, whether packets received on one ICL are forwarded to other ICLs is determined by using Rule 3.

b. Configure the ICL to be fully meshed among the MC-LAG network devices. In this case, traffic received on the ICL would not be forwarded to any other ICLs.

In either case, duplicate packets could be forwarded to the MC-LAG clients. Consider the topology shown in Figure 8 on page 70, where if network routing instance N1 receives a packet from ge-0/0/0.0, it could be flooded to ICL1 and ICL3.

When receiving from ICL1 and ICL3, network routing instances N3 and N2 could flood the same packet to MCL2, as shown in Figure 8 on page 70. To prevent this from happening, the ICL designated forwarder should be elected between MC-LAG peers, and traffic received on an ICL could be forwarded to the active-active MC-LAG client by the designated forwarder only.

Figure 20: Loop Caused by the ICL Links



5. When received from an ICL, traffic should not be forwarded to the core-facing client link connection between two provider edge (PE) devices (MC-Link) if the peer chassis's (where the traffic is coming from) MC-Link is UP.

MAC Address Management

If an MC-LAG is configured to be active-active, upstream and downstream traffic could go through different MC-LAG network devices. Since the media access control (MAC) address is learned only on one of the MC-LAG network devices, the reverse direction's traffic could be going through the other MC-LAG network and be flooded unnecessarily. Also, a single-homed client's MAC address is only learned on the MC-LAG network device it is attached to. If a client attached to the peer MC-LAG network needs to communicate with that single-homed client, then traffic would be flooded on the peer MC-LAG network device. To avoid unnecessary flooding, whenever a MAC address is learned on one of the MC-LAG network devices, it gets replicated to the peer MC-LAG network device. The following conditions should be applied when MAC address replication is performed:

- MAC addresses learned on an MC-LAG of one MC-LAG network device should be replicated as learned on the same MC-LAG of the peer MC-LAG network device.
- MAC addresses learned on single-homed customer edge (CE) clients of one MC-LAG network device should be replicated as learned on the ICL-PL interface of the peer MC-LAG network device.
- MAC addresses learned on MC-LAG VE clients of one MC-LAG network device should be replicated as learned on the corresponding VE interface of the peer MC-LAG network device.
- MAC address learning on an ICL is disabled from the data path. It depends on software to install MAC addresses replicated through Inter-Chassis Control Protocol (ICCP).

MAC Aging

MAC aging support in Junos OS extends aggregated Ethernet logic for a specified MC-LAG. A MAC address in software is deleted until all Packet Forwarding Engines have deleted the MAC address. In the case of an MC-LAG, a remote provider edge is treated as a remote Packet Forwarding Engine and has a bit in the MAC data structure.

Layer 3 Routing

In general, when an MC-LAG is configured to provide Layer 3 routing functions to downstream clients, the MC-LAG network peers should be configured to provide the same gateway address to the downstream clients. To the upstream routers, the MC-LAG network peers could be viewed as either equal-cost multipath (ECMP) or two routes with different preference values.

Junos OS supports active-active MC-LAGs by using VRRP over IRB. Junos OS also supports active-active MC-LAGs by using IRB MAC address synchronization. You must configure IRB using the same IP address across MC-LAG peers. IRB MAC synchronization is supported on 32-bit interfaces and interoperates with earlier MPC and MIC releases.

To ensure that Layer 3 operates properly, instead of dropping the Layer 3 packet, the VRRP backup attempts to perform routing functions if the packet is received on an MC-LAG. A VRRP backup sends and responds to Address Resolution Protocol (ARP) requests.

For ARP, the same issue exists as with Layer 2 MAC addresses. Once ARP is learned, it must be replicated to the MC-LAG through ICCP. The peer must install an ARP route based on the ARP information received through ICCP.

For ARP aging, ARP requests on the MC-LAG peers can be aged out independently.

Address Resolution Protocol Active-Active MC-LAG Support Methodology

Suppose one of the PE routers issues an ARP request and another PE router gets the response and, because of the aggregated Ethernet distribution logic, the ARP resolution is not successful. Junos OS uses ARP response packet snooping to perform active-active multichassis link aggregation group support, providing easy synchronization without the need to maintain any specific state.

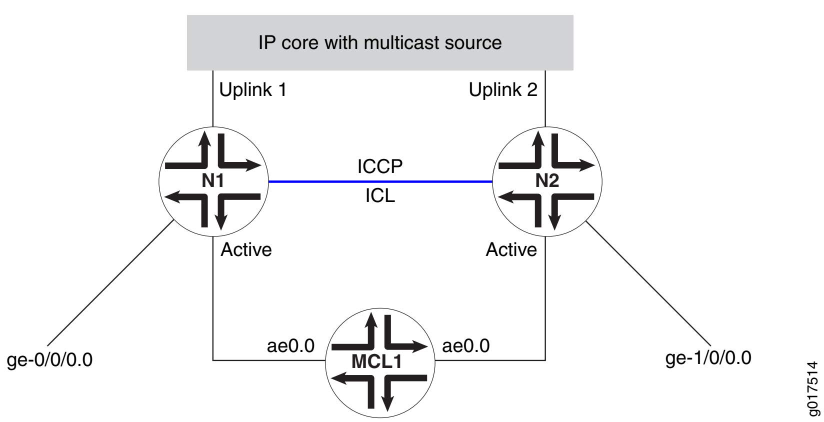
IGMP Snooping on Active-Active MC-LAG

For multicast to work in an active-active MC-LAG scenario, the typical topology is as shown in Figure 9 on page 72 and Figure 10 on page 73 with interested receivers over S-links and MC-Links. Starting in Junos OS Release 11.2, support is extended for sources connected over the Layer 2 interface.

If an MC-LAG is configured to be active-active, reports from MC-LAG clients could reach any of the MC-LAG network device peers. Therefore, the IGMP snooping module needs to replicate the states such that the Layer 2 multicast route state on both peers are the same. Additionally for S-Link clients, snooping needs to replicate these joins to its snooping peer, which in the case of Layer 3 connected source, passes this information to the PIM on IRB to enable the designated router to pull traffic for these groups,

The ICL should be configured as a router facing interface. For the scenario where traffic arrives through a Layer 3 interface, it is a requirement to have PIM and IGMP enabled on the IRB interface configured on the MC-LAG network device peers.

Figure 21: Multicast Topology with Source Connected Through Layer 3



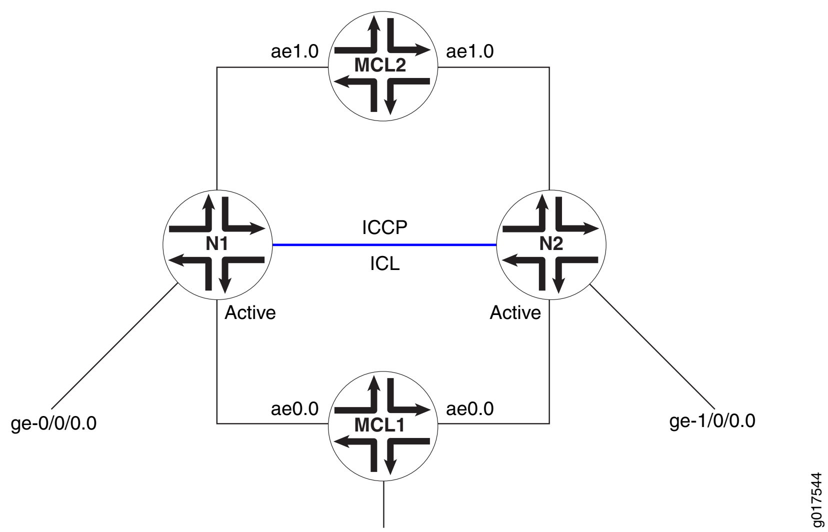
With reference to Figure 9 on page 72, either Device N1 or N2 becomes a designated router (for this example, N1 is the designated router). Router N1 therefore pulls the multicast traffic from the core. Once multicast data hits the network Device N1, the data is forwarded based on the snooping learned route.

For MC-Link clients, data is forwarded through N1. In the case of failover of the MC-Links, the data reaches the client through N2. For S-Link clients on N1, data would be forwarded through normal snooping routes.

For S-Link clients on N2, data is forwarded through the ICL interface. Layer 2 multicast routes on N1 do not show these groups unless there is interest for the same group over MC-Links or over S-Links on N1. For the IRB scenario, the IGMP membership and Layer 3 multicast route on N1 does however show these groups learned over the IRB interface.

Therefore, for a case where a specific group interest is only on the S-Link on N2, data arriving on N1 reaches N2 through the default route, and the Layer 2 multicast route on N2 has the S-Link in the outgoing interface list.

Figure 22: Multicast Topology with Source Connected Through MC-Link



In Figure 10 on page 73, MCL1 and MCL2 are on different devices, and the multicast source or IGMP querier is connected through MCL2. The data forwarding behavior seen is similar to that explained for multicast topology with source connected through Layer 3.

NOTE: **IGMP snooping should not be configured in proxy mode. There should be no IGMP hosts or IGMP or PIM routers sitting on the ICL interface.**

Up and Down Event Handling

The following conditions apply to up and down event handling:

- If the Inter-Chassis Control Protocol (ICCP) connection is UP but the ICL interface goes DOWN, the router configured as the backup brings down all the multichassis aggregated Ethernet interfaces shared with the peer that is connected to ICL. This ensures that there are no loops in the network. Otherwise, both PEs become PIM-designated routers and, hence, forward multiple copies of the same packet to the customer edge.
- If the ICCP connection is UP and the ICL comes UP, the router configured as the backup brings up the multichassis aggregated Ethernet interfaces shared with the peer.

- If both the ICCP connection and the ICL are DOWN, the router configured as the backup brings up the multichassis aggregated Ethernet interfaces shared with the peer.
- The Layer 2 address learn daemon (l2ald) does not store the information about a MAC address learned from a peer in the kernel. If l2ald restarts, and if the MAC address was not learned from the local multichassis aggregated Ethernet interface, l2ald clears the MAC addresses, which causes the router to flood the packets destined to this MAC address. This behavior is similar to that in a Routing Engine switchover. (Note that currently l2ald runs on a Routing Engine only when it is a master). Also, during the time l2ald is DOWN, ARP packets received from an ICCP peer are dropped. ARP retry takes care of this situation. This is the case with Routing Engine switchover, too.
- If ICCP restarts, l2ald does not identify that a MAC address was learned from a peer and, if the MAC address was learned only from the peer, that MAC address is deleted, and the packets destined to this MAC address are flooded.

VRRP Active-Standby Support

VRRP in active-standby mode enables Layer 3 routing over the multichassis aggregated Ethernet interfaces on the MC-LAG peers. In this mode, the MC-LAG peers act as virtual routers. The virtual routers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG. This virtual IP address, known as a routed VLAN interface (RVI), maps to either of the VRRP MAC addresses or the logical interfaces of the MC-LAG peers. The host or server uses the VRRP MAC address to send any Layer 3 upstream packets. At any time, one of the VRRP routers is the master (active), and the other is a backup (standby). Both VRRP active and VRRP backup routers forward Layer 3 traffic arriving on the multichassis aggregated Ethernet interface. If the master router fails, all the traffic shifts to the multichassis aggregated Ethernet link on the backup router.

NOTE: **You must configure VRRP on both MC-LAG peers for both the active and standby members to accept and route packets. Additionally, configure the VRRP backup router to send and receive ARP requests.**

Routing protocols run on the primary IP address of the RVI, and both of the MC-LAG peers run routing protocols independently. The routing protocols use the primary IP address of the RVI and the RVI MAC address to communicate with the MC-LAG peers. The RVI MAC address of each MC-LAG peer is replicated on the other MC-LAG peer and is installed as a MAC address that has been learned on the ICL-PL.

In many cases, MC-LAG devices are Layer 3 routing devices and perform the default gateway functionality for hosts that are part of the attached IP subnets. The MC-LAG device-pair can therefore share the default gateway routing functionality with the VRRP protocol. The VRRP active-standby operation can be optimized to be an active-active mode of processing because traffic flowing from an MC-LAG client to an MC-LAG device is always sent on one of the available links of an MC-LAG and reaches exactly one of the MC-LAG destination devices. Because of this behavior, both MC-LAG devices in the pair can be enabled as routers for IP traffic destined to the VRRP destination MAC address.

Both MC-LAG devices must be full members of the routing domain and have routing entries that allow them to reach the IP destination networks.

The active-active functionality works without changing any VRRP state machine and by activating the routing function in the forwarding plane of the VRRP backup system (similar to the VRRP master). The mechanism enables traffic forwarding in Layer 3 to be fully redundant, leveraging all available link bandwidth. All routers forward traffic and thereby load-share routed traffic.

Inter-Chassis Control Protocol

Inter-Chassis Control Protocol (ICCP) is used to synchronize configurations, states, and data.

ICCP supports the following types of state information:

- MC-LAG members and their operational states
- Single-homed members and their operational states

ICCP supports the following application database synchronization parameters:

- MAC addresses learned and to be aged
- ARP information learned over IRB

Inter-Chassis Control Protocol Message

ICCP messages and attribute-value pairs (AVPs) are used for synchronizing MAC address and ARP information.

Related Documentation

- Configuring Multichassis Link Aggregation on MX Series Routers on page 27
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers on page 87

- *multi-chassis-protection*
- *peer*
- *show interfaces mc-ae*
- *Ethernet Interfaces*

Example: Configuring IGMP Snooping in MC-LAG Active-Active Mode on MX Series Routers

Supported Platforms MX240, MX480, MX960

This example shows how to configure Internet Group Management Protocol (IGMP) snooping for uninterrupted traffic flow on MX Series routers with a multichassis link aggregation group (MC-LAG) in an active-active scenario.

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks MX Series routers
- Junos OS Release 11.2 or later running on all four routers

Before you begin, make sure that Protocol Independent Multicast (PIM) and IGMP are running on all interfaces that will receive multicast packets. IGMP is automatically enabled on all IPv4 interfaces on which you configure PIM.

Overview

When links are aggregated, the links can be treated as if they were a single link. Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. MC-LAG provides redundant Layer 2 access connectivity at the node level. This enables two or more systems to share a common LAG endpoint. The multiple end points present a single logical chassis to the start point, and the start node does not need to be aware that MC-LAG is being used.

In this example, the CE router is not aware that its aggregated Ethernet links are connected to two separate PE devices. The two PE devices each have a LAG connected to the CE device. The configured mode is active-active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time.

NOTE: **The other possible mode is active-standby, in which one of the router's ports only becomes active when failure is detected in the active links. In active-standby mode, the PE routers perform an election to determine the active and standby routers.**

In Figure 23 on page 117, from the perspective of the router CE, all four ports belonging to a LAG are connected to a single service provider device. Because the configured mode is active-active, all four ports are active, and the CE device load-balances the traffic to the peering PE devices. On the PE routers, a regular LAG is configured facing the CE device.

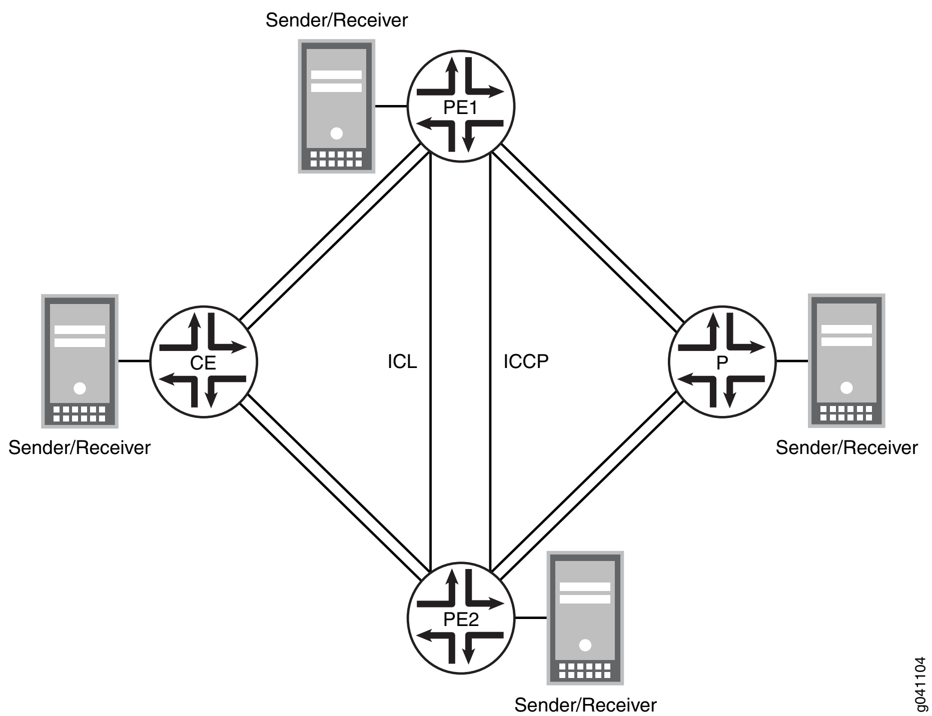
Inter-Chassis Control Protocol (ICCP) messages are sent between the two PE devices. These messages exchange MC-LAG configuration parameters and ensure that both chassis use the correct Link Aggregation Control Protocol (LACP) parameters when talking to the CE device.

The interchassis link-protection link (ICL) provides redundancy when a link failure occurs on one of the active links. The ICL-PL between the MC-LAG peering devices relays traffic that would otherwise be dropped due to a link failure.

Topology Diagram

Figure 23 on page 117 shows the topology used in this example.

Figure 23: IGMP Snooping in MC-LAG Active-Active Mode on MX Series Routers



Configuring the PE Routers

CLI Quick Configuration

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

Router PE1

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/1 gigether-options 802.3ad ae1
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.1/30
set interfaces ge-1/0/6 gigether-options 802.3ad ae0
set interfaces ge-1/1/1 flexible-vlan-tagging
set interfaces ge-1/1/1 encapsulation flexible-ethernet-services
set interfaces ge-1/1/1 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/1 unit 0 vlan-id-range 100-110
set interfaces ge-1/1/4 flexible-vlan-tagging
set interfaces ge-1/1/4 encapsulation flexible-ethernet-services
```

```
set interfaces ge-1/1/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/4 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/1/1.0
set bridge-domains bd0 interface ge-1/1/4.0
set bridge-domains bd0 interface ae0.0
set bridge-domains bd0 multicast-snooping-options multichassis-lag-replicate-state
set bridge-domains bd0 protocols igmp-snooping vlan 100 interface ge-1/1/4.0
  multicast-router-interface
set bridge-domains bd0 protocols igmp-snooping vlan 101 interface ge-1/1/4.0
  multicast-router-interface
set bridge-domains bd0 protocols igmp-snooping vlan 200 interface ge-1/1/4.0
  multicast-router-interface
set multicast-snooping-options multichassis-lag-replicate-state
set protocols iccp local-ip-addr 100.100.100.1
set protocols iccp peer 100.100.100.2 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.2 liveness-detection minimum-interval 1000
set switch-options service-id 10
```

Router PE2

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.2/30
set interfaces ge-1/0/3 flexible-vlan-tagging
set interfaces ge-1/0/3 encapsulation flexible-ethernet-services
set interfaces ge-1/0/3 unit 0 encapsulation vlan-bridge
```

```
set interfaces ge-1/0/3 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/4 flexible-vlan-tagging
set interfaces ge-1/0/4 encapsulation flexible-ethernet-services
set interfaces ge-1/0/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/4 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/5 gigether-options 802.3ad ae0
set interfaces ge-1/1/0 gigether-options 802.3ad ae1
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/0/4.0
set bridge-domains bd0 interface ae0.0
set bridge-domains bd0 multicast-snooping-options multichassis-lag-replicate-state
set bridge-domains bd0 protocols igmp-snooping vlan 100 interface ge-1/0/4.0
  multicast-router-interface
set bridge-domains bd0 protocols igmp-snooping vlan 101 interface ge-1/0/4.0
  multicast-router-interface
set bridge-domains bd0 protocols igmp-snooping vlan 200 interface ge-1/0/4.0
  multicast-router-interface
set multicast-snooping-options multichassis-lag-replicate-state
set protocols iccp local-ip-addr 100.100.100.2
set protocols iccp peer 100.100.100.1 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.1 liveness-detection minimum-interval 1000
set switch-options service-id 10
```

Configuring the PE1 Router

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router PE1:

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

   ```
   [edit chassis]
   user@PE1# set aggregated-devices ethernet device-count 5
   ```

2. Specify the members to be included within the aggregated Ethernet bundles.

   ```
   [edit interfaces]
   user@PE1# set ge-1/0/1 gigether-options 802.3ad ae1
   user@PE1# set ge-1/0/6 gigether-options 802.3ad ae0
   ```

3. Configure the interfaces that connect to multicast senders or receivers, the ICL interfaces, and the ICCP interfaces.

   ```
   [edit interfaces]
   user@PE1# set ge-1/1/1 flexible-vlan-tagging
   user@PE1# set ge-1/1/1 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/1 unit 0 encapsulation vlan-bridge
   user@PE1# set ge-1/1/1 unit 0 vlan-id-range 100-110
   user@PE1# set ge-1/1/4 flexible-vlan-tagging
   user@PE1# set ge-1/1/4 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/4 unit 0 encapsulation vlan-bridge
   user@PE1# set ge-1/1/4 unit 0 vlan-id-range 100-110
   user@PE1# set ge-1/0/2 unit 0 family inet address 100.100.100.1/30
   ```

4. Configure parameters on the aggregated Ethernet bundles.

   ```
   [edit interfaces ae0]
   user@PE1# set flexible-vlan-tagging
   user@PE1# set encapsulation flexible-ethernet-services
   user@PE1# set unit 0 encapsulation vlan-bridge
   user@PE1# set unit 0 vlan-id-range 100-110
   user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0

   [edit interfaces ae1]
   user@PE1# set flexible-vlan-tagging
   user@PE1# set encapsulation flexible-ethernet-services
   user@PE1# set unit 0 encapsulation vlan-bridge
   user@PE1# set unit 0 vlan-id-range 100-110
   user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
   ```

5. Configure LACP on the aggregated Ethernet bundles.

   ```
   [edit interfaces ae0 aggregated-ether-options]
   user@PE1# set lacp active
   user@PE1# set lacp system-priority 100
   user@PE1# set lacp system-id 00:00:00:00:00:05
   user@PE1# set lacp admin-key 1
   ```

```
[edit interfaces ae1 aggregated-ether-options]
user@PE1# set lacp active
user@PE1# set lacp system-priority 100
user@PE1# set lacp system-id 00:00:00:00:00:05
user@PE1# set lacp admin-key 1
```

6. Configure the MC-LAG interfaces.

```
[edit interfaces ae0 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 5
user@PE1# set mc-ae redundancy-group 10
user@PE1# set mc-ae chassis-id 1
user@PE1# set mc-ae mode active-active
user@PE1# set mc-ae status-control active

[edit interfaces ae1 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 10
user@PE1# set mc-ae redundancy-group 10
user@PE1# set mc-ae chassis-id 1
user@PE1# set mc-ae mode active-active
user@PE1# set mc-ae status-control active
```

   The multichassis aggregated Ethernet identification number (**mc-ae-id**) specifies which link aggregation group the aggregated Ethernet interface belongs to. The ae0 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 5**. The **ae1** interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 10**. (To refer to the configuration on Router PE2, see “Router PE2” on page 90).

   The **redundancy-group 10** statement is 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 ae0 and ae1 interfaces on Router PE1 and Router PE2 are configured with the same redundancy group **redundancy-group 10**.

   The **chassis-id** statement is used by LACP for calculating the port number of the MC-LAG's physical member links. Router PE1 uses **chassid-id 1** to identify both its ae0 and ae1 interfaces. Router PE2 (as shown in “Router PE2” on page 90) uses **chassis-id 0** to identify both its ae0 and ae1 interfaces.

   The **mode** statement 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.

7. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@PE1# set domain-type bridge
user@PE1# set vlan-id all
user@PE1# set service-id 20
user@PE1# set interface ae0.0
user@PE1# set interface ae1.0
user@PE1# set interface ge-1/0/3.0
user@PE1# set interface ge-1/1/1.0
user@PE1# set interface ge-1/1/4.0
```

   The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

The bridge-level **service-id** statement is required to link related bridge domains across peers (in this case Router PE1 and Router PE2), and should be configured with the same value.

8. At the global level and also in the bridge domain, replicate IGMP join and leave messages from the active link to the standby link of a dual-link MC-LAG interface, to enable faster recovery of membership information after failover.

```
[edit multicast-snooping-options]
user@PE1# set multichassis-lag-replicate-state
```

```
[edit bridge-domains bd0 multicast-snooping-options]
user@PE1# set multichassis-lag-replicate-state
```

9. Configure multicast snooping for the MC-LAG interfaces.

```
[edit bridge-domains bd0]
user@PE1# set protocols igmp-snooping vlan 100 interface ge-1/1/4.0
  multicast-router-interface
user@PE1# set protocols igmp-snooping vlan 101 interface ge-1/1/4.0
  multicast-router-interface
user@PE1# set protocols igmp-snooping vlan 200 interface ge-1/1/4.0
  multicast-router-interface
```

10. Configure ICCP parameters.

```
[edit protocols iccp]
user@PE1# set local-ip-addr 100.100.100.1
user@PE1# set peer 100.100.100.2 redundancy-group-id-list 10
user@PE1# set peer 100.100.100.2 liveness-detection minimum-interval 1000
```

11. Configure the service ID at the global level.

```
[edit switch-options]
user@PE1# set service-id 10
```

You must configure the same unique network-wide configuration for a service in the set of PE routers providing the service. This service ID is required if the multichassis aggregated Ethernet interfaces are part of a bridge domain.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, **show interfaces**, **show multicast-snooping-options**, **show protocols**, and **show switch-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1#  show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  service-id 20;
  interface ae1.0;
  interface ge-1/0/3.0;
  interface ge-1/1/1.0;
  interface ge-1/1/4.0;
```



```
  interface ae0.0;
  multicast-snooping-options {
    multichassis-lag-replicate-state;
  }
  protocols {
    igmp-snooping {
      vlan 100 {
        interface ge-1/1/4.0 {
          multicast-router-interface;
        }
      }
      vlan 101 {
        interface ge-1/1/4.0 {
          multicast-router-interface;
        }
      }
      vlan 200 {
        interface ge-1/1/4.0 {
          multicast-router-interface;
        }
      }
    }
  }
}
```

```
user@PE1# show chassis
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
```

```
user@PE1# show interfaces
ge-1/0/1 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-1/0/2 {
  unit 0 {
    family inet {
      address 100.100.100.1/30;
    }
  }
}
ge-1/1/1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-110;
  }
```

```
}
ge-1/1/4 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
   }
}
ae0 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   aggregated-ether-options {
      lacp {
         active;
         system-priority 100;
         system-id 00:00:00:00:00:05;
         admin-key 1;
      }
      mc-ae {
         mc-ae-id 5;
         redundancy-group 10;
         chassis-id 1;
         mode active-active;
         status-control active;
      }
   }
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
      multi-chassis-protection 100.100.100.2 {
         interface ge-1/1/4.0;
      }
   }
}
ae1 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   aggregated-ether-options {
      lacp {
         active;
         system-priority 100;
         system-id 00:00:00:00:00:05;
         admin-key 1;
      }
      mc-ae {
         mc-ae-id 10;
         redundancy-group 10;
         chassis-id 1;
         mode active-active;
         status-control active;
      }
   }
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
```



```
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
```

```
user@PE1# show multicast-snooping-options
multichassis-lag-replicate-state;
```

```
user@PE1# show protocols
iccp {
    local-ip-addr 100.100.100.1;
    peer 100.100.100.2 {
        redundancy-group-id-list 10;
        liveness-detection {
            minimum-interval 1000;
        }
    }
}
```

```
user@PE1# run show switch-options
service-id 10;
```

If you are done configuring the device, enter **commit** from configuration mode.

Repeat the procedure for Router PE2, using the appropriate interface names and addresses.

Configuring the CE Device

CLI Quick Configuration

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

Router CE

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-2/0/2 gigether-options 802.3ad ae0
set interfaces ge-2/0/3 gigether-options 802.3ad ae0
set interfaces ge-2/1/6 flexible-vlan-tagging
set interfaces ge-2/1/6 encapsulation flexible-ethernet-services
set interfaces ge-2/1/6 unit 0 encapsulation vlan-bridge
set interfaces ge-2/1/6 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-500
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 interface ge-2/1/6.0
set bridge-domains bd0 interface ae0.0
```

Configuring the CE Device

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the CE device:

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

   [edit chassis]
   user@CE# **set aggregated-devices ethernet device-count 2**

2. Specify the members to be included within the aggregated Ethernet bundle.

   [edit interfaces]
   user@CE# **set ge-2/0/2 gigether-options 802.3ad ae0**
   user@CE# **set ge-2/0/3 gigether-options 802.3ad ae0**

3. Configure an interface that connects to multicast senders or receivers.

   [edit interfaces ge-2/1/6]
   user@CE# **set flexible-vlan-tagging**
   user@CE# **set encapsulation flexible-ethernet-services**
   user@CE# **set unit 0 encapsulation vlan-bridge**
   user@CE# **set unit 0 vlan-id-range 100-110**

4. Configure parameters on the aggregated Ethernet bundle.

   [edit interfaces ae0]
   user@CE# **set flexible-vlan-tagging**
   user@CE# **set encapsulation flexible-ethernet-services**
   user@CE# **set unit 0 encapsulation vlan-bridge**
   user@CE# **set unit 0 vlan-id-range 100-500**

5. Configure LACP on the aggregated Ethernet bundle.

   [edit interfaces ae0 aggregated-ether-options]
   user@CE# **set lacp active**
   user@CE# **set lacp system-priority 100**

   The **active** statement initiates transmission of LACP packets.

   For the **system-priority** statement, a smaller value indicates a higher priority. The device with the lower system priority value determines which links between LACP partner devices are active and which are in standby mode for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

6. Configure a domain that includes the set of logical ports.

   [edit bridge-domains bd0]
   user@CE# **set domain-type bridge**
   user@CE# **set vlan-id all**
   user@CE# **set interface ge-2/1/6.0**
   user@CE# **set interface ae0.0**

The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@CE#  show bridge-domains
bd0 {
   domain-type bridge;
   vlan-id all;
   interface ge-2/1/6.0;
   interface ae0.0;
}
```

```
user@CE#  show chassis
aggregated-devices {
   ethernet {
      device-count 2;
   }
}
```

```
user@CE#  show interfaces
ge-2/0/2 {
   gigether-options {
      802.3ad ae0;
   }
}
ge-2/0/3 {
   gigether-options {
      802.3ad ae0;
   }
}
ge-2/1/6 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
   }
}
ae0 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   aggregated-ether-options {
      lacp {
         active;
         system-priority 100;
      }
   }
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-500;
```

```
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring the Provider Router

CLI Quick Configuration

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

Router P

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-1/0/5 gigether-options 802.3ad ae1
set interfaces ge-1/0/11 gigether-options 802.3ad ae1
set interfaces ge-1/1/3 flexible-vlan-tagging
set interfaces ge-1/1/3 encapsulation flexible-ethernet-services
set interfaces ge-1/1/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/3 unit 0 vlan-id-range 100-500
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 interface ge-1/1/3.0
set bridge-domains bd0 interface ae1.0
```

Configuring the Router P

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure router P:

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

   ```
   [edit chassis]
   user@P# set aggregated-devices ethernet device-count 2
   ```

2. Specify the members to be included within the aggregated Ethernet bundle.

   ```
   [edit interfaces]
   user@P# set ge-1/0/5 gigether-options 802.3ad ae1
   user@P# set ge-1/0/11 gigether-options 802.3ad ae1
   ```

3. Configure an interface that connects to multicast senders or receivers.

   ```
   [edit interfaces ge-1/1/3]
   user@P# set flexible-vlan-tagging
   user@P# set encapsulation flexible-ethernet-services
   user@P# set unit 0 encapsulation vlan-bridge
   user@P# set unit 0 vlan-id-range 100-500
   ```


4. Configure parameters on the aggregated Ethernet bundle.

```
[edit interfaces ae1]
user@P# set flexible-vlan-tagging
user@P# set encapsulation flexible-ethernet-services
user@P# set unit 0 encapsulation vlan-bridge
user@P# set unit 0 vlan-id-range 100-110
```

5. Configure LACP on the aggregated Ethernet bundle.

```
[edit interfaces ae1 aggregated-ether-options]
user@P# set lacp active
user@P# set lacp system-priority 100
```

6. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@P# set vlan-id all
user@P# set domain-type bridge
user@P# set interface ge-1/1/3.0
user@P# set interface ae1.0
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@P#  show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  interface ge-1/1/3.0;
  interface ae1.0;
}
```

```
user@P#  show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@P#  show interfaces
ge-1/0/5 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/11 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/1/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
```

```
      unit 0 {
         encapsulation vlan-bridge;
         vlan-id-range 100-500;
      }
   }
   ae1 {
      flexible-vlan-tagging;
      encapsulation flexible-ethernet-services;
      aggregated-ether-options {
         lacp {
            active;
            system-priority 100;
         }
      }
      unit 0 {
         encapsulation vlan-bridge;
         vlan-id-range 100-110;
      }
   }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly by running the following commands:

- **show iccp**
- ***show igmp snooping interface***
- ***show igmp snooping membership***
- **show interfaces ae0**
- **show interfaces ae1**
- **show interfaces mc-ae**
- ***show l2-learning instance* extensive**
- ***show multicast snooping route* extensive**

Related Documentation

- *IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview*
- Configuring IGMP Snooping in MC-LAG Active-Active on MX Series Routers on page 80
- *Configuring ICCP for MC-LAG*
- *show interfaces (Aggregated Ethernet)* in the CLI Explorer

Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on EX9200 Switches

Supported Platforms EX Series

There are two methods for enabling Layer 3 multicast functionality across a multichassis link aggregation group (MC-LAG). You can choose either to configure Virtual Router Redundancy Protocol (VRRP) over the integrated routing and bridging (IRB) interface or to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG. This provides redundancy and load balancing between the two MC-LAG peers. The procedure to configure VRRP for use in a Layer 3 multicast MC-LAG is included in this example.

Requirements

This example uses the following hardware and software components:

- Two EX9200 switches
- Junos OS Release 13.2R1 or later

Before you configure an MC-LAG for Layer 3 multicast using VRRP, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Configuring an Aggregated Ethernet Interface*.
- Configure Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Configuring Aggregated Ethernet LACP*.
- Configure Virtual Router Redundancy Protocol (VRRP) on a switch. See *Configuring Basic VRRP Support*.

For a list of best practice configuration guidelines and important functional behavior for MC-LAGs, see the "MC-LAG Configuration Guidelines and Functional Behavior" section in the topic *Understanding Multichassis Link Aggregation*.

Overview

In this example, you configure two MC-LAGs between two switches, consisting of two aggregated Ethernet interfaces (ae1 and ae2). To support the MC-LAG, you create a third aggregated Ethernet interface (ae0) for the interchassis link (ICL). You also configure a multichassis protection link for the ICL, Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the MC-LAG configuration, enable VRRP by completing the following tasks for each MC-LAG:

1. Create an IRB interface.
2. Create a VRRP group and assign a virtual IP address that is shared between each switch in the VRRP group.
3. Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group.
4. Configure Layer 3 connectivity between the VRRP groups.

Topology

The topology used in this example consists of two switches hosting two MC-LAGs—ae1 and ae2. The two switches are connected to a multicast source (Server 1) over MC-LAG ae1, and a multicast receiver (Server 2) over MC-LAG ae2. Figure 24 on page 132 shows the topology for this example.

Figure 24: Configuring Two MC-LAGs Between Switch A and Switch B

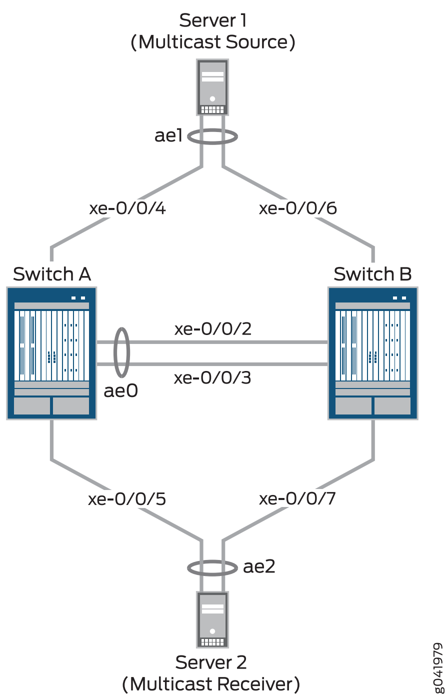


Table 10 on page 133 details the topology used in this configuration example.

Table 10: Components of the Topology for Configuring Two MC-LAGs Between Switch A and Switch B

Hostname	Base Hardware	Link Aggregation Groups
Switch A Switch B	EX9200 switch	• ae0 is configured as an aggregated Ethernet interface, and is used as an ICL. The following two interfaces are part of ae0: xe-0/0/2 and xe-0/0/3 on Switch A and xe-0/0/2 and xe-0/0/3 on Switch B. • ae1 is configured as an MC-LAG for the multicast source (Server 1), and the following two interfaces are part of ae1: xe-0/0/4 on Switch A and xe-0/0/6 on Switch B. • ae2 is configured as an MC-LAG for the multicast receiver (Server 2), and the following two interfaces are part of ae2: xe-0/0/5 on Switch A and xe-0/0/7 on Switch B.

Configuration

CLI Quick Configuration

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

Switch A

```
set chassis aggregated-devices ethernet device-count 3
set interfaces xe-0/0/2 ether-options 802.3ad ae0
set interfaces xe-0/0/3 ether-options 802.3ad ae0
set interfaces xe-0/0/4 ether-options 802.3ad ae1
set interfaces xe-0/0/5 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control active
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching interface-mode trunk
```



```
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority 200
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority 200
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 accept-data
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface irb.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 60
set protocols igmp-snooping vlan v100
set protocols igmp-snooping vlan v200
set protocols igmp-snooping vlan v500
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection transmit-interval
  threshold 500
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection transmit-interval
  threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface irb.100 priority 200
set protocols pim interface irb.200 priority 600
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch B

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/2 ether-options 802.3ad ae0
set interfaces xe-0/0/3 ether-options 802.3ad ae0
set interfaces xe-0/0/6 ether-options 802.3ad ae1
set interfaces xe-0/0/7 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
```



```
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control standby
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority 150
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 accept-data
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority 150
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 accept-data
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface irb.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 60
set protocols igmp-snooping vlan v100
set protocols igmp-snooping vlan v200
set protocols igmp-snooping vlan v500
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface irb.100 bfd-liveness-detection transmit-interval
  threshold 500
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface irb.200 bfd-liveness-detection transmit-interval
  threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface irb.100 priority 100
set protocols pim interface irb.200 priority 500
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Configuring MC-LAG for Layer 3 Multicast Using VRRP on Two Switches

Step-by-Step Procedure

The following procedure requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable a multichassis protection link between MC-LAG peers:

1. Configure the number of LAGs on both Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit chassis]
   user@switch# set aggregated-devices ethernet device-count 3
   ```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/2 ether-options 802.3ad ae0
   user@switch# set xe-0/0/3 ether-options 802.3ad ae0
   ```

   Switch A:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/4 ether-options 802.3ad ae1
   user@switch# set xe-0/0/5 ether-options 802.3ad ae2
   ```

   Switch B:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/6 ether-options 802.3ad ae1
   user@switch# set xe-0/0/7 ether-options 802.3ad ae2
   ```

3. Configure ae0 as the trunk interface between Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switching interface-mode trunk
   ```

4. Configure ae0 as the multichassis protection link between Switch A and Switch B.

   Switch A:

   ```
   [edit]
   user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
   ```

   Switch B:

   ```
   [edit]
   user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
   ```


Step-by-Step Procedure

To enable ICCP:

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address, minimum receive interval, and minimum transmit interval for a Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

   NOTE: Configuring the minimum receive interval is required to enable BFD. We recommend a minimum receive interval value of 60 seconds.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 60
   user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
     minimum-interval 60
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
     60
   user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
     minimum-interval 60
   ```

3. (Optional) Configure the time during which an ICCP connection must be established between MC-LAG peers on Switch A and Switch B.

   NOTE: Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
   ```

4. (Optional) Configure the backup-liveness-detection statement on the management interface (fxp0) only.

   We recommend that you configure the backup liveness detection feature to implement faster failover of data traffic during an MC-LAG peer reboot.

   NOTE: The backup-liveness-detection statement is supported starting in Junos OS Release 13.2R1.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip
     10.207.64.233
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
     10.207.64.234
   ```

5. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit vlans]
   user@switch# set v500 vlan-id 500
   user@switch# set v500 l3-interface irb.500
   ```

   ```
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switching vlan members v500
   ```

   Switch A:

   ```
   [edit interfaces]
   user@switch# set irb unit 500 family inet address 3.3.3.2/24
   ```

   Switch B:

   ```
   [edit interfaces]
   user@switch# set irb unit 500 family inet address 3.3.3.1/24
   ```

Step-by-Step Procedure

To enable the ae1 and ae2 MC-LAG interfaces:

1. Enable LACP on the MC-LAG interfaces on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp active
   ```

user@switch# **set ae2 aggregated-ether-options lacp active**

2. Specify the same multichassis aggregated Ethernet identification number for each MC-LAG peer on Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **mc-ae-id 3**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **mc-ae-id 4**

3. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **chassis-id 0**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **chassis-id 0**

   Switch B:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **chassis-id 1**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **chassis-id 1**

4. Specify the operating mode of the MC-LAGs on both Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **mode active-active**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **mode active-active**

5. Specify the status control for the MC-LAGs on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B that host the MC-LAGs. If one peer is in active mode, the other must be in standby mode.

   Switch A:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **status-control active**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **status-control active**

   Switch B:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options** mc-ae **status-control standby**
   user@switch# **set ae2 aggregated-ether-options** mc-ae **status-control standby**

NOTE: You can configure the **prefer-status-control-active** statement with the mc-ae **status-control standby** configuration to prevent the LACP MC-LAG system ID from reverting to the default LACP system ID on ICCP failure. Use this configuration only if you can ensure that ICCP will not go down unless the switch is down. You must also configure the **hold-time down** value (at the **[edit interfaces *interface-name*]** hierarchy level) for the ICL with the mc-ae **status-control standby** configuration to be higher than the ICCP BFD timeout. This configuration prevents data traffic loss by ensuring that when the switch with the mc-ae **status-control active** configuration goes down, the switch with the mc-ae **status-control standby** configuration does not go into standby mode.

To make the **prefer-status-control-active** configuration work with the mc-ae **status-control standby** configuration when an ICL logical interface is configured on an aggregated Ethernet interface, you must either configure the ***lacp*** **periodic interval** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level as slow or configure the **detection-time threshold** statement at the **[edit protocols iccp peer *liveness-detection*]** hierarchy level as less than 3 seconds.

The **prefer-status-control-active** statement is supported starting in Junos OS Release 13.2R1.

6. To minimize traffic loss, specify the number of seconds by which to delay bringing the multichassis aggregated Ethernet interface back to the up state when you reboot Switch A or Switch B.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae init-delay-time 240
user@switch# set ae2 aggregated-ether-options mc-ae init-delay-time 240
```

7. Specify the same LACP system ID for each MC-LAG on Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05
user@switch# set ae2 aggregated-ether-options lacp system-ID 00:01:02:03:04:06
```

8. Specify the same LACP administration key on both Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp admin-key 3
user@switch# set ae2 aggregated-ether-options lacp admin-key 3
```

9. Enable a VLAN for each MC-LAG on Switch A and Switch B.

```
[edit vlans]
user@switch# set v100 vlan-id 100
user@switch# set v200 vlan-id 200
```

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
```

```
user@switch# set ae2 unit 0 family ethernet-switching vlan members v200
```

10. Configure ae1 and ae2 as trunk interfaces between Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ae2 unit 0 family ethernet-switching interface-mode trunk
```

Step-by-Step Procedure

To enable VRRP on the MC-LAGs:

1. Create an integrated routing and bridging (IRB) interface for each MC-LAG, assign a virtual IP address that is shared between each switch in the VRRP groups, and assign an individual IP address for each switch in the VRRP groups.

Switch A:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  virtual-address 10.1.1.2
```

Switch B:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  virtual-address 10.1.1.2
```

2. Assign the priority for each switch in the VRRP groups.

NOTE: The switch configured with the highest priority is the master.

Switch A:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority
  200
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority
  200
```

Switch B:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority
  150
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority
  150
```

3. Enable the switch to accept all packets destined for the virtual IP address if it is the master in a VRRP group.

Switch A:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  accept-data
```

Switch B:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  accept-data
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  accept-data
```

4. Configure Layer 3 connectivity between Switch A and Switch B.

```
[edit]
user@switch# set v100 l3-interface irb.100
user@switch# set v200 l3-interface irb.200
```

Step-by-Step Procedure

To enable IGMP snooping:

- Enable IGMP snooping for all VLANs on Switch A and Switch B.

```
[edit protocols]
user@switch# set igmp-snooping vlan v100
user@switch# set igmp-snooping vlan v200
user@switch# set igmp-snooping vlan v500
```

NOTE: You must configure the **multichassis-lag-replicate-state** statement for IGMP snooping to work properly in an MC-LAG environment.

Step-by-Step Procedure

To configure OSPF as the Layer 3 protocol:

1. Configure an OSPF area on Switch A and Switch B.

```
[edit protocols ospf]
user@switch# set area 0.0.0.0
```

2. Assign the VLAN interfaces for the MC-LAGs as interfaces to the OSPF area on Switch A and Switch B.

```
[edit protocols ospf area 0.0.0.0]
user@switch# set interface irb.100
user@switch# set interface irb.200
```

3. Configure the minimum receive interval, minimum transmit interval, and transmit interval threshold for a Bidirectional Forwarding Detection (BFD) session for the OSPF interfaces on Switch A and Switch B.

```
[edit protocols ospf area 0.0.0.0]
user@switch# set interface irb.100 bfd-liveness-detection minimum-receive-interval
  700
```



```
user@switch# set interface irb.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface irb.100 bfd-liveness-detection transmit-interval threshold
  500
user@switch# set interface irb.200 bfd-liveness-detection minimum-receive-interval
  700
user@switch# set interface irb.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface irb.200 bfd-liveness-detection transmit-interval
  threshold 500
```

Step-by-Step Procedure

To configure Protocol Independent Multicast (PIM) as the multicast protocol:

1. Configure a static rendezvous point (RP) address on Switch A and Switch B.

   ```
   [edit protocols pim]
   user@switch# set rp static address 1.0.0.3
   ```

2. Configure the address ranges of the multicast groups for which Switch A and Switch B can be an RP.

   ```
   [edit protocols pim rp static address 1.0.0.3]
   user@switch# set group-ranges 239.0.0.0/8
   ```

3. Configure the priority of each PIM interface for being selected as the designated router.

   An interface with a higher priority value has a higher probability of being selected as the designated router.

   NOTE: Configure the IP address on the active MC-LAG peer with a high IP address or a high designated router priority.

   Switch A:

   ```
   [edit protocols pim]
   user@switch# set interface irb.100 priority 200
   user@switch# set interface irb.200 priority 600
   ```

   Switch B:

   ```
   [edit protocols pim]
   user@switch# set interface irb.100 priority 100
   user@switch# set interface irb.200 priority 500
   ```

Results

From configuration mode on Switch A, confirm your configuration by entering the **show chassis**, **show interfaces**, **show multi-chassis**, **show protocols**, and **show vlans** commands. If the output does not display the required configuration, repeat the instructions in this example to correct the configuration.

Switch A

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 3;
  }
}
```

```
user@SwitchA# show interfaces
xe-0/0/2 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/3 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/4 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/5 {
  ether-options {
    802.3ad ae2;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
      vlan {
        members v500;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
      active;
      system-id 00:01:02:03:04:05;
      admin-key 3;
    }
    mc-ae {
      mc-ae-id 3;
      chassis-id 0;
      mode active-active;
      status-control active;
      init-delay-time 240;
    }
  }
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
```



```
                vlan {
                    members v100;
                }
            }
        }
    }
    ae2 {
        aggregated-ether-options {
            lacp {
                active;
                system-id 00:01:02:03:04:06;
                admin-key 3;
            }
            mc-ae {
                mc-ae-id 4;
                chassis-id 0;
                mode active-active;
                status-control active;
                init-delay-time 240;
            }
        }
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members v200;
                }
            }
        }
    }
    irb {
        unit 100 {
            family inet {
                address 10.1.1.11/24 {
                    vrrp-group 1 {
                        virtual-address 10.1.1.1;
                        priority 200;
                        accept-data;
                    }
                }
            }
        }
        unit 200 {
            family inet {
                address 10.1.1.21/24 {
                    vrrp-group 2 {
                        virtual-address 10.1.1.2;
                        priority 200;
                        accept-data;
                    }
                }
            }
        }
        unit 500 {
            family inet {
                address 3.3.3.2/24;
```

```
        }
    }
}
user@SwitchA# show protocols
ospf {
    area 0.0.0.0 {
        interface irb.100 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
        interface irb.200 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
    }
}
pim {
    rp {
        static {
            address 1.0.0.3 {
                group-ranges {
                    239.0.0.0/8;
                }
            }
        }
    }
    interface irb.100 {
        priority 200;
    }
    interface irb.200 {
        priority 600;
    }
}
iccp {
    local-ip-addr 3.3.3.2;
    peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 60;
            transmit-interval {
                minimum-interval 60;
            }
```



```
        }
      }
    }
    igmp-snooping {
      vlan v100;
      vlan v200;
      vlan v500;
    }
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
  interface ae0;
}
```

```
user@SwitchA# show vlans
v100 {
  vlan-id 100;
  l3-interface irb.100;
}
v200 {
  vlan-id 200;
  l3-interface irb.200;
}
v500 {
  vlan-id 500;
  l3-interface irb.500;
}
```

Switch B

```
user@SwitchB# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchB# show interfaces
xe-0/0/2 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/3 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/6 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/7 {
  ether-options {
    802.3ad ae2;
  }
```



```
}
ae0 {
   unit 0 {
      family ethernet-switching {
         interface-mode trunk;
         vlan {
            members v500;
         }
      }
   }
}
ae1 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:05;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 3;
         chassis-id 1;
         mode active-active;
         status-control standby;
         init-delay-time 240;
      }
   }
   unit 0 {
      family ethernet-switching {
         interface-mode trunk;
         vlan {
            members v100;
         }
      }
   }
}
ae2 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:06;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 4;
         chassis-id 1;
         mode active-active;
         status-control standby;
         init-delay-time 240;
      }
   }
   unit 0 {
      family ethernet-switching {
         interface-mode trunk;
         vlan {
            members v200;
         }
```



```
        }
      }
    }
    irb {
      unit 100 {
        family inet {
          address 10.1.1.10/24 {
            vrrp-group 1 {
              virtual-address 10.1.1.1;
              priority 150;
              accept-data;
            }
          }
        }
      }
      unit 200 {
        family inet {
          address 10.1.1.20/24 {
            vrrp-group 2 {
              virtual-address 10.1.1.2;
              priority 150;
              accept-data;
            }
          }
        }
      }
      unit 500 {
        family inet {
          address 3.3.3.1/24;
        }
      }
    }

user@SwitchB# show protocols
ospf {
  area 0.0.0.0 {
    interface irb.100 {
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
    interface irb.200 {
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
  }
}
```

```
pim {
   rp {
      static {
         address 1.0.0.3 {
            group-ranges {
               239.0.0.0/8;
            }
         }
      }
   }
   interface irb.100 {
      priority 100;
   }
   interface irb.200 {
      priority 500;
   }
}
iccp {
   local-ip-addr 3.3.3.1;
   peer 3.3.3.2 {
      session-establishment-hold-time 50;
      backup-liveness-detection {
         backup-peer-ip 10.207.64.234;
      }
      liveness-detection {
         minimum-receive-interval 60;
         transmit-interval {
            minimum-interval 60;
         }
      }
   }
}
igmp-snooping {
   vlan v100;
   vlan v200;
   vlan v500;
}
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
   interface ae0;
}
```

```
user@SwitchB# show vlans
v100 {
   vlan-id 100;
   l3-interface irb.100;
}
v200 {
   vlan-id 200;
   l3-interface irb.200;
}
v500 {
   vlan-id 500;
   l3-interface irb.500;
}
```


Verification

Verify that the configuration is working properly.

- Confirm That Switch A Is the Master Designated Router on page 151
- Verifying That Switch B Is the Backup Designated Router on page 151

Confirm That Switch A Is the Master Designated Router

Purpose Verify that Switch A is the master designated router (DR).

Action

```
user@switch> 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          Down S     4 2   P2P,NotCap        0 0/0
irb.100             Up   S     4 2  DDR-DR,NotCap      1 0/0            10.1.1.11
irb.200             Up   S     4 2  DDR-DR,NotCap      2 0/0            10.1.1.21
```

Meaning The **DDR-DR** state of the VLAN interfaces in the output shows that Switch A is the master designated router.

Verifying That Switch B Is the Backup Designated Router

Purpose Confirm that Switch B is the backup designated router.

Action

```
user@switch> 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          Down S     4 2   P2P,NotCap        0 0/0
irb.100             Up   S     4 2  DDR-BDR,NotCap     1 0/0            10.1.1.11
irb.200             Up   S     4 2  DDR-BDR,NotCap     2 0/0            10.1.1.21
```

Meaning The **DDR-BDR** state of the VLAN interfaces in the output shows that Switch B is the backup designated router.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on EX Series Switches on page 32
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on EX9200 Switches on page 152
- Example: Configuring DHCP Relay on MC- LAG with VRRP on an EX9200 Switch on page 82

Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on EX9200 Switches

Supported Platforms EX Series

There are two methods for enabling Layer 3 unicast functionality across a multichassis link aggregation group (MC-LAG). You can choose either to configure Virtual Router Redundancy Protocol (VRRP) over the integrated routing and bridging (IRB) interface or to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG. The procedure to configure VRRP for use in a Layer 3 unicast MC-LAG is included in this example.

- Requirements on page 152
- Overview on page 152
- Configuration on page 154
- Verification on page 165
- Troubleshooting on page 170

Requirements

This example uses the following hardware and software components:

- Two EX9200 switches
- Junos OS Release 13.2R1 or later

Before you configure an MC-LAG, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Configuring an Aggregated Ethernet Interface*.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Configuring Aggregated Ethernet LACP*.
- Configure Virtual Router Redundancy Protocol (VRRP) on a switch. See *Configuring Basic VRRP Support*.

For a list of best practice configuration guidelines and important functional behavior for MC-LAGs, see the “MC-LAG Configuration Guidelines and Functional Behavior” section in the topic *Understanding Multichassis Link Aggregation*.

Overview

In this example, you configure an MC-LAG between two switches by including interfaces from both switches in an aggregated Ethernet interface (ae1). To support the MC-LAG, create a second aggregated Ethernet interface (ae0) for the interchassis link (ICL). Configure a multichassis protection link for the ICL, Interchassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the MC-LAG configuration, enable VRRP by completing the following tasks:

1. Create an integrated routing and bridging (IRB) interface.
2. Create a VRRP group and assign a virtual IP address that is shared between each switch in the VRRP group.
3. Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group.
4. Configure Layer 3 connectivity between the VRRP groups.

Topology

The topology used in this example consists of two switches that host an MC-LAG, ae1. The two switches are connected to a server. Figure 25 on page 153 shows the topology for this example.

Figure 25: Configuring an MC-LAG Between Switch A and Switch B

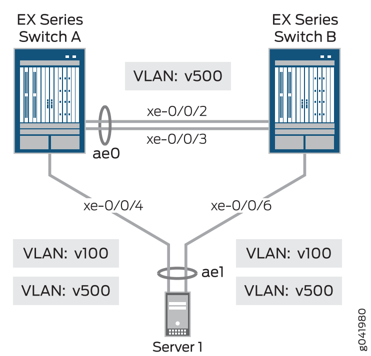


Table 8 on page 41 details the topology used in this configuration example.

Table 11: Components of the Topology for Configuring an MC-LAG Between Two Switches

Hostname	Base Hardware	Link Aggregation Groups
Switch A Switch B	EX9200 switch	• ae0 is configured as an aggregated Ethernet interface, and is used as an ICL. The following interfaces are part of ae0: xe-0/0/2 and xe-0/0/3 on Switch A and xe-0/0/2 and xe-0/0/3 on Switch B. • ae1 is configured as an MC-LAG, and the following two interfaces are part of ae1: xe-0/0/4 on Switch A and xe-0/0/6 on Switch B.

Configuration

CLI Quick Configuration

To quickly configure this example:

- Copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of Switch A.

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/2 ether-options 802.3ad ae0
set interfaces xe-0/0/3 ether-options 802.3ad ae0
set interfaces xe-0/0/4 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 60
set protocols rstp interface ae0.0 disable
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

- Copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of Switch B.

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/2 ether-options 802.3ad ae0
set interfaces xe-0/0/3 ether-options 802.3ad ae0
set interfaces xe-0/0/6 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
```



```
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 priority 150
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 accept-data
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 60
set protocols rstp interface ae0.0 disable
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Configuring MC-LAG for Layer 3 Unicast Using VRRP on Two Switches

Step-by-Step Procedure

To enable a multichassis protection link between MC-LAG peers:

The following procedure requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the number of LAGs on both Switch A and Switch B.

   ```
   [edit chassis]
     user@switch# set aggregated-devices ethernet device-count 2
   ```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   Switch A and Switch B

   ```
   [edit interfaces]
     user@switch# set xe-0/0/2 ether-options 802.3ad ae0
   [edit interfaces]
     user@switch# set xe-0/0/3 ether-options 802.3ad ae0
   ```

   Switch A

   ```
   [edit interfaces]
     user@switch# set xe-0/0/4 ether-options 802.3ad ae1
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set xe-0/0/6 ether-options 802.3ad ae1
   ```

3. Configure a trunk interface between Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set ae0 unit 0 family ethernet-switching interface-mode trunk
   ```

4. Configure a multichassis protection link between Switch A and Switch B.

Switch A

```
[edit]
  user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Switch B

```
[edit]
  user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Step-by-Step Procedure

To enable ICCP:

The following procedure requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address, minimum receive interval, and minimum transmit interval for a Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

   NOTE: **Configuring the minimum receive interval is required to enable BFD. We recommend a minimum receive interval value of 6 seconds.**

   Switch A

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval
     60
     user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
     minimum-interval 60
   ```

   Switch B

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
     60
     user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
     minimum-interval 60
   ```

3. (Optional) Configure the time during which an ICCP connection must be established between MC-LAG peers on Switch A and Switch B.

NOTE: Configuring session establishment hold time helps in faster ICCP connection establishment. The recommended value is 50 seconds.

Switch A

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
```

Switch B

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
```

4. (Optional) We recommend that you configure the backup liveness detection feature to implement faster failover of data traffic during an MC-LAG peer reboot. Configure the backup-liveness-detection statement on the management interface (fxp0) only.

NOTE: The backup-liveness-detection statement is supported starting in Junos OS Release 13.2R1.

Switch A

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip
  10.207.64.233
```

Switch B

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
  10.207.64.234
```

5. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B.

Switch A and B

```
[edit vlans]
  user@switch# set v500 vlan-id 500
  user@switch# set v500 l3-interface irb.500
[edit interfaces]
  user@switch# set ae0 unit 0 family ethernet-switching vlan members v500
```

Switch A

```
user@switch# set vlan unit 500 family inet address 3.3.3.2/24
```

Switch B

```
user@switch# set vlan unit 500 family inet address 3.3.3.1/24
```

Step-by-Step Procedure

To enable the MC-LAG interface:

The following procedure requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Enable LACP on the MC-LAG interface on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options lacp active
   ```

2. Specify the same multichassis aggregated Ethernet identification number on both MC-LAG peers on Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
   ```

3. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 0
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 1
   ```

4. Specify the operating mode of the MC-LAG on both Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
   ```

5. Specify the status control for MC-LAG on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAG. If one peer is in active mode, the other must be in standby mode.

   Switch A

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae status-control active
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae status-control standby
   ```

NOTE: You can configure the **prefer-status-control-active** statement with the mc-ae **status-control standby** configuration to prevent the LACP MC-LAG system ID from reverting to the default LACP system ID on ICCP failure. Use this configuration only if you can ensure that ICCP will not go down unless the router or switch is down. You must also configure the **hold-time down** value (at the **[edit interfaces *interface-name*]** hierarchy level) for the ICL with the mc-ae **status-control standby** configuration to be higher than the ICCP BFD timeout. This configuration prevents data traffic loss by ensuring that when the router or switch with the mc-ae **status-control active** configuration goes down, the router or switch with the mc-ae **status-control standby** configuration does not go into standby mode.

To make the **prefer-status-control-active** configuration work with the mc-ae **status-control standby** configuration when an ICL logical interface is configured on an aggregate Ethernet interface, you must either configure the ***lacp* periodic interval** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level as slow or configure the **detection-time threshold** statement at the **[edit protocols iccp peer *liveness-detection*]** hierarchy level as less than 3 seconds.

The **prefer-status-control-active** statement is supported starting in Junos OS Release 13.2R1.

6. To minimize traffic loss, specify the number of seconds by which to delay bringing the mc-ae interface back to the up state when you reboot Switch A or Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae init-delay-time 240**

7. Specify the same LACP system ID for the MC-LAG on Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05**

8. Specify the same LACP administration key on both Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options lacp admin-key 3**

9. Enable a VLAN on the MC-LAG on Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 unit 0 family ethernet-switching vlan members v100**

   [edit]
   user@switch# **set vlans v100 vlan-id 100**

10. Configure ae1 as the trunk interface between Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 unit 0 family ethernet-switching interface-mode trunk**

Step-by-Step Procedure

To enable VRRP on the MC-LAGs on Switch A and Switch B:

1. Create an integrated routing and bridging (IRB) interface for each MC-LAG, assign a virtual IP address that is shared between each switch in the VRRP group, and assign an individual IP address for each switch in the VRRP group.

   Switch A

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1
     virtual-address 10.1.1.1
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
     virtual-address 10.1.1.1
   ```

2. Assign the priority for each switch in the VRRP group:

   NOTE: The switch configured with the highest priority is the master.

   Switch A

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority
     200
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority
     150
   ```

3. Enable the switch to accept all packets destined for the virtual IP address if it is the master in a VRRP group:

   Switch A

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1
     accept-data
   ```

   Switch B

   ```
   [edit interfaces]
     user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
     accept-data
   ```

4. Configure Layer 3 connectivity between Switch A and Switch B.

   ```
   [edit]
     user@switch# set vlans v100 l3-interface irb.100
   ```

Step-by-Step Procedure

To disable RSTP:

NOTE: STP is not supported on the ICL or MC-LAG interfaces.

The following procedure requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Disable RSTP on the ICL interfaces on Switch A and Switch B:

```
[edit]
user@switch# set protocols rstp interface ae0.0 disable
```

Results

Display the results of the configuration on Switch A.

```
chassis {
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}
    interfaces {
        xe-0/0/2 {
            ether-options {
                802.3ad ae0;
            }
        }
        xe-0/0/3 {
            ether-options {
                802.3ad ae0;
            }
        }
        xe-0/0/4 {
            ether-options {
                802.3ad ae1;
            }
        }
        ae0 {
            unit 0 {
                family ethernet-switching {
                    interface-mode trunk;
                    vlan {
                        members v500;
                    }
                }
            }
        }
        ae1 {
            aggregated-ether-options {
```

```
            lacp {
                active;
                system-id 00:01:02:03:04:05;
                admin-key 3;
            }
            mc-ae {
                mc-ae-id 3;
                chassis-id 0;
                mode active-active;
                status-control active;
                init-delay-time 240;
            }
        }
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members v100;
                }
            }
        }
    }
    irb {
        unit 100 {
            family inet {
                address 100.1.1.11/24 {
                    vrrp-group 1 {
                        virtual-address 100.1.1.1;
                        priority 200;
                        accept-data;
                    }
                }
            }
        }
        unit 500 {
            family inet {
                address 3.3.3.2/24;
            }
        }
    }
}
protocols {
    iccp {
        local-ip-addr 3.3.3.2;
        peer 3.3.3.1 {
            session-establishment-hold-time 50;
            backup-liveness-detection {
                backup-peer-ip 10.207.64.233;
            }
            liveness-detection {
                minimum-receive-interval 60;
                transmit-interval {
                    minimum-interval 60;
                }
            }
        }
```



```
      }
      rstp {
        interface ae0.0 {
          disable;
        }
      }
    }
    multi-chassis {
      multi-chassis-protection 3.3.3.1 {
        interface ae0;
      }
    }
    vlans {
      v100 {
        vlan-id 100;
        l3-interface irb.100;
      }
      v500 {
        vlan-id 500;
        l3-interface irb.500;
      }
    }
```

Display the results of the configuration on Switch B.

```
chassis {
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}
  interfaces {
    xe-0/0/2 {
      ether-options {
        802.3ad ae0;
      }
    }
    xe-0/0/3 {
      ether-options {
        802.3ad ae0;
      }
    }
    xe-0/0/4 {
      ether-options {
        802.3ad ae1;
      }
    }
    ae0 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
            members v500;
          }
        }
```

```
            }
        }
        ae1 {
            aggregated-ether-options {
                lacp {
                    active;
                    system-id 00:01:02:03:04:05;
                    admin-key 3;
                }
                mc-ae {
                    mc-ae-id 3;
                    chassis-id 1;
                    mode active-active;
                    status-control active;
                    init-delay-time 240;
                }
            }
            unit 0 {
                family ethernet-switching {
                    interface-mode trunk;
                    vlan {
                        members v100;
                    }
                }
            }
        }
        irb {
            unit 100 {
                family inet {
                    address 100.1.1.10/24 {
                        vrrp-group 1 {
                            virtual-address 100.1.1.1;
                            priority 200;
                            accept-data;
                        }
                    }
                }
            }
            unit 500 {
                family inet {
                    address 3.3.3.1/24;
                }
            }
        }
    }
    protocols {
        iccp {
            local-ip-addr 3.3.3.1;
            peer 3.3.3.2 {
                session-establishment-hold-time 50;
                backup-liveness-detection {
                    backup-peer-ip 10.207.64.234;
                }
                liveness-detection {
                    minimum-receive-interval 60;
                    transmit-interval {
```



```
                        minimum-interval 60;
                    }
                }
            }
        }
        rstp {
            interface ae0.0 {
                disable;
            }
        }
    }
    multi-chassis {
        multi-chassis-protection 3.3.3.2 {
            interface ae0;
        }
    }
    vlans {
        v100 {
            vlan-id 100;
            l3-interface irb.100;
        }
        v500 {
            vlan-id 500;
            l3-interface irb.500;
        }
    }
```

Verification

To verify that the MC-LAG group has been created and is working properly, perform these tasks:

Verifying That ICCP Is Working on Switch A

Purpose Verify that ICCP is running on Switch A.

Action

```
[edit]
user@switch# show iccp
Redundancy Group Information for peer 3.3.3.1
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That ICCP Is Working on Switch B

Purpose Verify that ICCP is running on Switch B.

Action **show iccp**

```
[edit]
user@switch# show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That LACP Is Active on Switch A

Purpose Verify that LACP is active on Switch A.

Action

```
[edit]
user@switch# show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role    Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/6       Actor    No    No   Yes   Yes  Yes   Yes     Fast    Active
      xe-0/0/6     Partner    No    No   Yes   Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/6                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch A is participating in LACP negotiation.

Verifying That LACP Is Active on Switch B

Purpose Verify that LACP is active on Switch B

Action

```
[edit]
user@switch# show lacp interfaces

Aggregated interface: ae1
    LACP state:       Role    Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/4       Actor     No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/4     Partner     No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/4                  Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch B is participating in LACP negotiation.

Verifying That the MC-AE and ICL Interfaces Are Up on Switch A

Purpose Verify that the MC-AE and ICL interfaces are up on Switch A.

Action

```
[edit]
user@switch# 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         : 3.3.3.1 ae0.0 up
```

Meaning This output shows that the MC-AE interface on Switch A is up and active.

Verifying That the MC-AE and ICL Interfaces Are Up on Switch B

Purpose Verify that the MC-AE and ICL interfaces are up on Switch B.

Action

```
[edit]
user@switch# 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         : 3.3.3.2 ae0.0 up
```

Meaning This output shows that the MC-AE interface on Switch B is up and active.

Verifying That MAC Learning Is Occurring on Switch A

Purpose Verify that MAC learning is working on Switch A.

Action

```
[edit]
user@switch# show ethernet-switching table
Ethernet-switching table: 6 entries, 1 learned, 0 persistent entriesC
  VLAN              MAC address       Type         Age Interfaces
  v100              *                 Flood          - All-members
  v100              00:00:5e:00:01:01 Static         - Router
  v100              78:fe:3d:5a:07:42 Static         - Router
  v100              78:fe:3d:5b:ad:c2 Learn(R)       0 ae0.0
  v500              *                 Flood          - All-members
  v500              78:fe:3d:5a:07:42 Static         - Router
```

Meaning The output shows two static MAC address in VLAN v100 and one static MAC address in VLAN v500. These addresses belong to the Layer 3 IRB addresses on both Switch A and Switch B that you configured in the MC-LAG. The ICL interface configured on the VRRP master member learned the VLAN v100 Learn (R) MAC address of the VRRP backup member.

Verifying That MAC Learning Is Occurring on Switch B

Purpose Verify that MAC learning is working on Switch B.

Action

```
[edit]
user@switch# show ethernet-switching table
Ethernet-switching table: 7 entries, 1 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v100              *                 Flood          - All-members
  v100              00:00:5e:00:01:01 Static         - Router
  v100              78:fe:3d:5a:07:42 Learn(R)       0 ae0.0
  v100              78:fe:3d:5b:ad:c2 Static         - Router
  v200              78:fe:3d:5b:ad:c2 Static         - Router
  v500              *                 Flood          - All-members
  v500              78:fe:3d:5b:ad:c2 Static         - Router
```

Meaning The output shows two static MAC address in VLAN v100 and one static MAC address in VLAN v500. These addresses belong to the Layer 3 IRB addresses on both Switch A and Switch B that you configured in the MC-LAG. The ICL interface configured on the VRRP backup member learned the VLAN v100 Learn (R) MAC address of the VRRP master member.

Verifying That Switch A is the Master in the VRRP Group

Purpose Verify that Switch A is the master member in the VRRP group.

Action

```
[edit]
user@switch# show vrrp
Interface     State       Group   VR state VR Mode    Timer    Type   Address
 irb.100      up              1   master   Active      A  0.605 lcl    100.1.1.11

                                                              vip    100.1.1.1
```

Meaning The output shows that Switch A is the master member in the VRRP group.

Verifying That Switch B is the Backup Member in the VRRP Group

Purpose Verify that Switch B is the backup member in the VRRP group.

Action

```
[edit]
user@switch# show vrrp
Interface     State       Group   VR state VR Mode    Timer    Type   Address
  irb.100      up              1   backup   Active      A  0.605 lcl    100.1.1.10

                                                              vip    100.1.1.1
```

Meaning The output shows that Switch B is the backup member in the VRRP group.

Verifying That the Virtual IP Address is Attached to an Individual Address on Switch A

Action

```
[edit]
user@switch# run show interfaces terse vlan
Interface               Admin Link Proto    Local                 Remote
irb                     up    up
irb.100                 up    up   inet     100.1.1.1/24
                                            100.1.1.11/24
irb.500                 up    up   inet     3.3.3.2/24
```

Meaning The output shows that the virtual IP address (100.1.1.1/24) is bound to the individual IP address (100.1.1.11/24) on Switch A.

Verifying That the Virtual IP Address is Attached to an Individual Address on Switch B

Action

```
[edit]
user@switch# run show interfaces terse vlan
Interface               Admin Link Proto    Local                 Remote
irb                     up    up
irb.100                 up    up   inet     100.1.1.1/24
                                            100.1.1.10/24
irb.500                 up    up   inet     3.3.3.1/24
```

Meaning The output shows that the virtual IP address (100.1.1.1/24) is bound to the individual IP address (100.1.1.10/24) on Switch B.

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**

Solution Check the following:

- Verify that there is no configuration mismatch.
- Verify that all member ports are up.
- Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
- Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on EX Series Switches on page 32
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on EX9200 Switches on page 130
- Example: Configuring DHCP Relay on MC- LAG with VRRP on an EX9200 Switch on page 82

Example: Configuring Multichassis Link Aggregation with Layer 3 MAC Address Synchronization

Supported Platforms EX4600, QFX Series standalone switches

NOTE: Multichassis link aggregation (MC-LAG) is supported on QFX3500 and QFX3600 standalone switches running the original CLI and QFX5100 standalone switches running Enhanced Layer 2 Software.

NOTE: Issuing a PING request on an MC-LAG with MAC synchronization enabled does not work.

There are two methods for enabling Layer 3 unicast functionality across a multichassis link aggregation group (MC-LAG) to control the traffic. You can choose either to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG, or you can configure Virtual Router Redundancy Protocol (VRRP), but you cannot configure both at the same time. Because RVI interfaces share the same MAC address, if you enable MAC address synchronization, packets received on an MC-LAG peer with a destination MAC address that is the same as that of the peer's IRB MAC address will not be forwarded. The procedure to configure MAC address synchronization is included in this example. For more information about configuring VRRP for use in a Layer 3 unicast MC-LAG, see "Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP" on page 208.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.3 or later for the QFX3500 and QFX3600 standalone switches and Junos OS Release 13.2X51-D10 or later for the QFX5100 standalone switches
- Two QFX3500 or QFX3600 standalone switches, or two QFX5100 standalone switches

Before you configure an MC-LAG for Layer 3 unicast, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch*.
- Configure Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch*.

Overview

In this example, you configure an MC-LAG across two switches, consisting of two aggregated Ethernet interfaces, an interchassis control link-protection link (ICL-PL), multichassis protection link for the ICL-PL, Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers. Layer 3 connectivity is required for ICCP.

Topology

The topology used in this example consists of two switches hosting an MC-LAG. The two switches are connected to a server. Figure 1 on page 40 shows the topology of this example.

Figure 26: Configuring a Multichassis LAG Between Switch A and Switch B

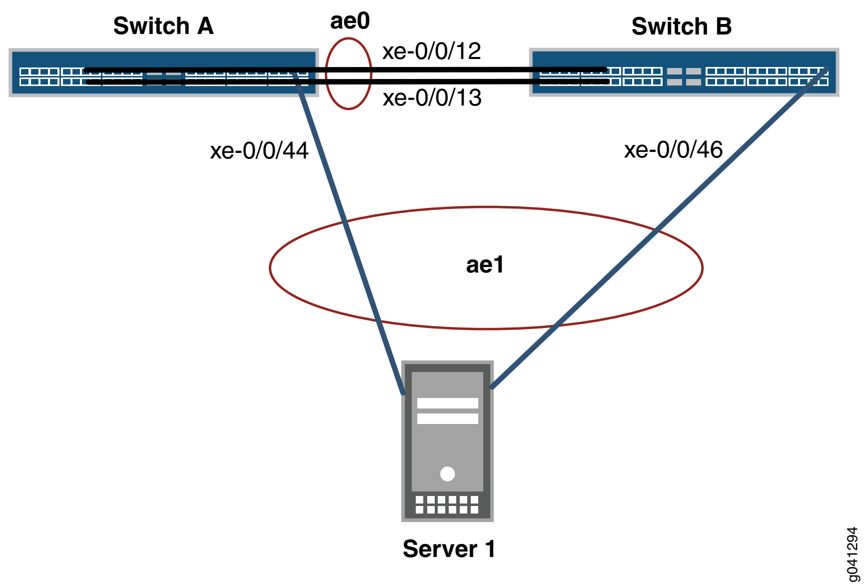


Table 8 on page 41 details the topology used in this configuration example.

Table 12: Components of the Topology for Configuring a Multichassis LAG Between Two Switches

Hostname	Base Hardware	Multichassis Link Aggregation Group
Switch A Switch B	QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch	ae0 is configured as an aggregated Ethernet interface, and is used as an ICL-PL. The following interfaces are part of ae0: xe-0/0/12 and xe-0/0/13 Switch A and xe-0/0/12 and xe-0/0/13 on Switch B. ae1 is configured as an MC-LAG, and the following two interfaces are part of ae1: xe-0/0/44 on Switch A and xe-0/0/46 on Switch B. .

Configuration

CLI Quick Configuration

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

NOTE: This example shows how to configure MC-LAG using both the original CLI and Enhanced Layer 2 Software (ELS).

In ELS, there are different statements and one additional statement that are different from the original CLI:

- The **port-mode** statement in the **[edit interfaces *interface-name* unit *number* family ethernet-switching]** hierarchy is not supported. Use the **interface-mode** statement instead.
- The **vlan** statement in the **[edit interfaces *interface-name*]** hierarchy is not supported. Use the **irb** statement instead.
- The **vlan.*logical-interface-number*** hierarchy in the **[edit vlans *vlan-name* l3-interface]** option is not supported. Use the **irb.*logical-interface-number*** option instead.
- The **service-id** statement in the **[edit switch-options]** hierarchy is required in the ELS CLI.

Switch A—Original CLI

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch A—ELS

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
set switch-options service-id 10
```

Switch B—Original CLI

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
```



```
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Switch B—ELS

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
set switch-options service-id 10
```

Configuring MC-LAG on Two Switches

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable multichassis protection link between MC-LAG peers:

1. Configure the number of LAGs on both Switch A and Switch B.

   ```
   [edit chassis]
   user@switch# set aggregated-devices ethernet device-count 2
   ```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set xe-0/0/12 ether-options 802.3ad ae0
   ```

```
[edit interfaces]
  user@switch# set xe-0/0/13 ether-options 802.3ad ae0
```

Switch A:

```
[edit interfaces]
  user@switch# set xe-0/0/44 ether-options 802.3ad ae1
```

Switch B:

```
[edit interfaces]
  user@switch# set xe-0/0/46 ether-options 802.3ad ae1
```

3. Configure a trunk interface between Switch A and Switch B.

Original CLI:

```
[edit interfaces]
  user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk
```

ELS:

```
[edit interfaces]
  user@switch# set ae0 unit 0 family ethernet-switching interface-mode trunk
```

4. Configure a multichassis protection link between Switch A and Switch B.

Switch A:

```
[edit]
  user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch B:

```
[edit]
  user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Step-by-Step Procedure

To enable ICCP:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

Switch A:

```
[edit protocols]
  user@switch# set iccp local-ip-addr 3.3.3.2
```

Switch B:

```
[edit protocols]
  user@switch# set iccp local-ip-addr 3.3.3.1
```

2. Configure the peer IP address and minimum receive interval for a (BFD) session for ICCP on Switch A and Switch B.

Switch A:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval
  1000
```

Switch B:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
  1000
```

3. Configure the peer IP address and minimum transmit interval for Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

Switch A:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
  minimum-interval 1000
```

Switch B:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
  minimum-interval 1000
```

4. (Optional) Configure the time during which an ICCP connection must succeed between MC-LAG peers on Switch A and Switch B.

NOTE: Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

Switch A:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
```

Switch B:

```
[edit protocols]
  user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
```

5. (Optional) Configure the backup IP address to be used for backup liveness detection on both Switch A and Switch B.

NOTE: By default, backup liveness detection is not enabled. Configuring a backup IP address helps achieve sub-second traffic loss during a MC-LAG peer reboot.

Switch A:

[edit protocols]
user@switch# **set** iccp peer **3.3.3.1** backup-liveness-detection backup-peer-ip **10.207.64.233**

Switch B:

[edit protocols]
user@switch# **set** iccp peer **3.3.3.2** backup-liveness-detection backup-peer-ip **10.207.64.234**

6. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B.

Original CLI:

[edit vlans]
user@switch# **set v100 vlan-id 100**

[edit vlans]
user@switch# **set v500 vlan-id 500**

[edit vlans]
user@switch# **set v500 l3-interface vlan.500**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching port-mode trunk**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching vlan members v500**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching vlan members v100**

ELS:

[edit vlans]
user@switch# **set v500 vlan-id 500**

[edit vlans]
user@switch# **set v500 l3-interface irb.500**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching interface-mode trunk**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching vlan members v500**

[edit interfaces]
user@switch# **set ae0 unit 0 family ethernet-switching vlan members v100**

Step-by-Step Procedure

To enable the MC-LAG interface:

1. Enable LACP on the MC-LAG interface on Switch A and Switch B.

NOTE: At least one end needs to be active. The other end can be either active or passive.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options lacp active
```

2. Specify the same multichassis aggregated Ethernet identification number on both MC-LAG peers on Switch A and Switch B.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
```

3. Specify the same service ID on Switch A and Switch B.

   ELS:

```
[edit]
  user@switch# set switch-options service-id 10
```

4. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A:

```
[edit interfaces]
  set ae1 aggregated-ether-options mc-ae chassis-id 0
```

   Switch B:

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 1
```

5. Specify the operating mode of the MC-LAG on both Switch A and Switch B.

   NOTE: Only active-active mode is supported at this time.

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
```

6. Specify the status control for MC-LAG on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAG. If one peer is in active mode, the other must be in standby mode.

   Switch A:

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae status-control active
```

   Switch B:

```
[edit interfaces]
  user@switch# set ae1 aggregated-ether-options mc-ae status-control standby
```

7. Specify the number of seconds by which the bring-up of the multichassis aggregated Ethernet interface should be deferred after you reboot Switch A and Switch B.

   NOTE: The recommended value for maximum VLAN configuration (for example, 4,000 VLANS) is 240 seconds. If IGMP snooping is enabled on all of the VLANs, the recommended value is 420 seconds.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options mc-ae init-delay-time 240
   ```

8. Specify the same LACP system ID for the MC-LAG on Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05
   ```

9. Specify the same LACP administration key on both Switch A and Switch B.

   ```
   [edit interfaces]
     user@switch# set ae1 aggregated-ether-options lacp admin-key 3
   ```

10. Enable a VLAN on the MC-LAG on Switch A and Switch B-—**Original CLI**:

    ```
    [edit interfaces]
      user@switch# set ae1 unit 0 family ethernet-switching port-mode trunk
    [edit]
      user@switch# set vlans v100 vlan-id 100
    [edit interfaces]
      user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
    ```

11. Enable a VLAN on the MC-LAG on Switch A and Switch B using **ELS**:

    ```
    [edit interfaces]
      user@switch# set ae1 unit 0 family ethernet-switching interface-mode trunk
    [edit]
      user@switch# set vlans v100 vlan-id 100
    [edit interfaces]
      user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
    ```

Step-by-Step Procedure

To enable RSTP:

1. Enable RSTP globally on all interfaces on Switch A and Switch B.

   NOTE: The **all** option is not available on ELS, so you cannot issue this command on ELS.

   ```
   [edit]
     user@switch# set protocols rstp interface all mode point-to-point
   ```


ELS:

```
[edit]
  user@switch# set protocols rstp interface ae1.0 mode point-to-point
```

2. Disable RSTP on the ICL-PL interfaces on Switch A and Switch B.

   NOTE: This command is not needed on ELS.

   ```
   [edit]
     user@switch# set protocols rstp interface ae0.0 disable
   ```

3. Configure the MC-LAG interfaces as edge ports on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
     user@switch# set protocols rstp interface ae1.0 edge
   ```

4. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
     user@switch# set protocols rstp bpdu-block-on-edge
   ```

Results

From configuration mode, confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Switch A—Original CLI

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}

user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
```



```
            802.3ad ae0;
        }
    }
    xe-0/0/13 {
        ether-options {
            802.3ad ae0;
        }
    }
    xe-0/0/44 {
        ether-options {
            802.3ad ae1;
        }
    }
    ae0 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members v500;
                }
            }
        }
    }
    ae1 {
        aggregated-ether-options {
            lacp {
                active;
                system-id 00:01:02:03:04:05;
                admin-key 3;
            }
            mc-ae {
                mc-ae-id 3;
                chassis-id 0;
                mode active-active;
                status-control active;
                init-delay-time 240;
            }
        }
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members v100;
                }
            }
        }
    }
    vlan {
        unit 500 {
            family inet {
                address 3.3.3.2/24;
            }
        }
    }
```

user@SwitchA# **show protocols**

```
iccp {
  local-ip-addr 3.3.3.2;
  peer 3.3.3.1 {
    session-establishment-hold-time 50;
    backup-liveness-detection {
      backup-peer-ip 10.207.64.233;
    }
    liveness-detection {
      minimum-receive-interval 1000;
      transmit-interval {
        minimum-interval 1000;
      }
    }
  }
}
rstp {
  interface ae0.0 {
    disable;
  }
  interface ae1.0 {
    edge;
  }
  interface all {
    mode point-to-point;
  }
  bpdu-block-on-edge;
}
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
  interface ae0;
}
```

```
user@SwitchA# show vlans
v100 {
  vlan-id 100;
}
v500 {
  vlan-id 500;
  l3-interface vlan.500;
}
```

Switch A--ELS

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
```

```
xe-0/0/13 {
   ether-options {
      802.3ad ae0;
   }
}
xe-0/0/44 {
   ether-options {
      802.3ad ae1;
   }
}
ae0 {
   unit 0 {
      family ethernet-switching {
         interface-mode trunk;
         vlan {
            members v500;
         }
      }
   }
}
ae1 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:05;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 3;
         chassis-id 0;
         mode active-active;
         status-control active;
         init-delay-time 240;
      }
   }
   unit 0 {
      family ethernet-switching {
         interface-mode trunk;
         vlan {
            members v100;
         }
      }
   }
}
vlan {
   unit 500 {
      family inet {
         address 3.3.3.2/24;
      }
   }
}

user@SwitchA# show protocols
iccp {
   local-ip-addr 3.3.3.2;
   peer 3.3.3.1 {
```



```
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae1.0 {
        edge;
    }
    mode point-to-point;
    }
    bpdu-block-on-edge;
    }
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
    interface ae0;
}
```

```
user@SwitchA# show switch-options
service-id 10;
```

```
user@SwitchA# show vlans
v100 {
    vlan-id 100;
}
v500 {
    vlan-id 500;
    l3-interface irb.500;
}
```

Switch B—Original CLI

```
user@SwitchB# show chassis
aggregated-devices {
    ethernet {
        device-count 2;
    }
}
```

```
user@SwitchB# show interfaces
xe-0/0/12 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/13 {
    ether-options {
        802.3ad ae0;
    }
}
```

```
xe-0/0/46 {
   ether-options {
      802.3ad ae1;
   }
}
ae0 {
   unit 0 {
      family ethernet-switching {
         port-mode trunk;
         vlan {
            members v500;
         }
      }
   }
}
ae1 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:05;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 3;
         chassis-id 1;
         mode active-active;
         status-control standby;
         init-delay-time 240;
      }
   }
   unit 0 {
      family ethernet-switching {
         port-mode trunk;
         vlan {
            members v100;
         }
      }
   }
}
vlan {
   unit 500 {
      family inet {
         address 3.3.3.1/24;
      }
   }
}

user@SwitchB# show protocols
iccp {
   local-ip-addr 3.3.3.1;
   peer 3.3.3.2 {
      session-establishment-hold-time 50;
      backup-liveness-detection {
         backup-peer-ip 10.207.64.234;
      }
      liveness-detection {
```



```
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
    interface ae0;
}
```

```
user@SwitchB# show vlans
v100 {
    vlan-id 100;
}
v500 {
    vlan-id 500;
    l3-interface vlan.500;
}
```

Switch B--ELS

```
user@SwitchB# show chassis
aggregated-devices {
    ethernet {
        device-count 2;
    }
}
```

```
user@SwitchB# show interfaces
xe-0/0/12 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/13 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/46 {
    ether-options {
        802.3ad ae1;
```

```
    }
}
ae0 {
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v500;
            }
        }
    }
}
ae1 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:05;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 3;
            chassis-id 1;
            mode active-active;
            status-control standby;
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 500 {
        family inet {
            address 3.3.3.1/24;
        }
    }
}
```

```
user@SwitchB# show protocols
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
```



```
      }
    }
  }
}
rstp {
  interface ae1.0 {
    edge;
  }
  mode point-to-point;
  }
  bpdu-block-on-edge;
  }
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
  interface ae0;
}
```

```
user@SwitchB# show switch-options
service-id 10;
```

```
user@SwitchB# show vlans
v100 {
  vlan-id 100;
}
v500 {
  vlan-id 500;
  l3-interface irb.500;
}
```

Verification

Verify that the configuration is working properly.

- Verifying That ICCP Is Working on Switch A on page 189
- Verifying That ICCP Is Working on Switch B on page 190
- Verifying That LACP Is Active on Switch A on page 190
- Verifying That LACP Is Active on Switch B on page 190
- Verifying That the Multichassis Aggregated Ethernet and ICL-PL Interfaces Are Up on Switch A on page 191
- Verifying That the Multichassis Aggregated Ethernet and ICL-PL Interfaces Are Up on Switch B on page 191
- Verifying That MAC Learning Is Occurring on Switch A and Switch B on page 192

Verifying That ICCP Is Working on Switch A

Purpose Verify that ICCP is running on Switch A.

Action

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.1
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That ICCP Is Working on Switch B

Purpose Verify that ICCP is running on Switch B.

Action **show iccp**

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That LACP Is Active on Switch A

Purpose Verify that LACP is active on Switch A.

Action

```
[edit]
user@switch> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/46      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/46    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/46                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch A is participating in LACP negotiation.

Verifying That LACP Is Active on Switch B

Purpose Verify that LACP is active on Switch B.

Action

```
[edit]
user@switch> show lacp interfaces

Aggregated interface: ae1
    LACP state:       Role    Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/44      Actor     No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/44    Partner     No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/44                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch B is participating in LACP negotiation.

Verifying That the Multichassis Aggregated Ethernet and ICL-PL Interfaces Are Up on Switch A

Purpose Verify that the multichassis aggregated Ethernet and ICL-PL interfaces are up on Switch A.

Action

```
[edit]
user@switch> 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        : 3.3.3.1 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet and ICL-PL interfaces on Switch A is up and active.

Verifying That the Multichassis Aggregated Ethernet and ICL-PL Interfaces Are Up on Switch B

Purpose Verify that the multichassis aggregated Ethernet and ICL-PL interfaces are up on Switch B.

Action

```
[edit]
user@switch> 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        : 3.3.3.2 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet and ICL-PL interface on Switch B is up and active.

Verifying That MAC Learning Is Occurring on Switch A and Switch B

Purpose Verify that MAC learning is working on Switch A and B.

Action

```
[edit]
user@switch> show ethernet-switching table
Ethernet-switching table: 10 entries, 4 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v222              *                 Flood          - All-members
  v222              00:00:5e:00:01:01 Static         - Router
  v222              00:10:94:00:00:05 Learn(L)      33 ae0.0 (MCAE)
  v222              84:18:88:df:ac:ae Learn(R)       0 ae2.0
```

Meaning The output shows four learned MAC addresses entries.

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**.

Solution Check the following:

1. Verify that there is no configuration mismatch.
2. Verify that all member ports are up.
3. Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
4. Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on page 35

• Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on page 235

Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast using MAC Address Synchronization

Supported Platforms QFabric System, QFX Series standalone switches

There are two methods for enabling Layer 3 unicast functionality across a multichassis link aggregation group (MC-LAG). You can choose either to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG, or you can configure Virtual Router Redundancy Protocol (VRRP), but you cannot configure both at the same time. Because RVI interfaces share the same MAC address, if you enable MAC address synchronization, packets received on an MC-LAG peer with a destination MAC address that is the same as that of the peer's IRB MAC address will not be forwarded. The procedure to configure MAC address synchronization is included in this example. For more information on configuring VRRP for use in a Layer 3 unicast MC-LAG, see "Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP" on page 208.

• Requirements on page 193
• Overview on page 193
• Configuration on page 195
• Verification on page 205
• Troubleshooting on page 208

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.3 or later for the QFX Series
- Two QFX3500 or QFX3600 switches

Before you configure an MC-LAG for Layer 3 unicast, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch*.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch*.
- Configure a standard MC-LAG between switches. See "Example: Configuring Multichassis Link Aggregation" on page 39.

Overview

In this example, you configure an MC-LAG across two switches by including interfaces from both switches in an aggregated Ethernet interface (ae1). To support the MC-LAG, create a second aggregated Ethernet interface (ae0) for the interchassis control link-protection link (ICL-PL). Configure a multichassis protection link for the ICL-PL, Interchassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the configuration, configure MAC address synchronization between the peers and specify the same IP address on both Layer 3 interface members (also known as the routed VLAN interface [RVI] or the integrated routing and bridging (IRB) interface) in the MC-LAG VLAN.

Topology

The topology used in this example consists of two switches hosting an MC-LAG. The two switches are connected to a server. Figure 27 on page 194 shows the topology of this example.

Figure 27: Configuring a Multichassis LAG Between Switch A and Switch B

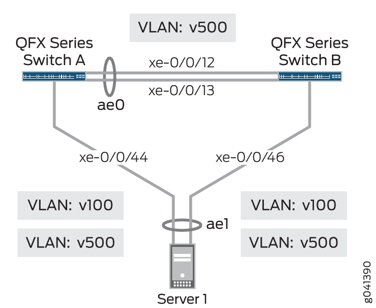


Table 8 on page 41 details the topology used in this configuration example.

Table 13: Components of the Topology for Configuring a Multichassis LAG Between Two Switches

Hostname	Base Hardware	Multichassis Link Aggregation Group
Switch A	QFX3500 switch or QFX3600 switch	**ae0** is configured as an aggregated Ethernet interface, and is used as an ICL-PL. The following interfaces are part of **ae0**: **xe-0/0/12** and **xe-0/0/13** on Switch A and **xe-0/0/12** and **xe-0/0/13** on Switch B. These interfaces are included in VLAN v500. **ae1** is configured as an MC-LAG, and the following two interfaces are part of **ae1**: **xe-0/0/44** on Switch A and **xe-0/0/46** on Switch B. These interfaces are included in VLAN v100.
Switch B	QFX3500 switch or QFX3600 switch	

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of Switch A.

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 100 family inet address 100.1.1.10
set interfaces vlan unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v100 mcae-mac-synchronize
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 60
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of Switch B.

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae0 unit 0 family ethernet-switching vlan members v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
```

set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 100 family inet address 100.1.1.10
set interfaces vlan unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v100 mcae-mac-synchronize
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 60
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 60
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0

Configuring MC-LAG on Two Switches

Step-by-Step Procedure

To enable multichassis protection link between MC-LAG peers:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the number of LAGs on both Switch A and Switch B.

```
[edit chassis]
user@switch# set aggregated-devices ethernet device-count 2
```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

```
[edit interfaces]
user@switch# set xe-0/0/12 ether-options 802.3ad ae0
[edit interfaces]
user@switch# set xe-0/0/13 ether-options 802.3ad ae0
[edit interfaces]
user@switch# set xe-0/0/44 ether-options 802.3ad ae1
[edit interfaces]
user@switch# set xe-0/0/46 ether-options 802.3ad ae1
```

3. Configure a trunk interface between Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk
```

4. Configure a multichassis protection link between Switch A and Switch B.

   Switch A:

```
[edit]
user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

   Switch B:

```
[edit]
user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```


Step-by-Step Procedure

To enable ICCP:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address and minimum receive interval for a (BFD) session for ICCP on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 60
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 60
   ```

3. Configure the peer IP address and minimum transmit interval for Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval
   60
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval
   60
   ```

4. (Optional) Configure the time during which an ICCP connection must succeed between MC-LAG peers on Switch A and Switch B.

   NOTE: Configuring session establishment hold time helps in faster ICCP connection establishment. The recommended value is 50 seconds.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
   ```

   Switch B:

   ```
   [edit protocols]
   ```

```
user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
```

5. (Optional) Configure the backup IP address to be used for backup liveness detection on both Switch A and Switch B.

   NOTE: By default, backup liveness detection is not enabled. Configuring a backup IP address helps achieve sub-second traffic loss during a MC-LAG peer reboot.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
   ```

6. Configure Layer 3 connectivity across the ae0 ICCP link by adding a Layer 3 interface on both Switch A and Switch B.

   ```
   [edit vlans]
   user@switch# set v500 vlan-id 500
   [edit vlans]
   user@switch# set v500 l3-interface vlan.500
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk vlan members
   v500
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk vlan members
   v100
   ```

Step-by-Step Procedure

To enable the MC-LAG interface:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Enable LACP on the MC-LAG interface on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp active
   ```

2. Specify the same multichassis aggregated Ethernet identification number on both MC-LAG peers on Switch A and Switch B.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae mc-ae-id 3
   ```

3. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

Switch A:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 0
```

Switch B:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae chassis-id 1
```

4. Specify the operating mode of the MC-LAG on both Switch A and Switch B.

   NOTE: Only active-active mode is supported at this time.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
```

5. Specify the status control for MC-LAG on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAG. If one peer is in active mode, the other must be in standby mode.

   Switch A:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae status-control active
```

   Switch B:

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae status-control standby
```

6. Specify the number of seconds by which the bring-up of the MC-AE interface should be deferred after you reboot Switch A and Switch B.

   NOTE: The recommended value for maximum VLAN configuration (for example, 4,000 VLANS) is 240 seconds. If IGMP snooping is enabled on all of the VLANs, the recommended value is 420 seconds.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae init-delay-time 240
```

7. Specify the same LACP system ID for the MC-LAG on Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05
```

8. Specify the same LACP administration key on both Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options lacp admin-key 3
```

9. Enable a VLAN on the MC-LAG on Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching port-mode trunk
```

```
[edit]
user@switch# set vlans v100 vlan-id 100
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
```

10. Create a Layer 3 interface for the MC-LAG VLAN and assign the same IP address on both Switch A and Switch B.

```
[edit]
user@switch# set vlans v100 l3-interface vlan.100
[edit interfaces]
user@switch# set vlan unit 100 family inet address 100.1.1.10
```

11. Configure MAC address synchronization in the MC-LAG VLAN on both Switch A and Switch B.

```
[edit]
user@switch# set vlans v100 mcae-mac-synchronize
```

Step-by-Step Procedure

To enable RSTP:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Enable RSTP globally on all interfaces on Switch A and Switch B.

```
[edit]
user@switch# set protocols rstp interface all mode point-to-point
```

2. Disable RSTP on the ICL-PL interfaces on Switch A and Switch B:

```
[edit]
user@switch# set protocols rstp interface ae0.0 disable
```

3. Configure the MC-LAG interfaces as edge ports on Switch A and Switch B.

NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit]
user@switch# set protocols rstp interface ae1.0 edge
```

4. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on Switch A and Switch B.

NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit]
user@switch# set protocols rstp bpdu-block-on-edge
```

Results

Display the results of the configuration on Switch A.

```
chassis {
```



```
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}
interfaces {
  xe-0/0/12 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/0/13 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/0/44 {
    ether-options {
      802.3ad ae1;
    }
  }
  ae0 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members v500;
        }
      }
    }
  }
  ae1 {
    aggregated-ether-options {
      lacp {
        active;
        system-id 00:01:02:03:04:05;
        admin-key 3;
      }
      mc-ae {
        mc-ae-id 3;
        chassis-id 0;
        mode active-active;
        status-control active;
        init-delay-time 240
      }
    }
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members v100;
        }
      }
    }
  }
```

```
    vlan {
        unit 100 {
            family inet {
                address 100.1.1.10/32;
            }
        }
        unit 500 {
            family inet {
                address 3.3.3.2/24;
            }
        }
    }
}
protocols {
    iccp {
        local-ip-addr 3.3.3.2;
        peer 3.3.3.1 {
            session-establishment-hold-time 50;
            backup-liveness-detection {
                backup-peer-ip 10.207.64.233;
            }
            liveness-detection {
                minimum-receive-interval 60;
                transmit-interval {
                    minimum-interval 60;
                }
            }
        }
    }
    rstp {
        interface ae0.0 {
            disable;
        }
        interface ae1.0 {
            edge;
        }
        interface all {
            mode point-to-point;
        }
        bpdu-block-on-edge;
    }
}
multi-chassis {
    multi-chassis-protection 3.3.3.1 {
        interface ae0;
    }
}
vlans {
    v100 {
        vlan-id 100;
        l3-interface vlan.100;
        mcae-mac-synchronize;
    }
    v500 {
        vlan-id 500;
        l3-interface vlan.500;
```

```
    }
}
```

Display the results of the configuration on Switch B.

```
chassis {
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}
interfaces {
    xe-0/0/12 {
        ether-options {
            802.3ad ae0;
        }
    }
    xe-0/0/13 {
        ether-options {
            802.3ad ae0;
        }
    }
    xe-0/0/46 {
        ether-options {
            802.3ad ae1;
        }
    }
    ae0 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members v500;
                }
            }
        }
    }
    ae1 {
        aggregated-ether-options {
            lacp {
                active;
                system-id 00:01:02:03:04:05;
                admin-key 3;
            }
            mc-ae {
                mc-ae-id 3;
                chassis-id 1;
                mode active-active;
                status-control standby;
                init-delay-time 240
            }
        }
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
```

```
            vlan {
               members v100;
            }
         }
      }
   }
   vlan {
      unit 100 {
         family inet {
            address 100.1.1.10/32;
         }
      }
      unit 500 {
         family inet {
            address 3.3.3.1/24;
         }
      }
   }
}
protocols {
   iccp {
      local-ip-addr 3.3.3.1;
      peer 3.3.3.2 {
         session-establishment-hold-time 50;
         backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
         }
         liveness-detection {
            minimum-receive-interval 60;
            transmit-interval {
               minimum-interval 60;
            }
         }
      }
   }
   rstp {
      interface ae0.0 {
         disable;
      }
      interface ae1.0 {
         edge;
      }
      interface all {
         mode point-to-point;
      }
      bpdu-block-on-edge;
   }
}
multi-chassis {
   multi-chassis-protection 3.3.3.2 {
      interface ae0;
   }
}
vlans {
   v100 {
      vlan-id 100;
```



```
        l3-interface vlan.100;
        mcae-mac-synchronize;
      }
      v500 {
        vlan-id 500;
        l3-interface vlan.500;
      }
    }
```

Verification

To verify that the MC-LAG group has been created and is working properly, perform these tasks:

Verifying That ICCP Is Working on Switch A

Purpose Verify that ICCP is running on Switch A.

Action

```
[edit]
user@switch# show iccp
Redundancy Group Information for peer 3.3.3.1
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That ICCP Is Working on Switch B

Purpose Verify that ICCP is running on Switch B.

Action **show iccp**

```
[edit]
user@switch# show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD
```



```
Client Application: eswd
```

Meaning This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That LACP Is Active on Switch A

Purpose Verify that LACP is active on Switch A.

Action

```
[edit]
user@switch# show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/46      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/46    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/46                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch A is participating in LACP negotiation.

Verifying That LACP Is Active on Switch B

Purpose Verify that LACP is active on Switch B

Action

```
[edit]
user@switch# show lacp interfaces

Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/44      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/44    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/44                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch B is participating in LACP negotiation.

Verifying That the MC-AE and ICL-PL Interfaces Are Up on Switch A

Purpose Verify that the MC-AE and ICL-PL interfaces are up on Switch A.

Action

```
[edit]
user@switch# 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        : 3.3.3.1 ae0.0 up
```

Meaning This output shows that the MC-AE interface on Switch A is up and active.

Verifying That the MC-AE and ICL-PL Interfaces Are Up on Switch B

Purpose Verify that the MC-AE and ICL-PL interfaces are up on Switch B.

Action

```
[edit]
user@switch# 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        : 3.3.3.2 ae0.0 up
```

Meaning This output shows that the MC-AE interface on Switch B is up and active.

Verifying MAC Address Synchronization on Switch A and Switch B

Purpose Confirm that MAC address synchronization is working on both Switch A and Switch B.

Action

```
[edit]
user@switch# show ethernet-switching table vlan v100
Ethernet-switching table: 3 unicast entries
  VLAN              MAC address       Type         Age Interfaces
  v100               *                 Flood          - All-members
  v100               84:18:88:df:35:36 Static         - Router
  v100               84:18:88:df:83:0a Static         - Router
```

Meaning The output shows two static MAC addresses in VLAN v100. The addresses belong to the Layer 3 IRB/RVI interfaces of both Switch A and Switch B that you configured in the MC-LAG VLAN. Appearance of both addresses indicates that MAC address synchronization is working.

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**

Solution Check the following:

- Verify that there is no configuration mismatch.
- Verify that all member ports are up.
- Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
- Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on page 35
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on page 235
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on page 235

Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP

Supported Platforms EX4600, QFX Series standalone switches

There are two methods for enabling Layer 3 unicast functionality across a multichassis link aggregation group (MC-LAG) to control traffic flow. You can choose either to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG, or you can configure Virtual Router Redundancy Protocol (VRRP), but you cannot configure both at the same time. Because RVI interfaces share the same MAC address, if you enable MAC address synchronization, packets received on an MC-LAG peer with a destination MAC address that is the same as that of the peer's IRB MAC address will not be forwarded. The procedure to configure the VRRP for use in a Layer 3 unicast MC-LAG is included in this example. For more information about configuring MAC address synchronization, see "Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast using MAC Address Synchronization" on page 193.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.3 or later for the QFX Series
- Two QFX3500 or QFX3600 or QFX5100 switches

Before you configure an MC-LAG, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch*.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch*.
- Configure Virtual Router Redundancy Protocol (VRRP) on a switch. See *Configuring Basic VRRP Support*.

Overview

In this example, you configure an MC-LAG across two switches by including interfaces from both switches in an aggregated Ethernet interface (ae1). To support the MC-LAG, create a second aggregated Ethernet interface (ae0) for the interchassis control link-protection link (ICL-PL). Configure a multichassis protection link for the ICL-PL, the Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the configuration, enable VRRP by completing the following steps:

- Create a routed VLAN interface (RVI)
- Create a VRRP group and assign a virtual IP address that is shared between each switch in the VRRP group
- Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group
- Configure Layer 3 connectivity between the VRRP groups

Topology

The topology used in this example consists of two switches hosting an MC-LAGs. The two switches are connected to a server. Figure 25 on page 153 shows the topology of this example.

Figure 28: Configuring a Multichassis LAG Between Switch A and Switch B

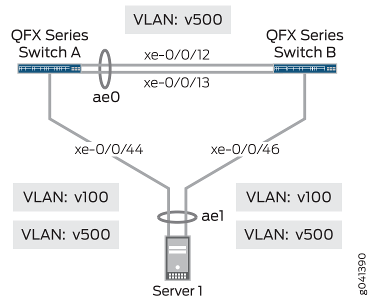


Table 8 on page 41 details the topology used in this configuration example.

Table 14: Components of the Topology for Configuring a Multichassis LAG Between Two Switches

Hostname	Base Hardware	Multichassis Link Aggregation Group
Switch A Switch B	QFX3500, QFX3600, or QFX5100 switch	ae0 is configured as an aggregated Ethernet interface, and is used as an ICL-PL. The following interfaces are part of ae0: xe-0/0/12 and xe-0/0/13 Switch A and xe-0/0/12 and xe-0/0/13 on Switch B. ae1 is configured as an MC-LAG, and the following two interfaces are part of ae1: xe-0/0/44 on Switch A and xe-0/0/46 on Switch B. .

Configuration

CLI Quick Configuration

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

NOTE: This example shows how to configure MC-LAG using both the original CLI and Enhanced Layer 2 Software (ELS).

In ELS, there are three different statements and one different option from the original CLI:

- The **port-mode** statement in the **[edit interfaces *interface-name* unit *number* family ethernet-switching]** hierarchy is not supported. Use the **interface-mode** statement instead.
- The **vlan** statement in the **[edit interfaces *interface-name*]** hierarchy is not supported. Use the **irb** statement instead.
- The **vlan.*logical-interface-number*** option in the **[edit vlans *vlan-name* l3-interface]** option is not supported. Use the **irb.*logical-interface-number*** option instead.
- The **service-id** statement in the **[edit switch-options]** hierarchy is required in the ELS CLI.

Switch A—Original CLI:

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500 v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200
set interfaces vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data
set interfaces vlan unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
```

```
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch A—ELS

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500 v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200
set interfaces irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
set switch-options service-id 10
```

Switch B—Original CLI:

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500 v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1 priority 150
set interfaces vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1 accept-data
set interfaces vlan unit 500 family inet address 3.3.3.1/24
```



```
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Switch B—ELS:

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500 v100
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 virtual-address 100.1.1.1
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 priority 150
set interfaces irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 accept-data
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
set switch-options service-id 10
```


Configuring MC-LAG on Two Switches

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable multichassis protection link between MC-LAG peers:

1. Configure the number of LAGs on both Switch A and Switch B.

   ```
   [edit chassis]
     user@switch# set aggregated-devices ethernet device-count 2
   ```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit interfaces]
     user@switch# set xe-0/0/12 ether-options 802.3ad ae0
   [edit interfaces]
     user@switch# set xe-0/0/13 ether-options 802.3ad ae0
   ```

   Switch A:

   ```
   [edit interfaces]
     user@switch# set xe-0/0/44 ether-options 802.3ad ae1
   ```

   Switch B:

   ```
   [edit interfaces]
     user@switch# set xe-0/0/46 ether-options 802.3ad ae1
   ```

3. Configure a trunk interface between Switch A and Switch B using the original CLI.

   ```
   [edit interfaces]
     user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk
   ```

4. Configure a trunk interface between Switch A and Switch B using ELS.

   ```
   [edit interfaces]
     user@switch# set ae0 unit 0 family ethernet-switching interface-mode trunk
   ```

5. Configure a multichassis protection link between Switch A and Switch B.

   Switch A:

   ```
   [edit]
     user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
   ```

   Switch B:

   ```
   [edit]
     user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
   ```


Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable ICCP:

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address and minimum receive interval for a Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval
     1000
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
     1000
   ```

3. Configure the peer IP address and minimum transmit interval for a BFD session for ICCP on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
     minimum-interval 1000
   ```

   Switch B:

   ```
   [edit protocols]
     user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
     minimum-interval 1000
   ```

4. (Optional) Configure the time during which an ICCP connection must succeed between MC-LAG peers on Switch A and Switch B.

   NOTE: Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

Switch A:

[edit protocols]
user@switch# **set** iccp peer **3.3.3.1** session-establishment-hold-time **50**

Switch B:

[edit protocols]
user@switch# **set** iccp peer **3.3.3.2** session-establishment-hold-time **50**

5. (Optional) Configure the backup IP address to be used for backup liveness detection on both Switch A and Switch B.

   NOTE: By default, backup liveness detection is not enabled. Configuring a backup IP address helps achieve sub-second traffic loss during an MC-LAG peer reboot.

   Switch A:

   [edit protocols]
   user@switch# **set** iccp peer **3.3.3.1** backup-liveness-detection backup-peer-ip **10.207.64.233**

   Switch B:

   [edit protocols]
   user@switch# **set** iccp peer **3.3.3.2** backup-liveness-detection backup-peer-ip **10.207.64.234**

6. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B using the original CLI.

   [edit vlans]
   user@switch# **set v500 vlan-id 500**

   [edit vlans]
   user@switch# **set v500 l3-interface vlan.500**

   [edit interfaces]
   user@switch# **set ae0 unit 0 family ethernet-switching port-mode trunk vlan members v500 v100**

7. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B using ELS.

   edit vlans]
   user@switch# **set v500 vlan-id 500**

   [edit vlans]
   user@switch# **set v500 l3-interface irb.500**

   [edit interfaces]
   user@switch# **set ae0 unit 0 family ethernet-switching interface-mode trunk vlan members v500 v100**

Step-by-Step Procedure

To enable the MC-LAG interface:

1. Enable LACP on the MC-LAG interface on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options lacp active**

2. Specify the same multichassis aggregated Ethernet identification number on both MC-LAG peers on Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae mc-ae-id 3**

3. Specify the same service ID on Switch A and Switch B.

   ELS:

   [edit]
   user@switch# **set switch-options service-id 10**

4. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae chassis-id 0**

   Switch B:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae chassis-id 1**

5. Specify the operating mode of the MC-LAG on both Switch A and Switch B.

   NOTE: Only active-active mode is supported at this time.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae mode active-active**

6. Specify the status control for MC-LAG on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAG. If one peer is in active mode, the other must be in standby mode.

Switch A:

[edit interfaces]
user@switch# **set ae1 aggregated-ether-options mc-ae status-control active**

Switch B:

[edit interfaces]
user@switch# **set ae1 aggregated-ether-options mc-ae status-control standby**

7. Specify the number of seconds by which the bring-up of the multichassis aggregated Ethernet interface should be deferred after you reboot Switch A and Switch B.

NOTE: The recommended value for maximum VLAN configuration (for example, 4,000 VLANS) is 240 seconds. If IGMP snooping is enabled on all of the VLANs, the recommended value is 420 seconds.

[edit interfaces]
user@switch# **set ae1 aggregated-ether-options mc-ae init-delay-time 240**

8. Specify the same LACP system ID for the MC-LAG on Switch A and Switch B.

[edit interfaces]
user@switch# **set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05**

9. Specify the same LACP administration key on both Switch A and Switch B.

[edit interfaces]
user@switch# **set ae1 aggregated-ether-options lacp admin-key 3**

10. Enable a VLAN on the MC-LAG on Switch A and Switch B using the original CLI.

[edit interfaces]
user@switch# **set ae1 unit 0 family ethernet-switching port-mode trunk**

[edit]
user@switch# **set vlans v100 vlan-id 100**

[edit interfaces]
user@switch# **set ae1 unit 0 family ethernet-switching vlan members v100**

11. Enable a VLAN on the MC-LAG on Switch A and Switch B using ELS.

[edit interfaces]
user@switch# **set ae1 unit 0 family ethernet-switching interface-mode trunk**

[edit]
user@switch# **set vlans v100 vlan-id 100**

[edit interfaces]
user@switch# **set ae1 unit 0 family ethernet-switching vlan members v100**

12. Enable VRRP on the MC-LAG on Switch A and Switch B:

- Create a routed VLAN interface (RVI), assign a virtual IP address that is shared between each switch in the VRRP group, and assign an individual IP address for each switch in the VRRP group:

Switch A:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1
  virtual-address 100.1.1.1
```

Switch B:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1
  virtual-address 100.1.1.1
```

- Assign the priority for each switch in the VRRP group:

NOTE: The switch configured with the highest priority is the master.

Switch A:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1
  priority 200
```

Switch B:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1
  priority 150
```

- Enable the switch to accept all packets destined for the virtual IP address if it is the master in the VRRP group:

Switch A:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1
  accept-data
```

Switch B:

```
[edit interfaces]
  user@switch# set vlan unit 100 family inet address 100.1.1.10/24 vrrp-group 1
  accept-data
```

- Configure Layer 3 connectivity between Switch A and Switch B.

```
[edit interfaces]
  user@switch# set vlans v100 l3-interface vlan.100
```

13. Enable VRRP on the MC-LAG on Switch A and Switch B using ELS:

- Create a routed VLAN interface (RVI), assign a virtual IP address that is shared between each switch in the VRRP group, and assign an individual IP address for each switch in the VRRP group:

Switch A:

```
[edit interfaces]
```

user@switch# **set irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1**

Switch B:

[edit interfaces]
user@switch# **set irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 virtual-address 100.1.1.1**

- Assign the priority for each switch in the VRRP group:

NOTE: The switch configured with the highest priority is the master.

Switch A:

[edit interfaces]
user@switch# **set irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200**

Switch B:

[edit interfaces]
user@switch# **set irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 priority 150**

- Enable the switch to accept all packets destined for the virtual IP address if it is the master in the VRRP group:

Switch A:

[edit interfaces]
user@switch# **set irb unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data**

Switch B:

[edit interfaces]
user@switch# **set irb unit 100 family inet address 100.1.1.10/24 vrrp-group 1 accept-data**

- Configure Layer 3 connectivity between Switch A and Switch B.

[edit interfaces]
user@switch# **set irb v100 l3-interface irb.100**

Step-by-Step Procedure

To enabled RSTP:

1. Enable RSTP globally on all interfaces on Switch A and Switch B.

NOTE: The all option is not available on ELS, so you cannot issue this command on ELS.


```
[edit]
  user@switch# set protocols rstp interface all mode point-to-point
```

ELS:

```
[edit]
  user@switch# set protocols rstp interface ae1.0 mode point-to-point
```

2. Disable RSTP on the ICL-PL interfaces on Switch A and Switch B.

   NOTE: This command is not needed on ELS.

   ```
   [edit]
     user@switch# set protocols rstp interface ae0.0 disable
   ```

3. Configure the MC-LAG interfaces as edge ports on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
     user@switch# set protocols rstp interface ae1.0 edge
   ```

4. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on Switch A and Switch B.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
     user@switch# set protocols rstp bpdu-block-on-edge
   ```

Results

From configuration mode , confirm your configuration by entering the **show chassis**, **show interfaces**, **show protocols**, **show multi-chassis**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Switch A—Original CLI

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchA# show interfaces
  interfaces {
    xe-0/0/12 {
      ether-options {
        802.3ad ae0;
      }
    }
    xe-0/0/13 {
      ether-options {
        802.3ad ae0;
      }
    }
    xe-0/0/44 {
      ether-options {
        802.3ad ae1;
      }
    }
    ae0 {
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members v500;
          }
        }
      }
    }
    ae1 {
      aggregated-ether-options {
        lacp {
          active;
          system-id 00:01:02:03:04:05;
          admin-key 3;
        }
        mc-ae {
          mc-ae-id 3;
          chassis-id 0;
          mode active-active;
          status-control active;
          init-delay-time 240;
        }
      }
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members v100;
          }
        }
      }
    }
    vlan {
      unit 100 {
        family inet {
          address 100.1.1.11/24 {
            vrrp-group 1 {
```



```
                    virtual-address 100.1.1.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 500 {
        family inet {
            address 3.3.3.2/24;
        }
    }
  }
}
```

user@SwitchA# **show protocols**

```
iccp {
    local-ip-addr 3.3.3.2;
    peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```

user@SwitchA# **show multi-chassis**

```
multi-chassis-protection 3.3.3.1 {
    interface ae0;
}
```

user@SwitchA# **show vlans**

```
v100 {
    vlan-id 100;
    l3-interface vlan.100;
}
v500 {
    vlan-id 500;
    l3-interface vlan.500;
```

```
}
```

Switch A—ELS

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchA# show interfaces
interfaces {
  xe-0/0/12 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/0/13 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/0/44 {
    ether-options {
      802.3ad ae1;
    }
  }
  ae0 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members v500;
        }
      }
    }
  }
  ae1 {
    aggregated-ether-options {
      lacp {
        active;
        system-id 00:01:02:03:04:05;
        admin-key 3;
      }
      mc-ae {
        mc-ae-id 3;
        chassis-id 0;
        mode active-active;
        status-control active;
        init-delay-time 240;
      }
    }
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
```



```
                members v100;
              }
            }
          }
        }
        vlan {
          unit 100 {
            family inet {
              address 100.1.1.11/24 {
                vrrp-group 1 {
                  virtual-address 100.1.1.1;
                  priority 200;
                  accept-data;
                }
              }
            }
          }
          unit 500 {
            family inet {
              address 3.3.3.2/24;
            }
          }
        }
      }
```

```
user@SwitchA# show protocols
iccp {
  local-ip-addr 3.3.3.2;
  peer 3.3.3.1 {
    session-establishment-hold-time 50;
    backup-liveness-detection {
      backup-peer-ip 10.207.64.233;
    }
    liveness-detection {
      minimum-receive-interval 1000;
      transmit-interval {
        minimum-interval 1000;
      }
    }
  }
}
rstp {
  interface ae1.0 {
    edge;
  }
  mode point-to-point;
  }
  bpdu-block-on-edge;
  }
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
  interface ae0;
}
```

```
user@SwitchA# show switch-options
service-id 10;
```

```
user@SwitchA# show vlans
v100 {
   vlan-id 100;
   l3-interface irb.100;
}
v500 {
   vlan-id 500;
   l3-interface irb.500;
}
```

Switch B—Original CLI

```
user@SwitchB# show chassis
aggregated-devices {
   ethernet {
      device-count 2;
   }
}

user@SwitchB# show interfaces
xe-0/0/12 {
   ether-options {
      802.3ad ae0;
   }
}
xe-0/0/13 {
   ether-options {
      802.3ad ae0;
   }
}
xe-0/0/44 {
   ether-options {
      802.3ad ae1;
   }
}
ae0 {
   unit 0 {
      family ethernet-switching {
         port-mode trunk;
         vlan {
            members v500;
         }
      }
   }
}
ae1 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:05;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 3;
         chassis-id 1;
         mode active-active;
         status-control active;
```



```
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 100 {
        family inet {
            address 100.1.1.10/24 {
                vrrp-group 1 {
                    virtual-address 100.1.1.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 500 {
        family inet {
            address 3.3.3.1/24;
        }
    }
}

user@SwitchB# show protocols
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface all {
        mode point-to-point;
```

```
  }
  bpdu-block-on-edge;
}
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
  interface ae0;
}
```

```
user@SwitchB# show vlans
v100 {
  vlan-id 100;
  l3-interface vlan.100;
}
v500 {
  vlan-id 500;
  l3-interface vlan.500;
}
```

Switch B—ELS

```
user@SwitchB# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@SwitchB# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/44 {
  ether-options {
    802.3ad ae1;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
      vlan {
        members v500;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
```



```
            active;
            system-id 00:01:02:03:04:05;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 3;
            chassis-id 1;
            mode active-active;
            status-control active;
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
vlan {
    unit 100 {
        family inet {
            address 100.1.1.10/24 {
                vrrp-group 1 {
                    virtual-address 100.1.1.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 500 {
        family inet {
            address 3.3.3.1/24;
        }
    }
}

user@SwitchB# show protocols
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
```

```
rstp {
  interface ae1.0 {
    edge;
  }
  mode point-to-point;
  }
  bpdu-block-on-edge;
  }
```

```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
  interface ae0;
}
```

```
user@SwitchB# show switch-options
service-id 10;
```

```
user@SwitchB# show vlans
v100 {
  vlan-id 100;
  l3-interface irb.100;
}
v500 {
  vlan-id 500;
  l3-interface irb.500;
}
```

Verification

Verify that the configuration is working properly.

Verifying That ICCP Is Working on Switch A

Purpose Verify that ICCP is running on Switch A.

Action

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.1
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning

This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That ICCP Is Working on Switch B

Purpose

Verify that ICCP is running on Switch B.

Action

show iccp

```
[edit]
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

 Client Application: MCSNOOPD

 Client Application: eswd
```

Meaning

This output shows that the TCP connection between the peers hosting the MC-LAG is up, liveness detection is up, and MCSNOOPD and ESWD client applications are running.

Verifying That LACP Is Active on Switch A

Purpose

Verify that LACP is active on Switch A.

Action

```
[edit]
user@switch> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/46      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/46    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/46                 Current   Fast periodic Collecting distributing
```

Meaning

This output shows that Switch A is participating in LACP negotiation.

Verifying That LACP Is Active on Switch B

Purpose

Verify that LACP is active on Switch B.

Action

```
[edit]
user@switch> show lacp interfaces

Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      xe-0/0/44      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      xe-0/0/44    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      xe-0/0/44                 Current   Fast periodic Collecting distributing
```

Meaning This output shows that Switch B is participating in LACP negotiation.

Verifying That the multichassis aggregated Ethernet and ICL-PL Interfaces Are Up on Switch A

Purpose Verify that the multichassis aggregated Ethernet and Inter-chassis Link Protection (ICL-PL) interfaces are up on Switch A.

Action

```
[edit]
user@switch> 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        : 3.3.3.1 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet and ICL-PL on Switch A is up and active.

Verifying That the Multichassis Aggregated Ethernet and ICL-PL Interfaces Are Up on Switch B

Purpose Verify that the multichassis aggregated Ethernet and ICL-PL interfaces are up on Switch B.

Action

```
[edit]
user@switch> 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        : 3.3.3.2 ae0.0 up
```

Meaning This output shows that the multichassis aggregated Ethernet and ICL-PL interface on Switch B is up and active.

Verifying that MAC Learning Is Occurring on Switch A

Purpose Verify that MAC learning is working on Switch A.

Action

```
[edit]
user@switch> show ethernet-switching table
Ethernet-switching table: 6 entries, 1 learned, 0 persistent entriesC
  VLAN              MAC address       Type         Age Interfaces
  v100              *                 Flood          - All-members
  v100              00:00:5e:00:01:01 Static         - Router
  v100              78:fe:3d:5a:07:42 Static         - Router
  v100              78:fe:3d:5b:ad:c2 Learn(R)        0 ae0.0
  v500              *                 Flood          - All-members
  v500              78:fe:3d:5a:07:42 Static         - Router
```

Meaning The output shows two static MAC address in VLAN v100 and one static MAC address in VLAN v500. These addresses belong to the Layer 3 RVI addresses on both Switch A and Switch B that you configured in the MC-LAG. The ICL-PL interface configured on the VRRP master member learned the VLAN v100 Learn (R) MAC address of the VRRP backup member.

Verifying that MAC Learning Is Occurring on Switch B

Purpose Verify that MAC learning is working on Switch B.

Action

```
[edit]
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 1 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v100              *                 Flood          - All-members
  v100              00:00:5e:00:01:01 Static         - Router
  v100              78:fe:3d:5a:07:42 Learn(R)       0 ae0.0
  v100              78:fe:3d:5b:ad:c2 Static         - Router
  v200              78:fe:3d:5b:ad:c2 Static         - Router
  v500              *                 Flood          - All-members
  v500              78:fe:3d:5b:ad:c2 Static         - Router
```

Meaning

The output shows two static MAC address in VLAN v100 and one static MAC address in VLAN v500. These addresses belong to the Layer 3 RVI addresses on both Switch A and Switch B that you configured in the MC-LAG. The ICL-PL interface configured on the VRRP backup member learned the VLAN v100 Learn (R) MAC address of the VRRP master member.

Verifying that Switch A is the Master in the VRRP Group

Purpose

Verify that Switch A is the master member in the VRRP group.

Action

```
[edit]
user@switch> show vrrp
Interface     State       Group   VR state VR Mode    Timer     Type   Address
vlan.100      up             1   master    Active      A  0.605 lcl     100.1.1.11

                                                                vip     100.1.1.1
```

Meaning

The output shows that Switch A is the master member in the VRRP group.

Verifying that Switch B is the Backup Member in the VRRP Group

Purpose

Verify that Switch B is the backup member in the VRRP group.

Action

```
[edit]
user@switch> show vrrp
Interface     State       Group   VR state VR Mode    Timer     Type   Address
vlan.100      up             1   backup    Active      A  0.605 lcl     100.1.1.10

                                                                vip     100.1.1.1
```

Meaning

The output shows that Switch B is the backup member in the VRRP group.

Verifying that the Virtual IP Address is Attached to an Individual Address on Switch A

Action

```
[edit]
user@switch# run show interfaces terse vlan
Interface               Admin Link Proto    Local                 Remote
vlan                    up    up
vlan.100                up    up   inet     100.1.1.1/24
                                            100.1.1.11/24
vlan.500                up    up   inet     3.3.3.2/24
```

Meaning The output shows that the virtual IP address (100.1.1.1/24) is bound to the individual IP address (100.1.1.11/24) on Switch A.

Verifying that the Virtual IP Address is Attached to an Individual Address on Switch B

Action

```
[edit]
user@switch# run show interfaces terse vlan
Interface               Admin Link Proto    Local                 Remote
vlan                    up    up
vlan.100                up    up   inet     100.1.1.1/24
                                            100.1.1.10/24
vlan.500                up    up   inet     3.3.3.1/24
```

Meaning The output shows that the virtual IP address (100.1.1.1/24) is bound to the individual IP address (100.1.1.10/24) on Switch B.

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**.

Solution Check the following:

1. Verify that there is no configuration mismatch.
2. Verify that all member ports are up.
3. Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
4. Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on page 35

Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP

Supported Platforms EX4600, QFX Series standalone switches

NOTE: Multichassis Link Aggregation (MC-LAG) is supported on QFX3500 and QFX3600 standalone switches running the original CLI and QFX5100 standalone switches running Enhanced Layer 2 Software (ELS).

There are two methods for enabling Layer 3 multicast functionality across a multichassis link aggregation group (MC-LAG) to control traffic. You can choose either to synchronize the MAC addresses for the Layer 3 interfaces of the switches participating in the MC-LAG, or you can configure Virtual Router Redundancy Protocol (VRRP), but you cannot configure both at the same time. Because RVI interfaces share the same MAC address, if you enable MAC address synchronization, packets received on an MC-LAG peer with a destination MAC address that is the same as that of the peer's IRB MAC address will not be forwarded. The procedure to configure VRRP for use in a Layer 3 multicast MC-LAG is included in this example.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.3 or later for the QFX3500 and QFX3600 standalone switches and Junos OS Release 13.2X51-D10 or later for the QFX5100 standalone switches.
- Two QFX3500 or QFX3600 standalone switches, or two QFX5100 standalone switches.

Before you configure an MC-LAG for Layer 3 multicast using VRRP, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch*.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a switch. See *Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch*.

Overview

In this example, you configure two MC-LAGs across two switches, consisting of two aggregated Ethernet interfaces (ae1 and ae2). To support the MC-LAG, create a third aggregated Ethernet interface (ae0) for the interchassis control link-protection link (ICL-PL). Configure a multichassis protection link for the ICL-PL, the Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the configuration, enable VRRP by completing the following steps for each MC-LAG:

1. Create a routed VLAN interface (RVI).
2. Create a VRRP group and assign a virtual IP address that is shared between each switch in the VRRP group.
3. Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group.
4. Configure Layer 3 connectivity between the VRRP groups.

Topology

The topology used in this example consists of two switches hosting two MC-LAGs—ae1 and ae2. The two switches are connected to a multicast source (Server 1) over the MC-LAG ae1, and a multicast receiver (Server 2) over the MC-LAG ae2. Figure 24 on page 132 shows the topology of this example.

Figure 29: Configuring a Multichassis LAG for Layer 3 Multicast Using VRRP

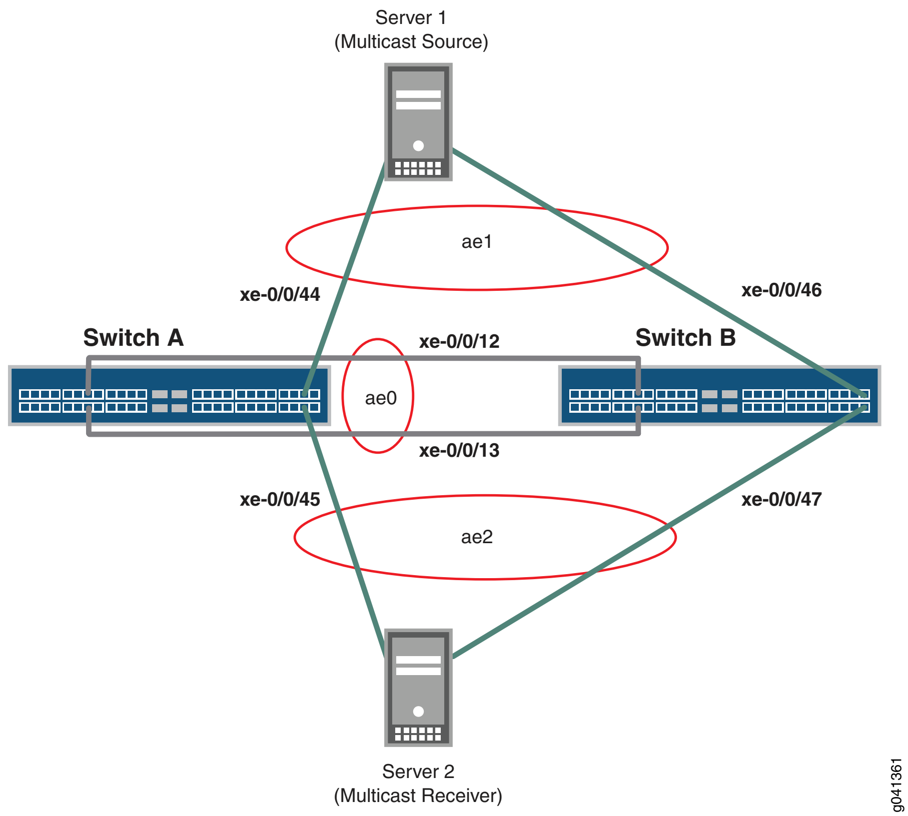


Table 10 on page 133 details the topology used in this configuration example.

Table 15: Components of the Topology for Configuring a Multichassis LAG for Layer 3 Multicast Using VRRP

Hostname	Base Hardware	Multichassis Link Aggregation Group
Switch A Switch B	QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch QFX3500 or QFX3600 standalone switch, or QFX5100 standalone switch	• ae0 is configured as an aggregated Ethernet interface, and is used as an ICL-PL. The following two interfaces are part of ae0: xe-0/0/12 and xe-0/0/13 on Switch A and xe-0/0/12 and xe-0/0/13 on Switch B. • ae1 is configured as an MC-LAG for the multicast source (Server 1), and the following two interfaces are part of ae1: xe-0/0/44 on Switch A and xe-0/0/46 on Switch B. • ae2 is configured as an MC-LAG for the multicast receiver (Server 2), and the following two interfaces are part of ae2: xe-0/0/45 on Switch A and xe-0/0/47 on Switch B.

Configuration

CLI Quick Configuration

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

NOTE: This example shows how to configure MC-LAG using both the original CLI and Enhanced Layer 2 Software (ELS).

In ELS, there are three different statements and one different option from the original CLI:

- The **port-mode** statement in the **[edit interfaces *interface-name* unit *number* family ethernet-switching]** hierarchy is not supported. Use the **interface-mode** statement instead.
- The **vlan** statement in the **[edit interfaces *interface-name*]** hierarchy is not supported. Use the **irb** statement instead.
- The **vlan.*logical-interface-number*** hierarchy in the **[edit vlans *vlan-name* l3-interface]** option is not supported. Use the **irb.*logical-interface-number*** option instead.
- The **service-id** statement in the **[edit switch-options]** hierarchy is required in the ELS CLI.

Switch A—Original CLI

```
set chassis aggregated-devices ethernet device-count 3
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces xe-0/0/45 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control active
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching port-mode trunk
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority 200
set interfaces vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data
set interfaces vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority 200
set interfaces vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2 accept-data
set interfaces vlan unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface vlan.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval
  1000
set protocols igmp-snooping vlan all
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  threshold 500
```

```
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface vlan.100 priority 200
set protocols pim interface vlan.100 dual-dr
set protocols pim interface vlan.100 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval threshold
  500
set protocols pim interface vlan.200 priority 600
set protocols pim interface vlan.200 dual-dr
set protocols pim interface vlan.200 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval threshold
  500
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae2.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
```

Switch A—ELS

```
set chassis aggregated-devices ethernet device-count 3
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/44 ether-options 802.3ad ae1
set interfaces xe-0/0/45 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control active
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching interface-mode trunk
```



```
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority 200
set interfaces irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority 200
set interfaces irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 accept-data
set interfaces irb unit 500 family inet address 3.3.3.2/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface irb.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.2
set protocols iccp peer 3.3.3.1 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip 10.207.64.233
set protocols iccp peer 3.3.3.1 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.1 liveness-detection transmit-interval minimum-interval
  1000
set protocols igmp-snooping vlan all
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  threshold 500
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface vlan.100 priority 200
set protocols pim interface vlan.100 dual-dr
set protocols pim interface vlan.100 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval threshold
  500
set protocols pim interface vlan.200 priority 600
set protocols pim interface vlan.200 dual-dr
set protocols pim interface vlan.200 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval threshold
  500
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae2.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
```

```
set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
set switch-options service-id 10
```

Switch B—Original CLI:

```
set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces xe-0/0/47 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control active
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching port-mode trunk
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority 150
set interfaces vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 accept-data
set interfaces vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority 150
set interfaces vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 accept-data
set interfaces vlan unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface vlan.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface vlan.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface vlan.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval
  1000
set protocols igmp-snooping vlan all
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
```


set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval threshold 500
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface vlan.100 priority 100
set protocols pim interface vlan.100 dual-dr
set protocols pim interface vlan.100 bfd-liveness-detection minimum-receive-interval 700
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval minimum-interval 350
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval threshold 500
set protocols pim interface vlan.200 priority 500
set protocols pim interface vlan.200 dual-dr
set protocols pim interface vlan.200 bfd-liveness-detection minimum-receive-interval 700
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval minimum-interval 350
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval threshold 500
set protocols rstp interface ae0.0 disable
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae2.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0

Switch B—ELS:

set chassis aggregated-devices ethernet device-count 2
set interfaces xe-0/0/12 ether-options 802.3ad ae0
set interfaces xe-0/0/13 ether-options 802.3ad ae0
set interfaces xe-0/0/46 ether-options 802.3ad ae1
set interfaces xe-0/0/47 ether-options 802.3ad ae2
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members v500
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-id 00:01:02:03:04:05
set interfaces ae1 aggregated-ether-options lacp admin-key 3
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 3
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control standby
set ae1 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae1 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae1 unit 0 family ethernet-switching vlan members v100
set interfaces ae2 aggregated-ether-options lacp active
set interfaces ae2 aggregated-ether-options lacp system-id 00:01:02:03:04:06
set interfaces ae2 aggregated-ether-options lacp admin-key 3
set interfaces ae2 aggregated-ether-options mc-ae mc-ae-id 4
set interfaces ae2 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae2 aggregated-ether-options mc-ae mode active-active
set interfaces ae2 aggregated-ether-options mc-ae status-control active

```
set interfaces ae2 aggregated-ether-options mc-ae init-delay-time 240
set interfaces ae2 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae2 unit 0 family ethernet-switching vlan members v200
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 virtual-address
  10.1.1.1
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority 150
set interfaces irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 accept-data
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 virtual-address
  10.1.1.2
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority 150
set interfaces irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 accept-data
set interfaces irb unit 500 family inet address 3.3.3.1/24
set vlans v100 vlan-id 100
set vlans v100 l3-interface irb.100
set vlans v200 vlan-id 200
set vlans v200 l3-interface irb.200
set vlans v500 vlan-id 500
set vlans v500 l3-interface irb.500
set protocols iccp local-ip-addr 3.3.3.1
set protocols iccp peer 3.3.3.2 session-establishment-hold-time 50
set protocols iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip 10.207.64.234
set protocols iccp peer 3.3.3.2 liveness-detection minimum-receive-interval 1000
set protocols iccp peer 3.3.3.2 liveness-detection transmit-interval minimum-interval
  1000
set protocols igmp-snooping vlan all
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.100 bfd-liveness-detection transmit-interval
  threshold 500
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols ospf area 0.0.0.0 interface vlan.200 bfd-liveness-detection transmit-interval
  threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface vlan.100 priority 100
set protocols pim interface vlan.100 dual-dr
set protocols pim interface vlan.100 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.100 bfd-liveness-detection transmit-interval threshold
  500
set protocols pim interface vlan.200 priority 500
set protocols pim interface vlan.200 dual-dr
set protocols pim interface vlan.200 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface vlan.200 bfd-liveness-detection transmit-interval threshold
  500
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae2.0 edge
```

```
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
set switch-options service-id 10
```

Configuring MC-LAG for Layer 3 Multicast Using VRRP on Two Switches

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To enable multichassis protection link between MC-LAG peers:

1. Configure the number of LAGs on both Switch A and Switch B.

   ```
   [edit chassis]
   user@switch# set aggregated-devices ethernet device-count 3
   ```

2. Add member interfaces to the aggregated Ethernet interfaces on both Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/12 ether-options 802.3ad ae0
   user@switch# set xe-0/0/13 ether-options 802.3ad ae0
   ```

   Switch A:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/44 ether-options 802.3ad ae1
   user@switch# set xe-0/0/45 ether-options 802.3ad ae2
   ```

   Switch B:

   ```
   [edit interfaces]
   user@switch# set xe-0/0/46 ether-options 802.3ad ae1
   user@switch# set xe-0/0/47 ether-options 802.3ad ae2
   ```

3. Configure ae0 as the trunk interface between Switch A and Switch B.

   Switch A and Switch B:

   ```
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switching port-mode trunk
   ```

   Switch A and Switch B Using ELS:

   ```
   [edit interfaces]
   user@switch# set ae0 unit 0 family ethernet-switchinginterface-mode trunk
   ```

4. Configure ae0 as the multichassis protection link between Switch A and Switch B.

   Switch A:

   ```
   [edit]
   user@switch# set multi-chassis multi-chassis-protection 3.3.3.1 interface ae0
   ```

Switch B:

```
[edit]
user@switch# set multi-chassis multi-chassis-protection 3.3.3.2 interface ae0
```

Step-by-Step Procedure

To enable ICCP:

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the local IP address to be in the ICCP connection on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.2
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp local-ip-addr 3.3.3.1
   ```

2. Configure the peer IP address, minimum receive interval, and minimum transmit interval for a Bidirectional Forwarding Detection (BFD) session for ICCP on Switch A and Switch B.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 liveness-detection minimum-receive-interval
     1000
   user@switch# set iccp peer 3.3.3.1 liveness-detection transmit-interval
     minimum-interval 1000
   ```

   Switch B:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.2 liveness-detection minimum-receive-interval
     1000
   user@switch# set iccp peer 3.3.3.2 liveness-detection transmit-interval
     minimum-interval 1000
   ```

3. (Optional) Configure the time during which an ICCP connection must succeed between MC-LAG peers on Switch A and Switch B.

   NOTE: Configuring session establishment hold time helps to establish a faster ICCP connection . The recommended value is 50 seconds.

   Switch A:

   ```
   [edit protocols]
   user@switch# set iccp peer 3.3.3.1 session-establishment-hold-time 50
   ```


Switch B:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.2 session-establishment-hold-time 50
```

4. (Optional) Configure the backup IP address to be used for backup liveness detection on both Switch A and Switch B.

> NOTE: By default, backup liveness detection is not enabled. Configuring a backup IP address helps achieve sub-second traffic loss during an MC-LAG peer reboot.

Switch A:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.1 backup-liveness-detection backup-peer-ip
  10.207.64.233
```

Switch B:

```
[edit protocols]
user@switch# set iccp peer 3.3.3.2 backup-liveness-detection backup-peer-ip
  10.207.64.234
```

5. Configure Layer 3 connectivity between the MC-LAG peers on both Switch A and Switch B.

> NOTE: In ELS, use the irb.*logical-interface-number* instead.

Switch A and Switch B:

```
[edit vlans]
user@switch# set v500 vlan-id 500
user@switch# set v500 l3-interface vlan.500
```

Switch A and Switch B Using ELS:

```
[edit vlans]
user@switch# set v500 vlan-id 500
user@switch# set v500 l3-interface irb.500
```

Switch A and Switch B:

```
[edit interfaces]
user@switch# set ae0 unit 0 family ethernet-switching vlan members v500
```

Switch A:

```
[edit interfaces]
user@switch# set vlan unit 500 family inet address 3.3.3.2/24
```


Switch A Using ELS:

[edit interfaces]
user@switch# **set irbunit 500 family inet address 3.3.3.2/24**

Switch B:

[edit interfaces]
user@switch# **set vlan unit 500 family inet address 3.3.3.1/24**

Switch B Using ELS:

[edit interfaces]
user@switch# **set irb unit 500 family inet address 3.3.3.1/24**

Step-by-Step Procedure

To enable the ae1 and ae2 MC-LAG interfaces:

1. Enable LACP on the MC-LAG interfaces on Switch A and Switch B.

   NOTE: At least one end needs to be active. The other end can be either active or passive.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options lacp active**
   user@switch# **set ae2 aggregated-ether-options lacp active**

2. Specify the same multichassis aggregated Ethernet identification number for each MC-LAG peer on Switch A and Switch B.

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae mc-ae-id 3**
   user@switch# **set ae2 aggregated-ether-options mc-ae mc-ae-id 4**

3. Specify the same service ID on Switch A and Switch B.

   ELS:

   [edit]
   set switch-options service-id 10

4. Specify a unique chassis ID for the MC-LAG on the MC-LAG peers on Switch A and Switch B.

   Switch A:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae chassis-id 0**
   user@switch# **set ae2 aggregated-ether-options mc-ae chassis-id 0**

   Switch B:

   [edit interfaces]
   user@switch# **set ae1 aggregated-ether-options mc-ae chassis-id 1**
   user@switch# **set ae2 aggregated-ether-options mc-ae chassis-id 1**

5. Specify the operating mode of the MC-LAGs on both Switch A and Switch B.

NOTE: Only active-active mode is supported at this time.

```
[edit interfaces]
user@switch# set ae1 aggregated-ether-options mc-ae mode active-active
user@switch# set ae2 aggregated-ether-options mc-ae mode active-active
```

6. Specify the status control for the MC-LAGs on Switch A and Switch B.

   NOTE: You must configure status control on both Switch A and Switch B hosting the MC-LAGs. If one peer is in active mode, the other must be in standby mode.

   Switch A:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae status-control active
   user@switch# set ae2 aggregated-ether-options mc-ae status-control active
   ```

   Switch B:

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae status-control standby
   user@switch# set ae2 aggregated-ether-options mc-ae status-control standby
   ```

7. Specify the number of seconds by which the bring-up of the MC-LAG interfaces should be deferred after you reboot Switch A or Switch B.

   NOTE: The recommended value for maximum VLAN configuration (for example, 4,000 VLANS) is 240 seconds. If IGMP snooping is enabled on all of the VLANs, the recommended value is 420 seconds.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options mc-ae init-delay-time 420
   user@switch# set ae2 aggregated-ether-options mc-ae init-delay-time 420
   ```

8. Specify the same LACP system ID for each MC-LAG on Switch A and Switch B.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp system-ID 00:01:02:03:04:05
   user@switch# set ae2 aggregated-ether-options lacp system-ID 00:01:02:03:04:06
   ```

9. Specify the same LACP administration key on both Switch A and Switch B.

   ```
   [edit interfaces]
   user@switch# set ae1 aggregated-ether-options lacp admin-key 3
   user@switch# set ae2 aggregated-ether-options lacp admin-key 3
   ```

10. Enable a VLAN for each MC-LAG on Switch A and Switch B.

   ```
   [edit vlans]
   ```

```
user@switch# set v100 vlan-id 100
user@switch# set v200 vlan-id 200
```

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching vlan members v100
user@switch# set ae2 unit 0 family ethernet-switching vlan members v200
```

11. Configure ae1 and ae2 as trunk interfaces between Switch A and Switch B.

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching port-mode trunk
user@switch# set ae2 unit 0 family ethernet-switching port-mode trunk
```

ELS:

```
[edit interfaces]
user@switch# set ae1 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ae2 unit 0 family ethernet-switching interface-mode trunk
```

Step-by-Step Procedure

To enable VRRP on the MC-LAGs on Switch A and Switch B:

1. Create a routed VLAN interface (RVI) for each MC-LAG, assign a virtual IP address that is shared between each switch in the VRRP groups, and assign an individual IP address for each switch in the VRRP groups.

Switch A:

```
[edit interfaces]
user@switch# set vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  virtual-address 10.1.1.2
```

Switch A Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  virtual-address 10.1.1.2
```

Switch B:

```
[edit interfaces]
user@switch# set vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  virtual-address 10.1.1.2
```

Switch B Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  virtual-address 10.1.1.1
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  virtual-address 10.1.1.2
```

2. Assign the priority for each switch in the VRRP groups:

NOTE: The switch configured with the highest priority is the master.

Switch A:

```
[edit interfaces]
user@switch# set vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority
  200
user@switch# set vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority
  200
```

Switch A Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority
  200
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority
  200
```

Switch B:

```
[edit interfaces]
user@switch# set vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority
  150
user@switch# set vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority
  150
```

Switch B Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority
  150
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority
  150
```

3. Enable the switch to accept all packets destined for the virtual IP address if it is the master in a VRRP group:

Switch A:

```
[edit interfaces]
user@switch# set vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1
  accept-data
user@switch# set vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  accept-data
```

Switch A Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data
user@switch# set irb unit 200 family inet address 10.1.1.21/24 vrrp-group 2
  accept-data
```

Switch B:

```
[edit interfaces]
```



```
user@switch# set vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  accept-data
user@switch# set vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  accept-data
```

Switch B Using ELS:

```
[edit interfaces]
user@switch# set irb unit 100 family inet address 10.1.1.10/24 vrrp-group 1
  accept-data
user@switch# set irb unit 200 family inet address 10.1.1.20/24 vrrp-group 2
  accept-data
```

4. Configure Layer 3 connectivity between Switch A and Switch B.

```
[edit interfaces]
user@switch# set v100 l3-interface vlan.100
user@switch# set v200 l3-interface vlan.200
```

ELS:

```
[edit interfaces]
user@switch# set v100 l3-interface irb.100
user@switch# set v200 l3-interface irb.200
```

Step-by-Step Procedure

To enable IGMP snooping:

1. Enable IGMP snooping for all VLANs on Switch A and Switch B.

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

Step-by-Step Procedure

To configure OSPF as the Layer 3 protocol:

1. Configure an OSPF area on Switch A and Switch B.

```
[edit protocols ospf]
user@switch# set area 0.0.0.0
```

2. Assign the VLAN interfaces for the MC-LAGs as interfaces to the OSPF area on Switch A and Switch B.

```
[edit protocols ospf area 0.0.0.0]
user@switch# set interface vlan.100
user@switch# set interface vlan.200
```

3. Configure the minimum receive interval, minimum transmit interval, and transmit interval threshold for a Bidirectional Forwarding Detection (BFD) session for the OSPF interfaces on Switch A and Switch B.

NOTE: On a QFX5100 switch, the minimum transmit interval must be 1000 milliseconds or greater. Sub-second timers are not supported in Junos OS 13.2X51-D10 and later. If you configure the minimum transmit interval timer lower than 1000 milliseconds, the state of the MC-LAG can be affected.


```
[edit protocols ospf area 0.0.0.0]
user@switch# set interface vlan.100 bfd-liveness-detection
  minimum-receive-interval 700
user@switch# set interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface vlan.100 bfd-liveness-detection transmit-interval
  threshold 500
user@switch# set interface vlan.200 bfd-liveness-detection
  minimum-receive-interval 700
user@switch# set interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface vlan.200 bfd-liveness-detection transmit-interval
  threshold 500
```

Step-by-Step Procedure

To configure PIM as the multicast protocol:

1. Configure a static rendezvous point (RP) address on Switch A and Switch B.

   ```
   [edit protocols pim]
   user@switch# set rp static address 1.0.0.3
   ```

2. Configure the address ranges of the multicast groups for which Switch A and Switch B can be a rendezvous point (RP).

   ```
   [edit protocols pim rp static address 1.0.0.3]
   user@switch# set group-ranges 239.0.0.0/8
   ```

3. Enable PIM on the VLAN interfaces for the MC-LAGs on Switch A and Switch B.

   ```
   [edit protocols pim]
   user@switch# set interface vlan.100 dual-dr
   user@switch# set interface vlan.200 dual-dr
   ```

4. Configure each PIM interface's priority for being selected as the designated router (DR).

   An interface with a higher priority value has a higher probability of being selected as the DR.

   Switch A:

   ```
   [edit protocols pim]
   user@switch# set interface vlan.100 priority 200
   user@switch# set interface vlan.200 priority 600
   ```

   Switch B:

   ```
   [edit protocols pim]
   user@switch# set interface vlan.100 priority 100
   user@switch# set interface vlan.200 priority 500
   ```

5. Configure the minimum receive interval, minimum transmit interval, and transmit interval threshold for a Bidirectional Forwarding Detection (BFD) session for the PIM interfaces on Switch A and Switch B.

   ```
   [edit protocols pim]
   user@switch# set interface vlan.100 bfd-liveness-detection
     minimum-receive-interval 700
   ```

```
user@switch# set interface vlan.100 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface vlan.100 bfd-liveness-detection transmit-interval
  threshold 500
user@switch# set interface vlan.200 bfd-liveness-detection
  minimum-receive-interval 700
user@switch# set interface vlan.200 bfd-liveness-detection transmit-interval
  minimum-interval 350
user@switch# set interface vlan.200 bfd-liveness-detection transmit-interval
  threshold 500
```

Step-by-Step Procedure

To enable RSTP:

1. Enable RSTP on Switch A.

```
[edit protocols rstp]
user@switch# set interface ae1.0 mode point-to-point
```

2. Enable RSTP on Switch B.

```
[edit protocols rstp]
user@switch# set interface ae1.0 mode point-to-point
```

3. Disable RSTP on the ICL-PL interfaces on Switch A and Switch B.

NOTE: This command does not apply on ELS.

```
[edit protocols rstp]
user@switch# set interface ae0.0 disable
```

4. Configure the MC-LAG interfaces as edge ports on Switch A and Switch B.

NOTE: The ae1 and ae2 interfaces are downstream interfaces. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit protocols rstp]
user@switch# set interface ae1.0 edge
user@switch# set interface ae2.0 edge
```

5. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on Switch A and Switch B.

NOTE: The ae1 and ae2 interfaces are downstream interfaces. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit protocols rstp]
user@switch# set bpdu-block-on-edge
```

Results

From configuration mode on Switch A, confirm your configuration by entering the **show chassis**, **show interfaces**, **show multi-chassis**, **show protocols**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Switch A—Original CLI:

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 3;
  }
}

user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/44 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/45 {
  ether-options {
    802.3ad ae2;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members v500;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
      active;
      system-id 00:01:02:03:04:05;
      admin-key 3;
    }
    mc-ae {
```

```
            mc-ae-id 3;
            chassis-id 0;
            mode active-active;
            status-control active;
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
ae2 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:06;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 4;
            chassis-id 0;
            mode active-active;
            status-control active;
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members v200;
            }
        }
    }
}
vlan {
    unit 100 {
        family inet {
            address 10.1.1.11/24 {
                vrrp-group 1 {
                    virtual-address 10.1.1.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 200 {
        family inet {
            address 10.1.1.21/24 {
                vrrp-group 2 {
```



```
                virtual-address 10.1.1.2;
                priority 200;
                accept-data;
            }
        }
    }
  }
  unit 500 {
    family inet {
      address 3.3.3.2/24;
    }
  }
}
}

user@SwitchA# show protocols
ospf {
  area 0.0.0.0 {
    interface vlan.100 {
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
    interface vlan.200 {
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
  }
}
pim {
  rp {
    static {
      address 1.0.0.3 {
        group-ranges {
          239.0.0.0/8;
        }
      }
    }
  }
  interface vlan.100 {
    priority 200;
    dual-dr;
    bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
      minimum-receive-interval 700;
      transmit-interval {
        minimum-interval 350;
        threshold 500;
```

```
            }
        }
    }
    interface vlan.200 {
        priority 600;
        dual-dr;
        bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
            minimum-receive-interval 700;
            transmit-interval {
                minimum-interval 350;
                threshold 500;
            }
        }
    }
}
iccp {
    local-ip-addr 3.3.3.2;
    peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
igmp-snooping {
    vlan all;
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface ae2.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
    interface ae0;
}
```

```
user@SwitchA# show vlans
v100 {
    vlan-id 100;
```



```
    l3-interface vlan.100;
  }
  v200 {
    vlan-id 200;
    l3-interface vlan.200;
  }
  v500 {
    vlan-id 500;
    l3-interface vlan.500;
  }
```

Switch A—ELS

```
user@SwitchA# show chassis
aggregated-devices {
  ethernet {
    device-count 3;
  }
}

user@SwitchA# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/44 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/45 {
  ether-options {
    802.3ad ae2;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
      vlan {
        members v100;
      }
    }
  }
}
ae1 {
  aggregated-ether-options {
    lacp {
      active;
      system-id 00:01:02:03:04:05;
      admin-key 3;
```

```
      }
      mc-ae {
        mc-ae-id 3;
        chassis-id 0;
        mode active-active;
        status-control active;
        init-delay-time 240;
      }
    }
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members v100;
        }
      }
    }
  }
  ae2 {
    aggregated-ether-options {
      lacp {
        active;
        system-id 00:01:02:03:04:06;
        admin-key 3;
      }
      mc-ae {
        mc-ae-id 4;
        chassis-id 0;
        mode active-active;
        status-control active;
        init-delay-time 240;
      }
    }
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members v200;
        }
      }
    }
  }
  irb {
    unit 100 {
      family inet {
        address 10.1.1.11/24 {
          vrrp-group 1 {
            virtual-address 10.1.1.1;
            priority 200;
            accept-data;
          }
        }
      }
    }
    unit 200 {
      family inet {
```



```
            address 10.1.1.21/24 {
                vrrp-group 2 {
                    virtual-address 10.1.1.2;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 500 {
        family inet {
            address 3.3.3.2/24;
        }
    }
}
```

```
user@SwitchA# show protocols
ospf {
    area 0.0.0.0 {
        interface vlan.100 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
        interface vlan.200 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
    }
}
pim {
    rp {
        static {
            address 1.0.0.3 {
                group-ranges {
                    239.0.0.0/8;
                }
            }
        }
    }
    interface vlan.100 {
        priority 200;
        dual-dr;
        bfd-liveness-detection {
            minimum-receive-interval 700;
            transmit-interval {
                minimum-interval 350;
```

```
            threshold 500;
          }
        }
      }
      interface vlan.200 {
        priority 600;
        dual-dr;
        bfd-liveness-detection {
          minimum-receive-interval 700;
          transmit-interval {
            minimum-interval 350;
            threshold 500;
          }
        }
      }
    }
    iccp {
      local-ip-addr 3.3.3.2;
      peer 3.3.3.1 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
          backup-peer-ip 10.207.64.233;
        }
        liveness-detection {
          minimum-receive-interval 1000;
          transmit-interval {
            minimum-interval 1000;
          }
        }
      }
    }
    igmp-snooping {
      vlan all;
    }
    rstp {
      interface ae1.0 {
        edge;
      }
      interface ae2.0 {
        edge;
      }
      interface ae1.0{
        mode point-to-point;
      }
      bpdu-block-on-edge;
    }
```

```
user@SwitchA# show multi-chassis
multi-chassis-protection 3.3.3.1 {
  interface ae0;
}
```

```
user@SwitchA# show switch-options
service-id 10;
```

```
user@SwitchA# show vlans
v100 {
```



```
    vlan-id 100;
    l3-interface irb.100;
  }
  v200 {
    vlan-id 200;
    l3-interface irb.200;
  }
  v500 {
    vlan-id 500;
    l3-interfac irb.500;
  }
```

From configuration mode on Switch B, confirm your configuration by entering the **show chassis**, **show interfaces**, **show multi-chassis**, **show protocols**, and **show vlans** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Switch B--Original CLI

```
user@SwitchB# show chassis
aggregated-devices {
  ethernet {
    device-count 3;
  }
}

user@SwitchB# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/46 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/47 {
  ether-options {
    802.3ad ae2;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members v500;
      }
    }
  }
```

```
}
ae1 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:05;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 3;
         chassis-id 1;
         mode active-active;
         status-control standby;
      }
   }
   unit 0 {
      family ethernet-switching {
         port-mode trunk;
         vlan {
            members v100;
         }
      }
   }
}
ae2 {
   aggregated-ether-options {
      lacp {
         active;
         system-id 00:01:02:03:04:06;
         admin-key 3;
      }
      mc-ae {
         mc-ae-id 4;
         chassis-id 1;
         mode active-active;
         status-control active;
         init-delay-time 240;
      }
   }
   unit 0 {
      family ethernet-switching {
         port-mode trunk;
         vlan {
            members v200;
         }
      }
   }
}
irb {
   unit 100 {
      family inet {
         address 10.1.1.10/24 {
            vrrp-group 1 {
               virtual-address 10.1.1.1;
               priority 150;
               accept-data;
```



```
            }
          }
        }
      }
      unit 200 {
        family inet {
          address 10.1.1.20/24 {
            vrrp-group 2 {
              virtual-address 10.1.1.2;
              priority 150;
              accept-data;
            }
          }
        }
      }
      unit 500 {
        family inet {
          address 3.3.3.1/24;
        }
      }
    }
    }

    user@SwitchB# show protocols
    ospf {
      area 0.0.0.0 {
        interface vlan.100 {
          bfd-liveness-detection {
            minimum-receive-interval 700;
            transmit-interval {
              minimum-interval 350;
              threshold 500;
            }
          }
        }
        interface vlan.200 {
          bfd-liveness-detection {
            minimum-receive-interval 700;
            transmit-interval {
              minimum-interval 350;
              threshold 500;
            }
          }
        }
      }
    }
    pim {
      rp {
        static {
          address 1.0.0.3 {
            group-ranges {
              239.0.0.0/8;
            }
          }
        }
      }
```

```
    interface vlan.100 {
        priority 100;
        dual-dr;
        bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
            minimum-receive-interval 700;
            transmit-interval {
                minimum-interval 350;
                threshold 500;
            }
        }
    }
    interface vlan.200 {
        priority 500;
        dual-dr;
        bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
            minimum-receive-interval 700;
            transmit-interval {
                minimum-interval 350;
                threshold 500;
            }
        }
    }
}
iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
        session-establishment-hold-time 50;
        backup-liveness-detection {
            backup-peer-ip 10.207.64.234;
        }
        liveness-detection {
            minimum-receive-interval 1000;
            transmit-interval {
                minimum-interval 1000;
            }
        }
    }
}
igmp-snooping {
    vlan all;
}
rstp {
    interface ae0.0 {
        disable;
    }
    interface ae1.0 {
        edge;
    }
    interface ae2.0 {
        edge;
    }
    interface all {
        mode point-to-point;
    }
    bpdu-block-on-edge;
}
```



```
}
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
  interface ae0;
}
user@SwitchB# show vlans
v100 {
  vlan-id 100;
  l3-interface vlan.100;
}
v200 {
  vlan-id 200;
  l3-interface vlan.200;
}
v500 {
  vlan-id 500;
  l3-interface vlan.500;
}
```

Switch B—-ELS

```
user@SwitchB# show chassis
aggregated-devices {
  ethernet {
    device-count 3;
  }
}
user@SwitchB# show interfaces
xe-0/0/12 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/13 {
  ether-options {
    802.3ad ae0;
  }
}
xe-0/0/46 {
  ether-options {
    802.3ad ae1;
  }
}
xe-0/0/47 {
  ether-options {
    802.3ad ae2;
  }
}
ae0 {
  unit 0 {
    family ethernet-switching {
      interface-mode trunk;
      vlan {
        members v100;
```

```
            }
        }
    }
}
ae1 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:05;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 3;
            chassis-id 1;
            mode active-active;
            status-control standby;
        }
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v100;
            }
        }
    }
}
ae2 {
    aggregated-ether-options {
        lacp {
            active;
            system-id 00:01:02:03:04:06;
            admin-key 3;
        }
        mc-ae {
            mc-ae-id 4;
            chassis-id 1;
            mode active-active;
            status-control active;
            init-delay-time 240;
        }
    }
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members v200;
            }
        }
    }
}
irb {
    unit 100 {
        family inet {
            address 10.1.1.10/24 {
                vrrp-group 1 {
```



```
                virtual-address 10.1.1.1;
                priority 150;
                accept-data;
            }
        }
    }
}
unit 200 {
    family inet {
        address 10.1.1.20/24 {
            vrrp-group 2 {
                virtual-address 10.1.1.2;
                priority 150;
                accept-data;
            }
        }
    }
}
unit 500 {
    family inet {
        address 3.3.3.1/24;
    }
}
}
```

```
user@SwitchB# show protocols
ospf {
    area 0.0.0.0 {
        interface vlan.100 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
        interface vlan.200 {
            bfd-liveness-detection {
                minimum-receive-interval 700;
                transmit-interval {
                    minimum-interval 350;
                    threshold 500;
                }
            }
        }
    }
}
pim {
    rp {
        static {
            address 1.0.0.3 {
                group-ranges {
                    239.0.0.0/8;
                }
            }
```

```
      }
    }
    interface vlan.100 {
      priority 100;
      dual-dr;
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
    interface vlan.200 {
      priority 500;
      dual-dr;
      bfd-liveness-detection {
        minimum-receive-interval 700;
        transmit-interval {
          minimum-interval 350;
          threshold 500;
        }
      }
    }
  }
  iccp {
    local-ip-addr 3.3.3.1;
    peer 3.3.3.2 {
      session-establishment-hold-time 50;
      backup-liveness-detection {
        backup-peer-ip 10.207.64.234;
      }
      liveness-detection {
        minimum-receive-interval 1000;
        transmit-interval {
          minimum-interval 1000;
        }
      }
    }
  }
  igmp-snooping {
    vlan all;
  }
  rstp {
    interface ae1.0 {
      edge;
    }
    interface ae2.0 {
      edge;
    }
    interface ae1.0{
      mode point-to-point;
    }
    bpdu-block-on-edge;
  }
```



```
user@SwitchB# show multi-chassis
multi-chassis-protection 3.3.3.2 {
  interface ae0;
}
```

```
user@SwitchB# show switch-options
service-id 10;
```

```
user@SwitchB# show vlans
v100 {
  vlan-id 100;
  l3-interface irb.100;
}
v200 {
  vlan-id 200;
  l3-interface irb.200;
}
v500 {
  vlan-id 500;
  l3-interface irb.500;
}
```

Verification

Verify that the configuration is working properly.

- Verifying That Switch A is the Master Designated Router on page 271
- Verifying That Switch B is the Backup Designated Router on page 271

Verifying That Switch A is the Master Designated Router

Purpose Verify that Switch A is the master designated router (DR).

Action From operational mode, enter the **show pim interfaces** command.

```
user@switch> 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        Down S     4 2   P2P,NotCap       0 0/0
vlan.100          Up   S     4 2  DDR-DR,NotCap     1 0/0            10.1.1.11
vlan.200          Up   S     4 2  DDR-DR,NotCap     2 0/0            10.1.1.21
```

Meaning The DDR-DR state of the VLAN interfaces in the output shows that Switch A is the master designated router.

Verifying That Switch B is the Backup Designated Router

Purpose Verify that Switch B is the backup designated router (BDR).

Action From operational mode, enter the **show pim interfaces** command.

```
user@switch> 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         Down S     4 2  P2P,NotCap        0 0/0
vlan.100           Up   S     4 2  DDR-BDR,NotCap    1 0/0            10.1.1.11
vlan.200           Up   S     4 2  DDR-BDR,NotCap    2 0/0            10.1.1.21
```

Meaning The DDR-BDR state of the VLAN interfaces in the output shows that Switch B is the backup designated router.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Configuring Multichassis Link Aggregation on page 35

Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on MX Series Routers

Supported Platforms MX240, MX480, MX960

There are two methods for enabling Layer 3 multicast functionality across a multichassis link aggregation group (MC-LAG). You can choose either to configure the Virtual Router Redundancy Protocol (VRRP) or synchronize the MAC addresses for the Layer 3 interfaces of the routers participating in the MC-LAG to load balance the traffic. The procedure to configure VRRP for use in a Layer 3 multicast MC-LAG is included in this example.

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks MX Series routers
- Junos OS Release 11.2 or later running on all four routers

Before you configure an MC-LAG for Layer 3 multicast using VRRP, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a router.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a router.

- Configure the Virtual Router Redundancy Protocol (VRRP) on a router.

Overview

In this example, you configure an MC-LAG across two routers by including interfaces from both routers in an aggregated Ethernet interface (ae1). To support the MC-LAG, create a second aggregated Ethernet interface (ae0) for the interchassis control link-protection link (ICL-PL). Configure a multichassis protection link for the ICL-PL, Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the configuration, enable VRRP by completing the following steps:

- Create a routed VLAN interface (RVI).
- Create a VRRP group and assign a virtual IP address that is shared between each router in the VRRP group.
- Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group.

Consider a sample topology in which a customer edge router, CE, is connected to two provider edge (PE) routers, PE1 and PE2, respectively. The two PE devices each have a link aggregation group (LAG) connected to the CE device. The configured mode is active-active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time. PE1 and PE2 are connected to a single service provider router, P.

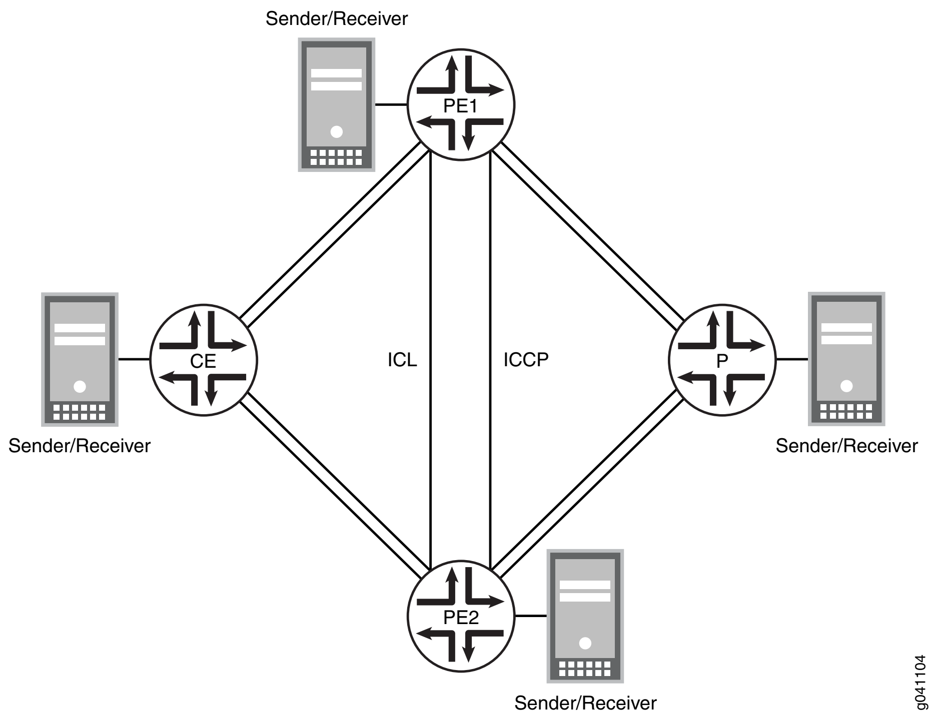
In Figure 13 on page 89, from the perspective of the CE device, all four ports belonging to a LAG are connected to a single service provider device. Because the configured mode is active-active, all four ports are active, and the CE device load-balances the traffic to the peering PE devices. On the PE routers, a regular LAG is configured facing the CE device.

On one end of an MC-LAG is an MC-LAG client device, such as a server, that has one or more physical links in a LAG. This client device does not need to detect the MC-LAG. On the other side of an MC-LAG are two MC-LAG routers. Each of the routers has one or more physical links connected to a single client device. The routers coordinate with each other to ensure that data traffic is forwarded properly.

Topology Diagram

Figure 13 on page 89 shows the topology used in this example.

Figure 30: MC-LAG Active-Active on MX Series Routers



Configuring the PE Routers

CLI Quick Configuration

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

Router PE1

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/1 gigether-options 802.3ad ae1
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.1/30
set interfaces ge-1/0/6 gigether-options 802.3ad ae0
set interfaces ge-1/1/1 flexible-vlan-tagging
set interfaces ge-1/1/1 encapsulation flexible-ethernet-services
set interfaces ge-1/1/1 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/1 unit 0 vlan-id-range 100-110
set interfaces ge-1/1/4 flexible-vlan-tagging
set interfaces ge-1/1/4 encapsulation flexible-ethernet-services
set interfaces ge-1/1/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/4 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
```

```
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/1/1.0
set bridge-domains bd0 interface ge-1/1/4.0
set bridge-domains bd0 interface ae0.0
set protocols iccp local-ip-addr 100.100.100.1
set protocols iccp peer 100.100.100.2 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.2 liveness-detection minimum-interval 1000
set protocols ospf area 0.0.0.0 interface ge-1/1/1.0 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface ge-1/1/1.0 bfd-liveness-detection
  transmit-interval minimum-interval 350
set protocols ospf area 0.0.0.0 interface ge-1/1/1.0 bfd-liveness-detection
  transmit-interval threshold 500
set protocols ospf area 0.0.0.0 interface ge-1/1/4.0 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface ge-1/1/4.0 bfd-liveness-detection
  transmit-interval minimum-interval 350
set protocols ospf area 0.0.0.0 interface ge-1/1/4.0 bfd-liveness-detection
  transmit-interval threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface ge-1/1/4.0 priority 200
set protocols pim interface ge-1/1/4.0 version 2
set protocols pim interface ge-1/1/4.0 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface ge-1/1/4.0 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface ge-1/1/4.0 bfd-liveness-detection transmit-interval threshold
  500
set protocols pim interface ge-1/1/1.0 priority 600
set protocols pim interface ge-1/1/1.0 version 2
set protocols pim interface ge-1/1/1.0 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface ge-1/1/1.0 bfd-liveness-detection transmit-interval
  minimum-interval 350
```

```
set protocols pim interface ge-1/1/1.0 bfd-liveness-detection transmit-interval threshold
  500
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set switch-options service-id 10
```

Router PE2

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.2/30
set interfaces ge-1/0/3 flexible-vlan-tagging
set interfaces ge-1/0/3 encapsulation flexible-ethernet-services
set interfaces ge-1/0/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/3 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/4 flexible-vlan-tagging
set interfaces ge-1/0/4 encapsulation flexible-ethernet-services
set interfaces ge-1/0/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/4 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/5 gigether-options 802.3ad ae0
set interfaces ge-1/1/0 gigether-options 802.3ad ae1
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/0/4.0
set bridge-domains bd0 interface ae0.0
set protocols iccp local-ip-addr 100.100.100.2
set protocols iccp peer 100.100.100.1 redundancy-group-id-list 10
```



```
set protocols iccp peer 100.100.100.1 liveness-detection minimum-interval 1000
set protocols ospf area 0.0.0.0 interface ge-1/0/4.0 bfd-liveness-detection
  minimum-receive-interval 700
set protocols ospf area 0.0.0.0 interface ge-1/0/4.0 bfd-liveness-detection
  transmit-interval minimum-interval 350
set protocols ospf area 0.0.0.0 interface ge-1/0/4.0 bfd-liveness-detection
  transmit-interval threshold 500
set protocols pim rp static address 1.0.0.3 group-ranges 239.0.0.0/8
set protocols pim interface ge-1/0/4.0 priority 200
set protocols pim interface ge-1/0/4.0 version 2
set protocols pim interface ge-1/0/4.0 bfd-liveness-detection minimum-receive-interval
  700
set protocols pim interface ge-1/0/4.0 bfd-liveness-detection transmit-interval
  minimum-interval 350
set protocols pim interface ge-1/0/4.0 bfd-liveness-detection transmit-interval threshold
  500
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set switch-options service-id 10
```

Router PE1

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router PE1:

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

   ```
   [edit chassis]
   user@PE1# set aggregated-devices ethernet device-count 5
   ```

2. Specify the members to be included within the aggregated Ethernet bundles.

   ```
   [edit interfaces]
   user@PE1# set ge-1/0/1 gigether-options 802.3ad ae1
   user@PE1# set ge-1/0/6 gigether-options 802.3ad ae0
   ```

3. Configure the interfaces that connect to senders or receivers, the interchassis link(ICL) interfaces, and the ICCP interfaces.

   ```
   [edit interfaces]
   user@PE1# set ge-1/1/1 flexible-vlan-tagging
   user@PE1# set ge-1/1/1 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/1 unit 0 encapsulation vlan-bridge
   user@PE1# set ge-1/1/1 unit 0 vlan-id-range 100-110
   user@PE1# set ge-1/1/4 flexible-vlan-tagging
   user@PE1# set ge-1/1/4 encapsulation flexible-ethernet-services
   user@PE1# set ge-1/1/4 unit 0 encapsulation vlan-bridge
   user@PE1# set ge-1/1/4 unit 0 vlan-id-range 100-110
   user@PE1# set ge-1/0/2 unit 0 family inet address 100.100.100.1/30
   ```

4. Configure parameters on the aggregated Ethernet bundles.

   ```
   [edit interfaces ae0]
   ```

user@PE1# **set flexible-vlan-tagging**
user@PE1# **set encapsulation flexible-ethernet-services**
user@PE1# **set unit 0 encapsulation vlan-bridge**
user@PE1# **set unit 0 vlan-id-range 100-110**
user@PE1# **set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0**

[edit interfaces ae1]
user@PE1# **set flexible-vlan-tagging**
user@PE1# **set encapsulation flexible-ethernet-services**
user@PE1# **set unit 0 encapsulation vlan-bridge**
user@PE1# **set unit 0 vlan-id-range 100-110**
user@PE1# **set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0**

5. Configure LACP on the aggregated Ethernet bundles.

[edit interfaces ae0 aggregated-ether-options]
user@PE1# **set lacp active**
user@PE1# **set lacp system-priority 100**
user@PE1# **set lacp system-id 00:00:00:00:00:05**
user@PE1# **set lacp admin-key 1**

[edit interfaces ae1 aggregated-ether-options]
user@PE1# **set lacp active**
user@PE1# **set lacp system-priority 100**
user@PE1# **set lacp system-id 00:00:00:00:00:05**
user@PE1# **set lacp admin-key 1**

6. Configure the MC-LAG interfaces.

[edit interfaces ae0 aggregated-ether-options]
user@PE1# **set mc-ae mc-ae-id 5**
user@PE1# **set mc-ae redundancy-group 10**
user@PE1# **set mc-ae chassis-id 1**
user@PE1# **set mc-ae mode active-active**
user@PE1# **set mc-ae status-control active**

[edit interfaces ae1 aggregated-ether-options]
user@PE1# **set mc-ae mc-ae-id 10**
user@PE1# **set mc-ae redundancy-group 10**
user@PE1# **set mc-ae chassis-id 1**
user@PE1# **set mc-ae mode active-active**
user@PE1# **set mc-ae status-control active**

The multichassis aggregated Ethernet identification number (**mc-ae-id**) specifies which link aggregation group the aggregated Ethernet interface belongs to. The ae0 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 5**. The ae1 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 10**. (To refer to the configuration on Router PE2, see "Router PE2" on page 90).

The **redundancy-group 10** statement is 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 **ae0** and **ae1** interfaces on Router PE1 and Router PE2 are configured with the same redundancy group **redundancy-group 10**.

The **chassis-id** statement is used by LACP for calculating the port number of the MC-LAG's physical member links. Router PE1 uses **chassid-id 1** to identify both its ae0 and ae1 interfaces. Router PE2 (as shown in “Router PE2” on page 90) uses **chassis-id 0** to identify both its ae0 and ae1 interfaces.

The **mode** statement 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.

7. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@PE1# set domain-type bridge
user@PE1# set vlan-id all
user@PE1# set service-id 20
user@PE1# set interface ae0.0
user@PE1# set interface ae1.0
user@PE1# set interface ge-1/0/3.0
user@PE1# set interface ge-1/1/1.0
user@PE1# set interface ge-1/1/4.0
```

The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

The bridge-level **service-id** statement is required to link related bridge domains across peers (in this case Router PE1 and Router PE2), and should be configured with the same value.

8. Configure ICCP parameters.

```
[edit protocols iccp]
user@PE1# set local-ip-addr 100.100.100.1
user@PE1# set peer 100.100.100.2 redundancy-group-id-list 10
user@PE1# set peer 100.100.100.2 liveness-detection minimum-interval 1000
```

9. Configure the service ID at the global level.

```
[edit switch-options]
user@PE1# set service-id 10
```

You must configure the same unique network-wide configuration for a service in the set of PE routers providing the service. This service ID is required if the multichassis aggregated Ethernet interfaces are part of a bridge domain.

Step-by-Step Procedure

To enable VRRP on the MC-LAGs :

1. Assign the priority for each router in the VRRP groups.

NOTE: The router configured with the highest priority is the master.

PE1

```
[edit interfaces]
user@PE1# set vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 priority 200
```

user@PE1 #**set vlan unit 200 family inet address 10.1.1.21/24 vrrp-group 2 priority 200**

PE2

[edit interfaces]
user@PE2# **set vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 priority 150**
user@PE2# **set vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 priority 150**

2. Enable the router to accept all packets destined for the virtual IP address if it is the master in a VRRP group.

PE1

[edit interfaces]
user@PE1# **set vlan unit 100 family inet address 10.1.1.11/24 vrrp-group 1 accept-data**

PE2

[edit interfaces]
user@PE2# **set vlan unit 100 family inet address 10.1.1.10/24 vrrp-group 1 accept-data**
user@PE2# **set vlan unit 200 family inet address 10.1.1.20/24 vrrp-group 2 accept-data**

Step-by-Step Procedure

To configure OSPF as the Layer 3 protocol:

1. Configure an OSPF area .

   [edit protocols ospf]
   user@PE1# **set area 0.0.0.0**

2. Assign the VLAN interfaces for the MC-LAGs as interfaces to the OSPF area .

   [edit protocols ospf area 0.0.0.0]
   user@PE1# **set interface ge-1/1/1.0**
   user@PE1# **set interface ge-1/4/1.0**

3. Configure the minimum receive interval, minimum transmit interval, and transmit interval threshold for a Bidirectional Forwarding Detection (BFD) session for the OSPF interfaces .

   [edit protocols ospf area 0.0.0.0]
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection minimum-receive-interval 700**
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection transmit-interval minimum-interval 350**
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection transmit-interval threshold 500**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection minimum-receive-interval 700**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection transmit-interval minimum-interval 350**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection transmit-interval threshold 500**

Step-by-Step Procedure

To configure PIM as the multicast protocol:

1. Configure a static rendezvous point (RP) address .

   [edit protocols pim]
   user@PE1# **set rp static address 1.0.0.3**

2. Configure the address ranges of the multicast groups for which PE1 and PE2 can be a rendezvous point (RP).

   [edit protocols pim rp static address 1.0.0.3]
   user@PE1# **set group-ranges 239.0.0.0/8**

3. Enable PIM on the VLAN interfaces for the MC-LAGs on PE1 and PE2.

   [edit protocols pim]
   user@PE1# **set interface ge-1/1/1.0 version 2**
   user@PE1# **set interface ge-1/4/1.0 version 2**

4. Configure each PIM interface's priority for being selected as the designated router (DR).

   An interface with a higher priority value has a higher probability of being selected as the DR.

   [edit protocols pim]
   user@PE1# **set interface ge-1/1/1.0 priority 600**
   user@PE1# **set interface ge-1/4/1.0 priority 200**

5. Configure the minimum receive interval, minimum transmit interval, and transmit interval threshold for a Bidirectional Forwarding Detection (BFD) session for the PIM interfaces on PE1 and PE2.

   [edit protocols pim]
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection minimum-receive-interval 700**
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection transmit-interval minimum-interval 350**
   user@PE1# **set interface ge-1/1/1.0 bfd-liveness-detection transmit-interval threshold 500**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection minimum-receive-interval 700**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection transmit-interval minimum-interval 350**
   user@PE1# **set interface ge-1/4/1.0 bfd-liveness-detection transmit-interval threshold 500**

Step-by-Step Procedure

To enable RSTP:

1. Enable RSTP globally on all interfaces.

   `[edit]`
   `user@PE1#` **set protocols rstp interface ae1.0 mode point-to-point**

2. Configure the MC-LAG interfaces as edge ports on PE1 and PE2.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit]
user@PE1# set protocols rstp interface ae1.0 edge
```

3. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces on PE1 and PE2.

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

```
[edit]
user@PE1# set protocols rstp bpdu-block-on-edge
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, **show interfaces**, **show protocols**, and **show switch-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  service-id 20;
  interface ae1.0;
  interface ge-1/0/3.0
  interface ge-1/1/1.0;
  interface ge-1/1/4.0;
  interface ae0.0;
}
```

```
user@PE1# show chassis
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
```

```
user@PE1# show interfaces
ge-1/0/1 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-1/0/2 {
  unit 0 {
    family inet {
      address 100.100.100.1/30;
    }
```



```
    }
  }
  ge-1/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
    }
  }
  ge-1/1/4 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
    }
  }
  ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
      lacp {
        active;
        system-priority 100;
        system-id 00:00:00:00:00:05;
        admin-key 1;
      }
      mc-ae {
        mc-ae-id 5;
        redundancy-group 10;
        chassis-id 1;
        mode active-active;
        status-control active;
      }
    }
    unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
      multi-chassis-protection 100.100.100.2 {
        interface ge-1/1/4.0;
      }
    }
  }
  ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
      lacp {
        active;
        system-priority 100;
        system-id 00:00:00:00:00:05;
        admin-key 1;
      }
      mc-ae {
        mc-ae-id 10;
```

```
            redundancy-group 10;
            chassis-id 1;
            mode active-active;
            status-control active;
        }
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
```

```
user@PE1# show vrrp
vlan {
    unit 100 {
        family inet {
            address 10.1.1.11/24 {
                vrrp-group 1 {
                    virtual-address 10.1.1.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 200 {
        family inet {
            address 10.1.1.21/24 {
                vrrp-group 2 {
                    virtual-address 10.1.1.2;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
}
```

```
user@PE1# show protocols
iccp {
    local-ip-addr 100.100.100.1;
    peer 100.100.100.2 {
        redundancy-group-id-list 10;
        liveness-detection {
            minimum-interval 1000;
        }
        }
    }
}
rstp {
    interface ae1.0 {
        edge;
    }
    interface ae1.0 {
```



```
        mode point-to-point;
      }
      bpdu-block-on-edge;
    }
    ospf {
      area 0.0.0.0 {
        interface ge-1/1/1.0 {
          bfd-liveness-detection {
            minimum-receive-interval 700;
            transmit-interval {
              minimum-interval 350;
              threshold 500;
            }
          }
        }
        interface ge-1/4/1.0 {
          bfd-liveness-detection {
            minimum-receive-interval 700;
            transmit-interval {
              minimum-interval 350;
              threshold 500;
            }
          }
        }
      }
    }
    pim {
      rp {
        static {
          address 1.0.0.3 {
            group-ranges {
              239.0.0.0/8;
            }
          }
        }
      }
      interface ge-1/1/1.0 {
        priority 600;
        version 2;
        bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
          minimum-receive-interval 700;
          transmit-interval {
            minimum-interval 350;
            threshold 500;
          }
        }
      }
      interface ge-1/4/1.0 {
        priority 200;
        version 2;
        bfd-liveness-detection { ## Warning: 'bfd-liveness-detection' is deprecated
          minimum-receive-interval 700;
          transmit-interval {
            minimum-interval 350;
            threshold 500;
          }
```

```
        }
      }
    }
```

user@PE1> **show switch-options**
service-id 10;

If you are done configuring the device, enter **commit** from configuration mode.

Repeat the procedure for Router PE2, using the appropriate interface names and addresses.

Configuring the CE Router

CLI Quick Configuration

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

Router CE

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-2/0/2 gigether-options 802.3ad ae0
set interfaces ge-2/0/3 gigether-options 802.3ad ae0
set interfaces ge-2/1/6 flexible-vlan-tagging
set interfaces ge-2/1/6 encapsulation flexible-ethernet-services
set interfaces ge-2/1/6 unit 0 encapsulation vlan-bridge
set interfaces ge-2/1/6 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-500
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 interface ge-2/1/6.0
set bridge-domains bd0 interface ae0.0
```

Router CE

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router CE:

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

   [edit chassis]
   user@CE# **set aggregated-devices ethernet device-count 2**

2. Specify the members to be included within the aggregated Ethernet bundle.

   [edit interfaces]
   user@CE# **set ge-2/0/2 gigether-options 802.3ad ae0**
   user@CE# **set ge-2/0/3 gigether-options 802.3ad ae0**

3. Configure an interface that connects to senders or receivers.

```
[edit interfaces ge-2/1/6]
user@CE# set flexible-vlan-tagging
user@CE# set encapsulation flexible-ethernet-services
user@CE# set unit 0 encapsulation vlan-bridge
user@CE# set unit 0 vlan-id-range 100-110
```

4. Configure parameters on the aggregated Ethernet bundle.

```
[edit interfaces ae0]
user@CE# set flexible-vlan-tagging
user@CE# set encapsulation flexible-ethernet-services
user@CE# set unit 0 encapsulation vlan-bridge
user@CE# set unit 0 vlan-id-range 100-500
```

5. Configure LACP on the aggregated Ethernet bundle.

```
[edit interfaces ae0 aggregated-ether-options]
user@CE# set lacp active
user@CE# set lacp system-priority 100
```

   The **active** statement initiates transmission of LACP packets.

   For the **system-priority** statement, a smaller value indicates a higher priority. The device with the lower system priority value determines which links between LACP partner devices are active and which are in standby mode for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

6. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@CE# set domain-type bridge
user@CE# set vlan-id all
user@CE# set interface ge-2/1/6.0
user@CE# set interface ae0.0
```

   The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@CE# show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  interface ge-2/1/6.0;
  interface ae0.0;
}
```

```
user@CE# show chassis
```

```
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@CE# show interfaces
ge-2/0/2 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/0/3 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-2/1/6 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-110;
  }
}
ae0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  aggregated-ether-options {
    lacp {
      active;
      system-priority 100;
    }
  }
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-500;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring the Provider Router

CLI Quick Configuration

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

Router P

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-1/0/5 gigether-options 802.3ad ae1
set interfaces ge-1/0/11 gigether-options 802.3ad ae1
set interfaces ge-1/1/3 flexible-vlan-tagging
set interfaces ge-1/1/3 encapsulation flexible-ethernet-services
set interfaces ge-1/1/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/3 unit 0 vlan-id-range 100-500
```

```
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 interface ge-1/1/3.0
set bridge-domains bd0 interface ae1.0
```

Router P

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router P:

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

   ```
   [edit chassis]
   user@P# set aggregated-devices ethernet device-count 2
   ```

2. Specify the members to be included within the aggregated Ethernet bundle.

   ```
   [edit interfaces]
   user@P# set ge-1/0/5 gigether-options 802.3ad ae1
   user@P# set ge-1/0/11 gigether-options 802.3ad ae1
   ```

3. Configure an interface that connects to senders or receivers.

   ```
   [edit interfaces ge-1/1/3]
   user@P# set flexible-vlan-tagging
   user@P# set encapsulation flexible-ethernet-services
   user@P# set unit 0 encapsulation vlan-bridge
   user@P# set unit 0 vlan-id-range 100-500
   ```

4. Configure parameters on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae1]
   user@P# set flexible-vlan-tagging
   user@P# set encapsulation flexible-ethernet-services
   user@P# set unit 0 encapsulation vlan-bridge
   user@P# set unit 0 vlan-id-range 100-110
   ```

5. Configure LACP on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae1 aggregated-ether-options]
   user@P# set lacp active
   user@P# set lacp system-priority 100
   ```

6. Configure a domain that includes the set of logical ports.

   ```
   [edit bridge-domains bd0]
   user@P# set vlan-id all
   user@P# set domain-type bridge
   user@P# set interface ge-1/1/3.0
   ```



```
user@P# set interface ae1.0
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@P# show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  interface ge-1/1/3.0;
  interface ae1.0;
}
```

```
user@P# show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@P# show interfaces
ge-1/0/5 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/11 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/1/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-500;
  }
}
ae1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  aggregated-ether-options {
    lacp {
      active;
      system-priority 100;
    }
  }
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-110;
  }
}
```


If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly by running the following commands:

- **show iccp**
- **show interfaces ae0**
- **show interfaces ae1**
- **show interfaces mc-ae**
- **show pim interfaces**
- **show vrrp**
- ***show l2-learning instance* extensive**

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**.

Solution Check the following:

- Verify that there is no configuration mismatch.
- Verify that all member ports are up.
- Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
- Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers on page 87
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on MX Series Routers on page 291

Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on MX Series Routers

Supported Platforms MX240, MX480, MX960

There are two methods for enabling Layer 3 unicast functionality across a multichassis link aggregation group (MC-LAG) to control traffic flow. You can choose either to configure the Virtual Router Redundancy Protocol (VRRP) or synchronize the MAC addresses for the Layer 3 interfaces of the routers participating in the MC-LAG. The procedure to configure VRRP for use in a Layer 3 unicast MC-LAG is included in this example.

Requirements

This example uses the following hardware and software components:

- Four Juniper Networks MX Series routers
- Junos OS Release 11.2 or later running on all four routers

Before you configure an MC-LAG, be sure that you understand how to:

- Configure aggregated Ethernet interfaces on a router.
- Configure the Link Aggregation Control Protocol (LACP) on aggregated Ethernet interfaces on a router.
- Configure the Virtual Router Redundancy Protocol (VRRP) on a router.

Overview

In this example, you configure an MC-LAG across two routers by including interfaces from both routers in an aggregated Ethernet interface (ae1). To support the MC-LAG, create a second aggregated Ethernet interface (ae0) for the interchassis control link-protection link (ICL-PL). Configure a multichassis protection link for the ICL-PL, Inter-Chassis Control Protocol (ICCP) for the peers hosting the MC-LAG, and Layer 3 connectivity between MC-LAG peers.

NOTE: Layer 3 connectivity is required for ICCP.

To complete the configuration, enable VRRP by completing the following steps:

1. Create a routed VLAN interface (RVI).
2. Create a VRRP group and assign a virtual IP address that is shared between each router in the VRRP group.

3. Enable a member of a VRRP group to accept all packets destined for the virtual IP address if it is the master in the VRRP group.

Consider a sample topology in which a customer edge router, CE, is connected to two provider edge (PE) routers, PE1 and PE2, respectively. The two PE devices each have a LAG connected to the CE device. The configured mode is active-active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time. PE1 and PE2 are connected to a single service provider router, P.

In this example, the CE router is not aware that its aggregated Ethernet links are connected to two separate PE devices. The two PE devices each have a LAG connected to the CE device. The configured mode is active-active, meaning that both PE routers' LAG ports are active and carrying traffic at the same time.

In Figure 13 on page 89, from the perspective of Router CE, all four ports belonging to a LAG are connected to a single service provider device. Because the configured mode is active-active, all four ports are active, and the CE device load-balances the traffic to the peering PE devices. On the PE routers, a regular LAG is configured facing the CE device.

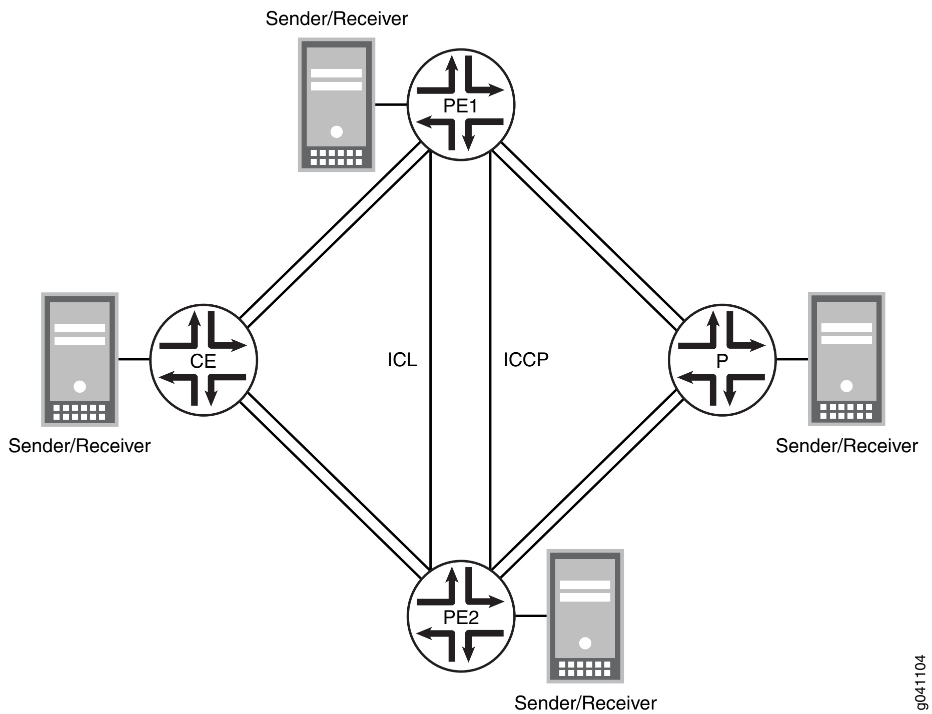
On one end of an MC-LAG is an MC-LAG client device, such as a server, that has one or more physical links in a link aggregation group (LAG). This client device does not need to detect the MC-LAG. On the other side of an MC-LAG are two MC-LAG routers. Each of the routers has one or more physical links connected to a single client device. The routers coordinate with each other to ensure that data traffic is forwarded properly.

ICCP messages are sent between the two PE devices. In this example, you configure an MC-LAG across two routers, consisting of two aggregated Ethernet interfaces, an interchassis control link-protection link (ICL-PL), multichassis protection link for the ICL-PL, and ICCP for the peers hosting the MC-LAG.

Topology Diagram

Figure 13 on page 89 shows the topology used in this example.

Figure 31: MC-LAG Active-Active on MX Series Routers



Configuring the PE Routers

CLI Quick Configuration

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

Router PE1

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/1 gigether-options 802.3ad ae1
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.1/30
set interfaces ge-1/0/6 gigether-options 802.3ad ae0
set interfaces ge-1/1/1 flexible-vlan-tagging
set interfaces ge-1/1/1 encapsulation flexible-ethernet-services
set interfaces ge-1/1/1 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/1 unit 0 vlan-id-range 100-110
set interfaces ge-1/1/4 flexible-vlan-tagging
set interfaces ge-1/1/4 encapsulation flexible-ethernet-services
set interfaces ge-1/1/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/4 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
```



```
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 1
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/1/1.0
set bridge-domains bd0 interface ge-1/1/4.0
set bridge-domains bd0 interface ae0.0
set vrrp vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1
set vrrp vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200
set vrrp vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data
set protocols iccp local-ip-addr 100.100.100.1
set protocols iccp peer 100.100.100.2 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.2 liveness-detection minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface all mode point-to-point
set protocols rstp bpdu-block-on-edge
set switch-options service-id 10
```

Router PE2

```
set chassis aggregated-devices ethernet device-count 5
set interfaces ge-1/0/2 unit 0 family inet address 100.100.100.2/30
set interfaces ge-1/0/3 flexible-vlan-tagging
set interfaces ge-1/0/3 encapsulation flexible-ethernet-services
set interfaces ge-1/0/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/3 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/4 flexible-vlan-tagging
set interfaces ge-1/0/4 encapsulation flexible-ethernet-services
set interfaces ge-1/0/4 unit 0 encapsulation vlan-bridge
set interfaces ge-1/0/4 unit 0 vlan-id-range 100-110
set interfaces ge-1/0/5 gigether-options 802.3ad ae0
set interfaces ge-1/1/0 gigether-options 802.3ad ae1
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae0 aggregated-ether-options lacp admin-key 1
set interfaces ae0 aggregated-ether-options mc-ae mc-ae-id 5
```

```
set interfaces ae0 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae0 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae0 aggregated-ether-options mc-ae mode active-active
set interfaces ae0 aggregated-ether-options mc-ae status-control active
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-110
set interfaces ae0 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 aggregated-ether-options lacp system-id 00:00:00:00:00:05
set interfaces ae1 aggregated-ether-options lacp admin-key 1
set interfaces ae1 aggregated-ether-options mc-ae mc-ae-id 10
set interfaces ae1 aggregated-ether-options mc-ae redundancy-group 10
set interfaces ae1 aggregated-ether-options mc-ae chassis-id 0
set interfaces ae1 aggregated-ether-options mc-ae mode active-active
set interfaces ae1 aggregated-ether-options mc-ae status-control active
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set interfaces ae1 unit 0 multi-chassis-protection 100.100.100.1 interface ge-1/0/4.0
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 service-id 20
set bridge-domains bd0 interface ae1.0
set bridge-domains bd0 interface ge-1/0/3.0
set bridge-domains bd0 interface ge-1/0/4.0
set bridge-domains bd0 interface ae0.0
set protocols iccp local-ip-addr 100.100.100.2
set protocols iccp peer 100.100.100.1 redundancy-group-id-list 10
set protocols iccp peer 100.100.100.1 liveness-detection minimum-interval 1000
set protocols rstp interface ae1.0 edge
set protocols rstp interface ae1.0 mode point-to-point
set protocols rstp bpdu-block-on-edge
set switch-options service-id 10
```

Router PE1

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router PE1:

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

   ```
   [edit chassis]
   user@PE1# set aggregated-devices ethernet device-count 5
   ```

2. Specify the members to be included within the aggregated Ethernet bundles.

   ```
   [edit interfaces]
   user@PE1# set ge-1/0/1 gigether-options 802.3ad ae1
   user@PE1# set ge-1/0/6 gigether-options 802.3ad ae0
   ```

3. Configure the interfaces that connect to senders or receivers, the ICL interfaces, and the ICCP interfaces.

```
[edit interfaces]
user@PE1# set ge-1/1/1 flexible-vlan-tagging
user@PE1# set ge-1/1/1 encapsulation flexible-ethernet-services
user@PE1# set ge-1/1/1 unit 0 encapsulation vlan-bridge
user@PE1# set ge-1/1/1 unit 0 vlan-id-range 100-110
user@PE1# set ge-1/1/4 flexible-vlan-tagging
user@PE1# set ge-1/1/4 encapsulation flexible-ethernet-services
user@PE1# set ge-1/1/4 unit 0 encapsulation vlan-bridge
user@PE1# set ge-1/1/4 unit 0 vlan-id-range 100-110
user@PE1# set ge-1/0/2 unit 0 family inet address 100.100.100.1/30
```

4. Configure parameters on the aggregated Ethernet bundles.

```
[edit interfaces ae0]
user@PE1# set flexible-vlan-tagging
user@PE1# set encapsulation flexible-ethernet-services
user@PE1# set unit 0 encapsulation vlan-bridge
user@PE1# set unit 0 vlan-id-range 100-110
user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0

[edit interfaces ae1]
user@PE1# set flexible-vlan-tagging
user@PE1# set encapsulation flexible-ethernet-services
user@PE1# set unit 0 encapsulation vlan-bridge
user@PE1# set unit 0 vlan-id-range 100-110
user@PE1# set unit 0 multi-chassis-protection 100.100.100.2 interface ge-1/1/4.0
```

5. Configure LACP on the aggregated Ethernet bundles.

```
[edit interfaces ae0 aggregated-ether-options]
user@PE1# set lacp active
user@PE1# set lacp system-priority 100
user@PE1# set lacp system-id 00:00:00:00:00:05
user@PE1# set lacp admin-key 1

[edit interfaces ae1 aggregated-ether-options]
user@PE1# set lacp active
user@PE1# set lacp system-priority 100
user@PE1# set lacp system-id 00:00:00:00:00:05
user@PE1# set lacp admin-key 1
```

6. Configure the MC-LAG interfaces.

```
[edit interfaces ae0 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 5
user@PE1# set mc-ae redundancy-group 10
user@PE1# set mc-ae chassis-id 1
user@PE1# set mc-ae mode active-active
user@PE1# set mc-ae status-control active

[edit interfaces ae1 aggregated-ether-options]
user@PE1# set mc-ae mc-ae-id 10
user@PE1# set mc-ae redundancy-group 10
```

user@PE1# **set mc-ae chassis-id 1**
user@PE1# **set mc-ae mode active-active**
user@PE1# **set mc-ae status-control active**

The multichassis aggregated Ethernet identification number (**mc-ae-id**) specifies which link aggregation group the aggregated Ethernet interface belongs to. The ae0 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 5**. The ae1 interfaces on Router PE1 and Router PE2 are configured with **mc-ae-id 10**. (To refer to the configuration on Router PE2, see "Router PE2" on page 90)

The **redundancy-group 10** statement is 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 **ae0** and **ae1** interfaces on Router PE1 and Router PE2 are configured with the same redundancy group, **redundancy-group 10**.

The **chassis-id** statement is used by LACP for calculating the port number of the MC-LAG's physical member links. Router PE1 uses **chassid-id 1** to identify both its ae0 and ae1 interfaces. Router PE2 (as shown in "Router PE2" on page 90) uses **chassis-id 0** to identify both its ae0 and ae1 interfaces.

The **mode** statement 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.

7. Configure a domain that includes the set of logical ports.

   [edit bridge-domains bd0]
   user@PE1# **set domain-type bridge**
   user@PE1# **set vlan-id all**
   user@PE1# **set service-id 20**
   user@PE1# **set interface ae0.0**
   user@PE1# **set interface ae1.0**
   user@PE1# **set interface ge-1/0/3.0**
   user@PE1# **set interface ge-1/1/1.0**
   user@PE1# **set interface ge-1/1/4.0**

   The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

   The bridge-level **service-id** statement is required to link related bridge domains across peers (in this case Router PE1 and Router PE2), and should be configured with the same value.

8. Configure ICCP parameters.

   [edit protocols iccp]
   user@PE1# **set local-ip-addr 100.100.100.1**
   user@PE1# **set peer 100.100.100.2 redundancy-group-id-list 10**
   user@PE1# **set peer 100.100.100.2 liveness-detection minimum-interval 1000**

9. Configure the service ID at the global level.

   [edit switch-options]
   user@PE1# **set service-id 10**

You must configure the same unique network-wide configuration for a service in the set of PE routers providing the service. This service ID is required if the multichassis aggregated Ethernet interfaces are part of a bridge domain.

Step-by-Step Procedure

To enable VRRP on the MC-LAGs :

1. Enable VRRP on the MC-LAG on PE1 :

   - Create a routed VLAN interface (RVI), assign a virtual IP address that is shared between each router in the VRRP group, and assign an individual IP address for each router in the VRRP group:

     ```
     [edit interfaces]
     user@PE1# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 virtual-address 100.1.1.1
     ```

   - Assign the priority for each router in the VRRP group:

     NOTE: The router configured with the highest priority is the master.

     ```
     [edit interfaces]
     user@PE1# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 priority 200
     ```

   - Enable the router to accept all packets destined for the virtual IP address if it is the master in the VRRP group:

     ```
     [edit interfaces]
     user@PE1# set vlan unit 100 family inet address 100.1.1.11/24 vrrp-group 1 accept-data
     ```

Step-by-Step Procedure

To enable RSTP:

1. Enable RSTP globally on all interfaces.

   ```
   [edit]
   user@PE1# set protocols rstp interface ae1.0 mode point-to-point
   ```

2. Configure the MC-LAG interfaces as edge ports .

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
   user@PE1# set protocols rstp interface ae1.0 edge
   ```

3. Enable BPDU blocking on all interfaces except for the ICL-PL interfaces .

   NOTE: The ae1 interface is a downstream interface. This is why RSTP and bpdu-block-on-edge need to be configured.

   ```
   [edit]
   user@PE1# set protocols rstp bpdu-block-on-edge
   ```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, **show interfaces**, **show protocols**, and **show switch-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  service-id 20;
  interface ae1.0;
  interface ge-1/0/3.0
  interface ge-1/1/1.0;
  interface ge-1/1/4.0;
  interface ae0.0;
}
```

```
user@PE1# show vrrp
vlan {
unit 100 {
  family inet {
    address 100.1.1.11/24 {
      vrrp-group 1 {
        virtual-address 100.1.1.1;
        priority 200;
        accept-data;
      }
    }
  }
}
```

```
user@PE1# show chassis
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
```

```
user@PE1# show interfaces
ge-1/0/1 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/6 {
  gigether-options {
    802.3ad ae0;
  }
}
ge-1/0/2 {
  unit 0 {
    family inet {
      address 100.100.100.1/30;
    }
```



```
    }
}
ge-1/1/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
    }
}
ge-1/1/4 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
    }
}
ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        lacp {
            active;
            system-priority 100;
            system-id 00:00:00:00:00:05;
            admin-key 1;
        }
        mc-ae {
            mc-ae-id 5;
            redundancy-group 10;
            chassis-id 1;
            mode active-active;
            status-control active;
        }
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        lacp {
            active;
            system-priority 100;
            system-id 00:00:00:00:00:05;
            admin-key 1;
        }
        mc-ae {
            mc-ae-id 10;
```

```
            redundancy-group 10;
            chassis-id 1;
            mode active-active;
            status-control active;
        }
    }
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id-range 100-110;
        multi-chassis-protection 100.100.100.2 {
            interface ge-1/1/4.0;
        }
    }
}
```

```
user@PE1# show protocols
iccp {
    local-ip-addr 100.100.100.1;
    peer 100.100.100.2 {
        redundancy-group-id-list 10;
        liveness-detection {
            minimum-interval 1000;
        }
        }
        rstp {
            interface ae1.0 {
                edge;
            }
            interface ae1.0 {
                mode point-to-point;
            }
            bpdu-block-on-edge;
        }
    }
}
```

```
user@PE1# show switch-options
service-id 10;
```

If you are done configuring the device, enter **commit** from configuration mode.

Repeat the procedure for Router PE2, using the appropriate interface names and addresses.

Configuring the CE Router

CLI Quick Configuration

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

Router CE

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-2/0/2 gigether-options 802.3ad ae0
set interfaces ge-2/0/3 gigether-options 802.3ad ae0
set interfaces ge-2/1/6 flexible-vlan-tagging
set interfaces ge-2/1/6 encapsulation flexible-ethernet-services
```



```
set interfaces ge-2/1/6 unit 0 encapsulation vlan-bridge
set interfaces ge-2/1/6 unit 0 vlan-id-range 100-110
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp system-priority 100
set interfaces ae0 unit 0 encapsulation vlan-bridge
set interfaces ae0 unit 0 vlan-id-range 100-500
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 interface ge-2/1/6.0
set bridge-domains bd0 interface ae0.0
```

Router CE

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router CE:

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

   ```
   [edit chassis]
   user@CE# set aggregated-devices ethernet device-count 2
   ```

2. Specify the members to be included within the aggregated Ethernet bundle.

   ```
   [edit interfaces]
   user@CE# set ge-2/0/2 gigether-options 802.3ad ae0
   user@CE# set ge-2/0/3 gigether-options 802.3ad ae0
   ```

3. Configure an interface that connects to senders or receivers.

   ```
   [edit interfaces ge-2/1/6]
   user@CE# set flexible-vlan-tagging
   user@CE# set encapsulation flexible-ethernet-services
   user@CE# set unit 0 encapsulation vlan-bridge
   user@CE# set unit 0 vlan-id-range 100-110
   ```

4. Configure parameters on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae0]
   user@CE# set flexible-vlan-tagging
   user@CE# set encapsulation flexible-ethernet-services
   user@CE# set unit 0 encapsulation vlan-bridge
   user@CE# set unit 0 vlan-id-range 100-500
   ```

5. Configure LACP on the aggregated Ethernet bundle.

   ```
   [edit interfaces ae0 aggregated-ether-options]
   user@CE# set lacp active
   user@CE# set lacp system-priority 100
   ```

   The **active** statement initiates transmission of LACP packets.

   For the **system-priority** statement, a smaller value indicates a higher priority. The device with the lower system priority value determines which links between LACP partner devices are active and which are in standby mode for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

6. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@CE# set domain-type bridge
user@CE# set vlan-id all
user@CE# set interface ge-2/1/6.0
user@CE# set interface ae0.0
```

The ports within a bridge domain share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@CE#  show bridge-domains
bd0 {
   domain-type bridge;
   vlan-id all;
   interface ge-2/1/6.0;
   interface ae0.0;
}
```

```
user@CE#  show chassis
aggregated-devices {
   ethernet {
      device-count 2;
   }
}
```

```
user@CE# show interfaces
ge-2/0/2 {
   gigether-options {
      802.3ad ae0;
   }
}
ge-2/0/3 {
   gigether-options {
      802.3ad ae0;
   }
}
ge-2/1/6 {
   flexible-vlan-tagging;
   encapsulation flexible-ethernet-services;
   unit 0 {
      encapsulation vlan-bridge;
      vlan-id-range 100-110;
   }
}
```



```
ae0 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  aggregated-ether-options {
    lacp {
      active;
      system-priority 100;
    }
  }
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-500;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring the Provider Router

CLI Quick Configuration

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

Router P

```
set chassis aggregated-devices ethernet device-count 2
set interfaces ge-1/0/5 gigether-options 802.3ad ae1
set interfaces ge-1/0/11 gigether-options 802.3ad ae1
set interfaces ge-1/1/3 flexible-vlan-tagging
set interfaces ge-1/1/3 encapsulation flexible-ethernet-services
set interfaces ge-1/1/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/3 unit 0 vlan-id-range 100-500
set interfaces ae1 flexible-vlan-tagging
set interfaces ae1 encapsulation flexible-ethernet-services
set interfaces ae1 aggregated-ether-options lacp active
set interfaces ae1 aggregated-ether-options lacp system-priority 100
set interfaces ae1 unit 0 encapsulation vlan-bridge
set interfaces ae1 unit 0 vlan-id-range 100-110
set bridge-domains bd0 vlan-id all
set bridge-domains bd0 domain-type bridge
set bridge-domains bd0 interface ge-1/1/3.0
set bridge-domains bd0 interface ae1.0
```

Router P

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router P:

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

   ```
   [edit chassis]
   user@P# set aggregated-devices ethernet device-count 2
   ```

2. Specify the members to be included within the aggregated Ethernet bundle.

```
[edit interfaces]
user@P# set ge-1/0/5 gigether-options 802.3ad ae1
user@P# set ge-1/0/11 gigether-options 802.3ad ae1
```

3. Configure an interface that connects to senders or receivers.

```
[edit interfaces ge-1/1/3]
user@P# set flexible-vlan-tagging
user@P# set encapsulation flexible-ethernet-services
user@P# set unit 0 encapsulation vlan-bridge
user@P# set unit 0 vlan-id-range 100-500
```

4. Configure parameters on the aggregated Ethernet bundle.

```
[edit interfaces ae1]
user@P# set flexible-vlan-tagging
user@P# set encapsulation flexible-ethernet-services
user@P# set unit 0 encapsulation vlan-bridge
user@P# set unit 0 vlan-id-range 100-110
```

5. Configure LACP on the aggregated Ethernet bundle.

```
[edit interfaces ae1 aggregated-ether-options]
user@P# set lacp active
user@P# set lacp system-priority 100
```

6. Configure a domain that includes the set of logical ports.

```
[edit bridge-domains bd0]
user@P# set vlan-id all
user@P# set domain-type bridge
user@P# set interface ge-1/1/3.0
user@P# set interface ae1.0
```

Results

From configuration mode, confirm your configuration by entering the **show bridge-domains**, **show chassis**, and **show interfaces** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@P#  show bridge-domains
bd0 {
  domain-type bridge;
  vlan-id all;
  interface ge-1/1/3.0;
  interface ae1.0;
}
```

```
user@P#  show chassis
aggregated-devices {
  ethernet {
    device-count 2;
  }
}
```

```
user@P#  show interfaces
```



```
ge-1/0/5 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/0/11 {
  gigether-options {
    802.3ad ae1;
  }
}
ge-1/1/3 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-500;
  }
}
ae1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  aggregated-ether-options {
    lacp {
      active;
      system-priority 100;
    }
  }
  unit 0 {
    encapsulation vlan-bridge;
    vlan-id-range 100-110;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly by running the following commands:

- **show iccp**
- **show interfaces ae0**
- **show interfaces ae1**
- **show interfaces mc-ae**
- **show vrrp**
- ***show l2-learning instance* extensive**

Troubleshooting

Troubleshooting a LAG That Is Down

Problem The **show interfaces terse** command shows that the MC-LAG is **down**.

Solution Check the following:

1. Verify that there is no configuration mismatch.
2. Verify that all member ports are up.
3. Verify that the MC-LAG is part of family Ethernet switching (Layer 2 LAG).
4. Verify that the MC-LAG member is connected to the correct MC-LAG member at the other end.

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63
- Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers on page 75
- Example: Configuring Multichassis Link Aggregation in an Active-Active Mode on MX Series Routers on page 87
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on MX Series Routers on page 272

CHAPTER 5

Configuring CoS for FCoE Transit Switch Traffic Across an MC-LAG

Understanding MC-LAGs on an FCoE Transit Switch

Supported Platforms EX4600, QFabric System, QFX Series standalone switches

Multichassis link aggregation groups (MC-LAGs) provide redundancy and load balancing between two switches, multihoming support for client devices such as servers, and a loop-free Layer 2 network without running Spanning Tree Protocol (STP).

You can use an MC-LAG to provide a redundant aggregation layer for Fibre Channel over Ethernet (FCoE) traffic. To support lossless transport of FCoE traffic across an MC-LAG, you must configure the appropriate class of service (CoS) on both of the switches with MC-LAG port members. The CoS configuration must be the same on both of the MC-LAG switches because MC-LAGs do not carry forwarding class and IEEE 802.1p priority information.

Ports that are part of an FCoE-FC gateway configuration (a virtual FCoE-FC gateway fabric) do not support MC-LAGs. Ports that are members of an MC-LAG act as passthrough transit switch ports.

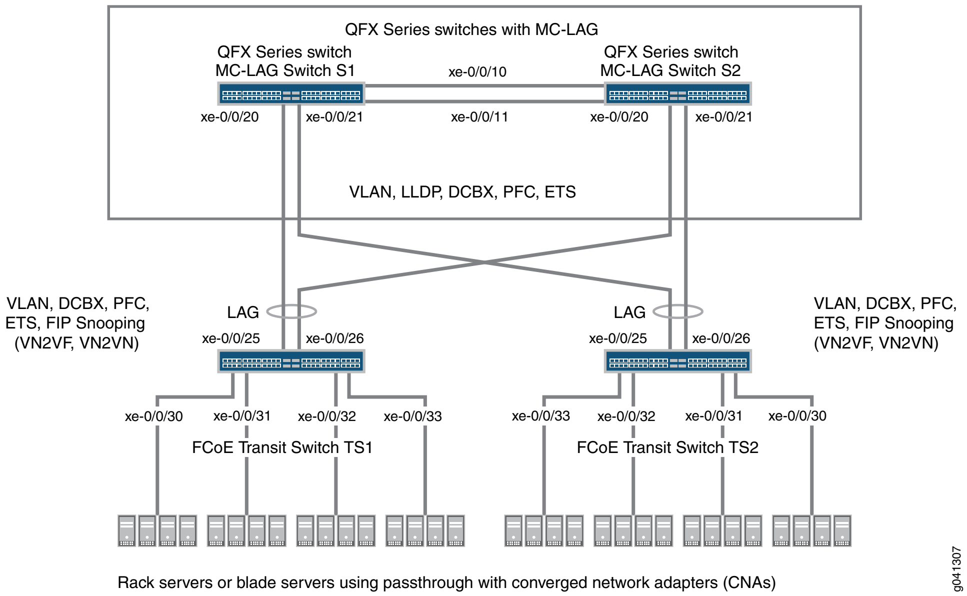
Standalone switches support MC-LAGs. QFabric system Node devices do not support MC-LAGs. Virtual Chassis (VC) and mixed-mode Virtual Chassis Fabric (VCF) configurations do not support FCoE. Only pure QFX5100 VCFs (consisting of only QFX5100 switches) support FCoE.

This topic describes:

Supported Topology

Switches that are not directly connected to FCoE hosts and that act as passthrough transit switches support MC-LAGs for FCoE traffic in an *inverted-U* network topology. Figure 32 on page 310 shows an inverted-U topology using QFX3500 switches.

Figure 32: Supported Topology for an MC-LAG on an FCoE Transit Switch



The following rules and guidelines apply to MC-LAGs when used for FCoE traffic. The rules and guidelines help ensure the proper handling and lossless transport characteristics required for FCoE traffic:

- The two switches that form the MC-LAG (Switches S1 and S2) cannot use ports that are part of an FCoE-FC gateway fabric. The MC-LAG switch ports must be passthrough transit switch ports (used as part of an intermediate transit switch that is not directly connected to FCoE hosts).
- MC-LAG Switches S1 and S2 cannot be not directly connected to the FCoE hosts.
- The two switches that serve as access devices for FCoE hosts (FCoE Transit Switches TS1 and TS2) use standard LAGs to connect to MC-LAG Switches S1 and S2. FCoE Transit Switches TS1 and TS2 can be standalone switches or they can be Node devices in a QFabric system.
- Transit Switches TS1 and TS2 must use transit switch ports for the FCoE hosts and for the standard LAGs to MC-LAG Switches S1 and S2.
- Enable FIP snooping on the FCoE VLAN on Transit Switches TS1 and TS2. You can configure either VN_Port to VF_Port (VN2VF_Port) FIP snooping or VN_Port to VN_Port (VN2VN_Port) FIP snooping, depending on whether the FCoE hosts need to access targets in the FC SAN (VN2VF_Port FIP snooping) or targets in the Ethernet network (VN2VN_Port FIP snooping).

FIP snooping should be performed at the access edge and is not supported on MC-LAG switches. Do not enable FIP snooping on MC-LAG Switches S1 and S2. (Do not enable FIP snooping on the MC-LAG ports that connect Switches S1 and S2 to Switches TS1 and TS2 or on the LAG ports that connect Switch S1 to S2.)

- The CoS configuration must be consistent on the MC-LAG switches. Because MC-LAGs carry no forwarding class or priority information, each MC-LAG switch needs to have the same CoS configuration to support lossless transport. (On each MC-LAG switch, the name, egress queue, and CoS provisioning of each forwarding class must be the same, and the priority-based flow control (PFC) configuration must be the same.)

Transit Switches (Server Access)

The role of FCoE Transit Switches TS1 and TS2 is to connect FCoE hosts in a multihomed fashion to the MC-LAG switches. In essence, Transit Switches TS1 and TS2 act as access switches for the FCoE hosts. (FCoE hosts are directly connected to Transit Switches TS1 and TS2.)

The transit switch configuration depends on whether you want to do VN2VF_Port FIP snooping or VN2VN_Port FIP snooping, and whether the transit switches also have ports configured as part of an FCoE-FC gateway virtual fabric. Ports that a QFX3500 switch uses in an FCoE-FC gateway virtual fabric cannot be included in the transit switch LAG connection to the MC-LAG switches. (Ports cannot belong to both a transit switch and an FCoE-FC gateway; you must use different ports for each mode of operation.)

MC-LAG Switches (FCoE Aggregation)

The role of MC-LAG Switches S1 and S2 is to provide redundant, load-balanced connections between FCoE transit switches. In essence, MC-LAG Switches S1 and S2 act as aggregation switches. FCoE hosts are not directly connected to the MC-LAG switches.

The MC-LAG switch configuration is the same regardless of which type of FIP snooping that FCoE Transit Switches TS1 and TS2 perform.

FIP Snooping and FCoE Trusted Ports

To maintain secure access, enable VN2VF_Port FIP snooping or VN2VN_Port FIP snooping at the transit switch access ports connected directly to the FCoE hosts. FIP snooping should be performed at the access edge of the network to prevent unauthorized access. For example, in Figure 32 on page 310, you enable FIP snooping on the FCoE VLANs on Transit Switches TS1 and TS2 that include the access ports connected to the FCoE hosts.

Do not enable FIP snooping on the switches used to create the MC-LAG. For example, in Figure 32 on page 310, you would not enable FIP snooping on the FCoE VLANs on Switches S1 and S2.

Configure links between switches as FCoE trusted ports to reduce FIP snooping overhead and ensure that the system performs FIP snooping only at the access edge. In the sample topology, configure the Transit Switch TS1 and TS2 LAG ports connected to the MC-LAG switches as FCoE trusted ports, configure the Switch S1 and S2 MC-LAG ports connected to Switches TS1 and TS2 as FCoE trusted ports, and configure the ports in the LAG that connects Switches S1 to S2 as FCoE trusted ports.

CoS and Data Center Bridging (DCB)

The MC-LAG links do not carry forwarding class or priority information. The following CoS properties must have the same configuration on each MC-LAG switch or on each MC-LAG interface to support lossless transport:

- FCoE forwarding class name—For example, the forwarding class for FCoE traffic could use the default **fcoe** forwarding class on both MC-LAG switches.
- FCoE output queue—For example, the **fcoe** forwarding class could be mapped to queue 3 on both MC-LAG switches (queue 3 is the default mapping for the **fcoe** forwarding class).
- Classifier—The forwarding class for FCoE traffic must be mapped to the same IEEE 802.1p code point on each member interface of the MC-LAG on both MC-LAG switches. For example, the FCoE forwarding class **fcoe** could be mapped to IEEE 802.1p code point **011** (code point **011** is the default mapping for the **fcoe** forwarding class).
- Priority-based flow control (PFC)—PFC must be enabled on the FCoE code point on each MC-LAG switch and applied to each MC-LAG interface using a congestion notification profile.

You must also configure enhanced transmission selection (ETS) on the MC-LAG interfaces to provide sufficient scheduling resources (bandwidth, priority) for lossless transport. The ETS configuration can be different on each MC-LAG switch, as long as enough resources are scheduled to support lossless transport for the expected FCoE traffic.

LLDP and DCBX must be enabled on each MC-LAG member interface (LLDP and DCBX are enabled by default on all interfaces).

NOTE: As with all other FCoE configurations, FCoE traffic requires a dedicated VLAN that carries only FCoE traffic, and IGMP snooping must be disabled on the FCoE VLAN.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Example: Configuring CoS for FCoE Transit Switch Traffic Across an MC-LAG on page 312
- Example: Configuring Multichassis Link Aggregation on page 39

Example: Configuring CoS for FCoE Transit Switch Traffic Across an MC-LAG

Supported Platforms EX4600, QFabric System, QFX Series standalone switches

Multichassis link aggregation groups (MC-LAGs) provide redundancy and load balancing between two switches, multihoming support for client devices such as servers, and a loop-free Layer 2 network without running Spanning Tree Protocol (STP).

NOTE: This example uses Junos OS without support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Example: Configuring CoS for FCoE Transit Switch Traffic Across an MC-LAG*.

You can use an MC-LAG to provide a redundant aggregation layer for Fibre Channel over Ethernet (FCoE) traffic in an *inverted-U* topology. To support lossless transport of FCoE traffic across an MC-LAG, you must configure the appropriate class of service (CoS) on both of the switches with MC-LAG port members. The CoS configuration must be the same on both of the MC-LAG switches because an MC-LAG does not carry forwarding class and IEEE 802.1p priority information.

NOTE: This example describes how to configure CoS to provide lossless transport for FCoE traffic across an MC-LAG that connects two switches. It also describes how to configure CoS on the FCoE transit switches that connect FCoE hosts to the two switches that form the MC-LAG.

This example does *not* describe how to configure the MC-LAG itself. For a detailed example of MC-LAG configuration, see "Example: Configuring Multichassis Link Aggregation" on page 39. However, this example includes a subset of MC-LAG configuration that only shows how to configure interface membership in the MC-LAG.

Ports that are part of an FCoE-FC gateway configuration (a virtual FCoE-FC gateway fabric) do not support MC-LAGs. Ports that are members of an MC-LAG act as FCoE passthrough transit switch ports.

QFX Series switches and EX4600 switches support MC-LAGs. QFabric system Node devices do not support MC-LAGs.

This topic describes:

Requirements

This example uses the following hardware and software components:

- Two Juniper Networks QFX3500 Switches that form an MC-LAG for FCoE traffic.
- Two Juniper Networks QFX3500 Switches that provide FCoE server access in transit switch mode and that connect to the MC-LAG switches. These switches can be standalone QFX3500 switches or they can be Node devices in a QFabric system.

- FCoE servers (or other FCoE hosts) connected to the transit switches.
- Junos OS Release 12.2 or later for the QFX Series.

Overview

FCoE traffic requires lossless transport. This example shows you how to:

- Configure CoS for FCoE traffic on the two QFX3500 switches that form the MC-LAG, including priority-based flow control (PFC) and enhanced transmission selection (ETS; hierarchical scheduling of resources for the FCoE forwarding class priority and for the forwarding class set priority group).

  NOTE: **Configuring or changing PFC on an interface blocks the entire port until the PFC change is completed. After a PFC change is completed, the port is unblocked and traffic resumes. Blocking the port stops ingress and egress traffic, and causes packet loss on all queues on the port until the port is unblocked.**

- Configure CoS for FCoE on the two FCoE transit switches that connect FCoE hosts to the MC-LAG switches and enable FIP snooping on the FCoE VLAN at the FCoE transit switch access ports.
- Disable IGMP snooping on the FCoE VLAN.

  NOTE: **This is only necessary if IGMP snooping is enabled on the VLAN. Before Junos OS Release 13.2, IGMP snooping was enabled by default on VLANs. Beginning with Junos OS Release 13.2, IGMP snooping is enabled by default only on the default VLAN.**

- Configure the appropriate port mode, MTU, and FCoE trusted or untrusted state for each interface to support lossless FCoE transport.

Topology

Switches that act as transit switches support MC-LAGs for FCoE traffic in an inverted-U network topology, as shown in Figure 33 on page 315.

Figure 33: Supported Topology for an MC-LAG on an FCoE Transit Switch

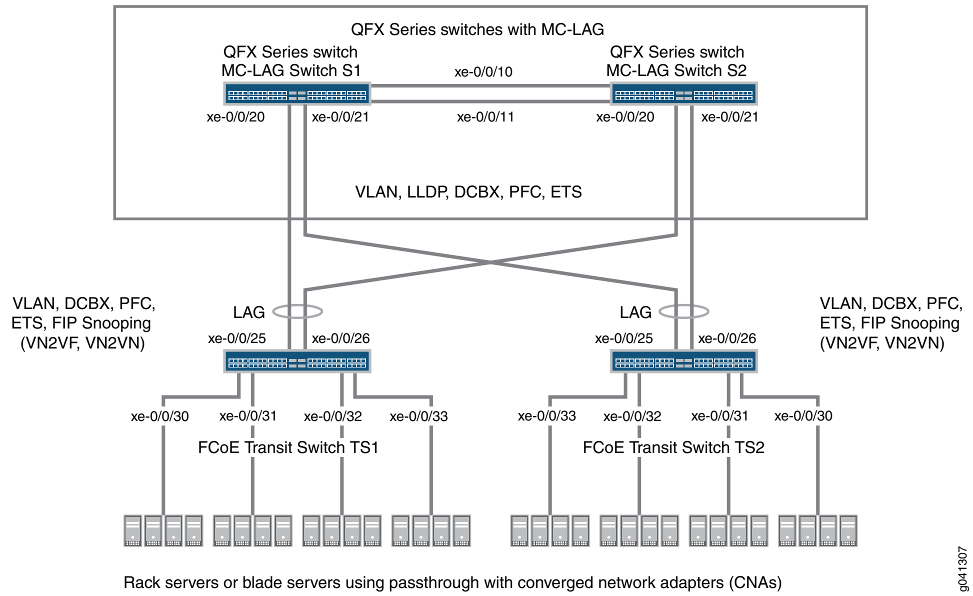


Table 16 on page 315 shows the configuration components for this example.

Table 16: Components of the CoS for FCoE Traffic Across an MC-LAG Configuration Topology

Component	Settings
Hardware	Four QFX3500 switches (two to form the MC-LAG as passthrough transit switches and two transit switches for FCoE access).
Forwarding class (all switches)	Default **fcoe** forwarding class.
Classifier (forwarding class mapping of incoming traffic to IEEE priority)	Default IEEE 802.1p trusted classifier on all FCoE interfaces.

Table 16: Components of the CoS for FCoE Traffic Across an MC-LAG Configuration Topology *(continued)*

Component	Settings
LAGs and MC-LAG	S1—Ports xe-0/0/10 and x-0/0/11 are members of LAG **ae0**, which connects Switch S1 to Switch S2. Ports xe-0/0/20 and xe-0/0/21 are members of MC-LAG **ae1**. All ports are configured in **trunk** port mode, as **fcoe-trusted**, and with an MTU of **2180**. S2—Ports xe-0/0/10 and x-0/0/11 are members of LAG **ae0**, which connects Switch S2 to Switch S1. Ports xe-0/0/20 and xe-0/0/21 are members of MC-LAG **ae1**. All ports are configured in **trunk** port mode, as **fcoe-trusted**, and with an MTU of **2180**. NOTE: Ports xe-0/0/20 and xe-0/0/21 on Switches S1 and S2 are the members of the MC-LAG. TS1—Ports xe-0/0/25 and x-0/0/26 are members of LAG **ae1**, configured in **trunk** port mode, as **fcoe-trusted**, and with an MTU of **2180**. Ports xe-0/0/30, xe-0/0/31, xe-0/0/32, and xe-0/0/33 are configured in **tagged-access** port mode, with an MTU of **2180**. TS2—Ports xe-0/0/25 and x-0/0/26 are members of LAG **ae1**, configured in **trunk** port mode, as **fcoe-trusted**, and with an MTU of **2180**. Ports xe-0/0/30, xe-0/0/31, xe-0/0/32, and xe-0/0/33 are configured in **tagged-access** port mode, with an MTU of **2180**.
FCoE queue scheduler (all switches)	**fcoe-sched**: Minimum bandwidth **3g** Maximum bandwidth **100%** Priority **low**
Forwarding class-to-scheduler mapping (all switches)	Scheduler map **fcoe-map**: Forwarding class **fcoe** Scheduler **fcoe-sched**
Forwarding class set (FCoE priority group, all switches)	**fcoe-pg**: Forwarding class **fcoe** Egress interfaces: • S1—LAG **ae0** and MC-LAG **ae1** • S2—LAG **ae0** and MC-LAG **ae1** • TS1—LAG **ae1**, interfaces **xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, and **xe-0/0/33** • TS2—LAG **ae1**, interfaces **xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, and **xe-0/0/33**
Traffic control profile (all switches)	**fcoe-tcp**: Scheduler map **fcoe-map** Minimum bandwidth **3g** Maximum bandwidth **100%**

Table 16: Components of the CoS for FCoE Traffic Across an MC-LAG Configuration Topology *(continued)*

Component	Settings
PFC congestion notification profile (all switches)	**fcoe-cnp**: Code point **011** Ingress interfaces: • S1—LAG **ae0** and MC-LAG **ae1** • S2—LAG **ae0** and MC-LAG **ae1** • TS1—LAG **ae1**, interfaces **xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, and **xe-0/0/33** • TS2—LAG **ae1**, interfaces **xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, and **xe-0/0/33**
FCoE VLAN name and tag ID	Name—**fcoe_vlan** ID—**100** Include the FCoE VLAN on the interfaces that carry FCoE traffic on all four switches. Disable IGMP snooping on the interfaces that belong to the FCoE VLAN on all four switches.
FIP snooping	Enable FIP snooping on Transit Switches TS1 and TS2 on the FCoE VLAN. Configure the LAG interfaces that connect to the MC-LAG switches as FCoE trusted interfaces so that they do not perform FIP snooping. This example enables VN2VN_Port FIP snooping on the FCoE transit switch interfaces connected to the FCoE servers. The example is equally valid with VN2VF_Port FIP snooping enabled on the transit switch access ports. The method of FIP snooping you enable depends on your network configuration.

NOTE: This example uses the default IEEE 802.1p trusted BA classifier, which is automatically applied to trunk mode and tagged access mode ports if you do not apply an explicitly configured classifier.

To configure CoS for FCoE traffic across an MC-LAG:

- Use the default FCoE forwarding class and forwarding-class-to-queue mapping (do not explicitly configure the FCoE forwarding class or output queue). The default FCoE forwarding class is **fcoe**, and the default output queue is queue **3**.

  NOTE: In Junos OS Release 12.2, traffic mapped to explicitly configured forwarding classes, even lossless forwarding classes such as fcoe, is treated as lossy (best-effort) traffic and does *not* receive lossless treatment. To receive lossless treatment in Release 12.2, traffic must use one of the default lossless forwarding classes (fcoe or no-loss).

  In Junos OS Release 12.3 and later, you can include the *no-loss* packet drop attribute in the explicit forwarding class configuration to configure a lossless forwarding class.

- Use the default trusted BA classifier, which maps incoming packets to forwarding classes by the IEEE 802.1p code point (CoS priority) of the packet. The trusted classifier is the default classifier for interfaces in trunk and tagged-access port modes. The default trusted classifier maps incoming packets with the IEEE 802.1p code point 3 (**011**) to the FCoE forwarding class. If you choose to configure the BA classifier instead of using the default classifier, you must ensure that FCoE traffic is classified into forwarding classes in exactly the same way on both MC-LAG switches. Using the default classifier ensures consistent classifier configuration on the MC-LAG ports.
- Configure a congestion notification profile that enables PFC on the FCoE code point (code point **011** in this example). The congestion notification profile configuration must be the same on both MC-LAG switches.
- Apply the congestion notification profile to the interfaces.
- Configure enhanced transmission selection (ETS, also known as hierarchical scheduling) on the interfaces to provide the bandwidth required for lossless FCoE transport. Configuring ETS includes configuring bandwidth scheduling for the FCoE forwarding class, a forwarding class set (priority group) that includes the FCoE forwarding class, and a traffic control profile to assign bandwidth to the forwarding class set that includes FCoE traffic.
- Apply the ETS scheduling to the interfaces.
- Configure the port mode, MTU, and FCoE trusted or untrusted state for each interface to support lossless FCoE transport.

In addition, this example describes how to enable FIP snooping on the Transit Switch TS1 and TS2 ports that are connected to the FCoE servers and how to disable IGMP snooping on the FCoE VLAN. To provide secure access, FIP snooping must be enabled on the FCoE access ports.

This example focuses on the CoS configuration to support lossless FCoE transport across an MC-LAG. This example does not describe how to configure the properties of MC-LAGs and LAGs, although it does show you how to configure the port characteristics required to support lossless transport and how to assign interfaces to the MC-LAG and to the LAGs.

Before you configure CoS, configure:

- The MC-LAGs that connect Switches S1 and S2 to Switches TS1 and TS2. ("Example: Configuring Multichassis Link Aggregation" on page 39 describes how to configure MC-LAGs.)
- The LAGs that connect the Transit Switches TS1 and TS2 to MC-LAG Switches S1 and S2. (*Configuring Link Aggregation* describes how to configure LAGs.)
- The LAG that connects Switch S1 to Switch S2.

Configuration

To configure CoS for lossless FCoE transport across an MC-LAG, perform these tasks:

CLI Quick Configuration

To quickly configure CoS for lossless FCoE transport across an MC-LAG, copy the following commands, paste them in a text file, remove line breaks, change variables and details to match your network configuration, and then copy and paste the commands into the CLI for MC-LAG Switch S1 and MC-LAG Switch S2 at the **[edit]** hierarchy level. The configurations on Switches S1 and S2 are identical because the CoS configuration must be identical, and because this example uses the same ports on both switches.

Switch S1 and Switch S2

```
set class-of-service schedulers fcoe-sched priority low transmit-rate 3g
set class-of-service schedulers fcoe-sched shaping-rate percent 100
set class-of-service scheduler-maps fcoe-map forwarding-class fcoe scheduler fcoe-sched
set class-of-service forwarding-class-sets fcoe-pg class fcoe
set class-of-service traffic-control-profiles fcoe-tcp scheduler-map fcoe-map guaranteed-rate
3g
set class-of-service traffic-control-profiles fcoe-tcp shaping-rate percent 100
set class-of-service interfaces ae0 forwarding-class-set fcoe-pg output-traffic-control-profile
fcoe-tcp
set class-of-service interfaces ae1 forwarding-class-set fcoe-pg output-traffic-control-profile
fcoe-tcp
set class-of-service congestion-notification-profile fcoe-cnp input ieee-802.1 code-point 011 pfc
set class-of-service interfaces ae0 congestion-notification-profile fcoe-cnp
set class-of-service interfaces ae1 congestion-notification-profile fcoe-cnp
set vlans fcoe_vlan vlan-id 100
set protocols igmp-snooping vlan fcoe_vlan disable
set interfaces xe-0/0/10 ether-options 802.3ad ae0
set interfaces xe-0/0/11 ether-options 802.3ad ae0
set interfaces xe-0/0/20 ether-options 802.3ad ae1
set interfaces xe-0/0/21 ether-options 802.3ad ae1
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
set interfaces ae0 mtu 2180
set interfaces ae1 mtu 2180
```

```
set ethernet-switching-options secure-access-port interface ae0 fcoe-trusted
set ethernet-switching-options secure-access-port interface ae1 fcoe-trusted
```

To quickly configure CoS for lossless FCoE transport across an MC-LAG, copy the following commands, paste them in a text file, remove line breaks, change variables and details to match your network configuration, and then copy and paste the commands into the CLI for Transit Switch TS1 and Transit Switch TS2 at the **[edit]** hierarchy level. The configurations on Switches TS1 and TS2 are identical because the CoS configuration must be identical, and because this example uses the same ports on both switches.

Switch TS1 and Switch TS2

```
set class-of-service schedulers fcoe-sched priority low transmit-rate 3g
set class-of-service schedulers fcoe-sched shaping-rate percent 100
set class-of-service scheduler-maps fcoe-map forwarding-class fcoe scheduler fcoe-sched
set class-of-service forwarding-class-sets fcoe-pg class fcoe
set class-of-service traffic-control-profiles fcoe-tcp scheduler-map fcoe-map guaranteed-rate
3g
set class-of-service traffic-control-profiles fcoe-tcp shaping-rate percent 100
set class-of-service interfaces ae1 forwarding-class-set fcoe-pg output-traffic-control-profile
fcoe-tcp
set class-of-service interfaces xe-0/0/30 forwarding-class-set fcoe-pg
output-traffic-control-profile fcoe-tcp
set class-of-service interfaces xe-0/0/31 forwarding-class-set fcoe-pg
output-traffic-control-profile fcoe-tcp
set class-of-service interfaces xe-0/0/32 forwarding-class-set fcoe-pg
output-traffic-control-profile fcoe-tcp
set class-of-service interfaces xe-0/0/33 forwarding-class-set fcoe-pg
output-traffic-control-profile fcoe-tcp
set class-of-service congestion-notification-profile fcoe-cnp input ieee-802.1 code-point 011 pfc
set class-of-service interfaces ae1 congestion-notification-profile fcoe-cnp
set class-of-service interfaces xe-0/0/30 congestion-notification-profile fcoe-cnp
set class-of-service interfaces xe-0/0/31 congestion-notification-profile fcoe-cnp
set class-of-service interfaces xe-0/0/32 congestion-notification-profile fcoe-cnp
set class-of-service interfaces xe-0/0/33 congestion-notification-profile fcoe-cnp
set vlans fcoe_vlan vlan-id 100
set protocols igmp-snooping vlan fcoe_vlan disable
set interfaces xe-0/0/25 ether-options 802.3ad ae1
set interfaces xe-0/0/26 ether-options 802.3ad ae1
set interfaces ae1 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
set interfaces xe-0/0/30 unit 0 family ethernet-switching port-mode tagged-access vlan members
fcoe_vlan
set interfaces xe-0/0/31 unit 0 family ethernet-switching port-mode tagged-access vlan members
fcoe_vlan
set interfaces xe-0/0/32 unit 0 family ethernet-switching port-mode tagged-access vlan members
fcoe_vlan
set interfaces xe-0/0/33 unit 0 family ethernet-switching port-mode tagged-access vlan members
fcoe_vlan
set interfaces ae1 mtu 2180
set interfaces xe-0/0/30 mtu 2180
set interfaces xe-0/0/31 mtu 2180
set interfaces xe-0/0/32 mtu 2180
set interfaces xe-0/0/33 mtu 2180
set ethernet-switching-options secure-access-port interface ae1 fcoe-trusted
set ethernet-switching-options secure-access-port vlan fcoe_vlan examine-fip examine-vn2v2
beacon-period 90000
```


Configuring MC-LAG Switches S1 and S2

Step-by-Step Procedure

To configure CoS resource scheduling (ETS), PFC, the FCoE VLAN, and the LAG and MC-LAG interface membership and characteristics to support lossless FCoE transport across an MC-LAG (this example uses the default **fcoe** forwarding class and the default classifier to map incoming FCoE traffic to the FCoE IEEE 802.1p code point **011**, so you do not configure them):

1. Configure output scheduling for the FCoE queue:

```
[edit class-of-service]
user@switch# set schedulers fcoe-sched priority low transmit-rate 3g
user@switch# set schedulers fcoe-sched shaping-rate percent 100
```

2. Map the FCoE forwarding class to the FCoE scheduler (**fcoe-sched**):

```
[edit class-of-service]
user@switch# set scheduler-maps fcoe-map forwarding-class fcoe scheduler fcoe-sched
```

3. Configure the forwarding class set (**fcoe-pg**) for the FCoE traffic:

```
[edit class-of-service]
user@switch# set forwarding-class-sets fcoe-pg class fcoe
```

4. Define the traffic control profile (**fcoe-tcp**) to use on the FCoE forwarding class set:

```
[edit class-of-service]
user@switch# set traffic-control-profiles fcoe-tcp scheduler-map fcoe-map
guaranteed-rate 3g
user@switch# set traffic-control-profiles fcoe-tcp shaping-rate percent 100
```

5. Apply the FCoE forwarding class set and traffic control profile to the LAG and MC-LAG interfaces:

```
[edit class-of-service]
user@switch# set interfaces ae0 forwarding-class-set fcoe-pg output-traffic-control-profile
fcoe-tcp
user@switch# set interfaces ae1 forwarding-class-set fcoe-pg output-traffic-control-profile
fcoe-tcp
```

6. Enable PFC on the FCoE priority by creating a congestion notification profile (**fcoe-cnp**) that applies FCoE to the IEEE 802.1 code point **011**:

```
[edit class-of-service]
user@switch# set congestion-notification-profile fcoe-cnp input ieee-802.1 code-point
011 pfc
```

7. Apply the PFC configuration to the LAG and MC-LAG interfaces:

```
[edit class-of-service]
user@switch# set interfaces ae0 congestion-notification-profile fcoe-cnp
user@switch# set interfaces ae1 congestion-notification-profile fcoe-cnp
```

8. Configure the VLAN for FCoE traffic (**fcoe_vlan**):

```
[edit vlans]
user@switch# set fcoe_vlan vlan-id 100
```

9. Disable IGMP snooping on the FCoE VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan fcoe_vlan disable
```

10. Add the member interfaces to the LAG between the two MC-LAG switches:

    ```
    [edit interfaces]
    user@switch# set xe-0/0/10 ether-options 802.3ad ae0
    user@switch# set xe-0/0/11 ether-options 802.3ad ae0
    ```

11. Add the member interfaces to the MC-LAG:

    ```
    [edit interfaces]
    user@switch# set xe-0/0/20 ether-options 802.3ad ae1
    user@switch# set xe-0/0/21 ether-options 802.3ad ae1
    ```

12. Configure the port mode as **trunk** and membership in the FCoE VLAN (**fcoe_vlan**) for the LAG (**ae0**) and for the MC-LAG (**ae1**):

    ```
    [edit interfaces]
    user@switch# set interfaces ae0 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
    user@switch# set interfaces ae1 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
    ```

13. Set the MTU to **2180** for the LAG and MC-LAG interfaces. 2180 bytes is the minimum size required to handle FCoE packets because of the payload and header sizes; you can configure the MTU to a higher number of bytes if desired, but not less than 2180 bytes:

    ```
    [edit interfaces]
    user@switch# set ae0 mtu 2180
    user@switch# set ae1 mtu 2180
    ```

14. Set the LAG and MC-LAG interfaces as FCoE trusted ports. Ports that connect to other switches should be trusted and should not perform FIP snooping:

    ```
    [edit]
    user@switch# set ethernet-switching-options secure-access-port interface ae0 fcoe-trusted
    user@switch# set ethernet-switching-options secure-access-port interface ae1 fcoe-trusted
    ```

Configuring FCoE Transit Switches TS1 and TS2

Step-by-Step Procedure

The CoS configuration on FCoE Transit Switches TS1 and TS2 is similar to the CoS configuration on MC-LAG Switches S1 and S2. However, the port configurations differ, and you must enable FIP snooping on the Switch TS1 and Switch TS2 FCoE access ports.

To configure resource scheduling (ETS), PFC, the FCoE VLAN, and the LAG interface membership and characteristics to support lossless FCoE transport across the MC-LAG (this example uses the default **fcoe** forwarding class and the default classifier to map incoming FCoE traffic to the FCoE IEEE 802.1p code point **011**, so you do not configure them):

1. Configure output scheduling for the FCoE queue:

    ```
    [edit class-of-service]
    user@switch# set schedulers fcoe-sched priority low transmit-rate 3g
    user@switch# set schedulers fcoe-sched shaping-rate percent 100
    ```

2. Map the FCoE forwarding class to the FCoE scheduler (**fcoe-sched**):

    ```
    [edit class-of-service]
    user@switch# set scheduler-maps fcoe-map forwarding-class fcoe scheduler fcoe-sched
    ```

3. Configure the forwarding class set (**fcoe-pg**) for the FCoE traffic:


```
[edit class-of-service]
user@switch# set forwarding-class-sets fcoe-pg class fcoe
```

4. Define the traffic control profile (**fcoe-tcp**) to use on the FCoE forwarding class set:

```
[edit class-of-service]
user@switch# set traffic-control-profiles fcoe-tcp scheduler-map fcoe-map guaranteed-rate 3g
user@switch# set traffic-control-profiles fcoe-tcp shaping-rate percent 100
```

5. Apply the FCoE forwarding class set and traffic control profile to the LAG interface and to the FCoE access interfaces:

```
[edit class-of-service]
user@switch# set interfaces ae1 forwarding-class-set fcoe-pg output-traffic-control-profile fcoe-tcp
user@switch# set class-of-service interfaces xe-0/0/30 forwarding-class-set fcoe-pg output-traffic-control-profile fcoe-tcp
user@switch# set class-of-service interfaces xe-0/0/31 forwarding-class-set fcoe-pg output-traffic-control-profile fcoe-tcp
user@switch# set class-of-service interfaces xe-0/0/32 forwarding-class-set fcoe-pg output-traffic-control-profile fcoe-tcp
user@switch# set class-of-service interfaces xe-0/0/33 forwarding-class-set fcoe-pg output-traffic-control-profile fcoe-tcp
```

6. Enable PFC on the FCoE priority by creating a congestion notification profile (**fcoe-cnp**) that applies FCoE to the IEEE 802.1 code point **011**:

```
[edit class-of-service]
user@switch# set congestion-notification-profile fcoe-cnp input ieee-802.1 code-point 011 pfc
```

7. Apply the PFC configuration to the LAG interface and to the FCoE access interfaces:

```
[edit class-of-service]
user@switch# set interfaces ae1 congestion-notification-profile fcoe-cnp
user@switch# set class-of-service interfaces xe-0/0/30 congestion-notification-profile fcoe-cnp
user@switch# set class-of-service interfaces xe-0/0/31 congestion-notification-profile fcoe-cnp
user@switch# set class-of-service interfaces xe-0/0/32 congestion-notification-profile fcoe-cnp
user@switch# set class-of-service interfaces xe-0/0/33 congestion-notification-profile fcoe-cnp
```

8. Configure the VLAN for FCoE traffic (**fcoe_vlan**):

```
[edit vlans]
user@switch# set fcoe_vlan vlan-id 100
```

9. Disable IGMP snooping on the FCoE VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan fcoe_vlan disable
```

10. Add the member interfaces to the LAG:

```
[edit interfaces]
user@switch# set xe-0/0/25 ether-options 802.3ad ae1
user@switch# set xe-0/0/26 ether-options 802.3ad ae1
```

11. On the LAG (**ae1**), configure the port mode as **trunk** and membership in the FCoE VLAN (**fcoe_vlan**):

```
[edit interfaces]
user@switch# set interfaces ae1 unit 0 family ethernet-switching port-mode trunk vlan members fcoe_vlan
```

12. On the FCoE access interfaces (**xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, **xe-0/0/33**), configure the port mode as **tagged-access** and membership in the FCoE VLAN (**fcoe_vlan**):

```
[edit interfaces]
user@switch# set interfaces xe-0/0/30 unit 0 family ethernet-switching port-mode tagged-access vlan members fcoe_vlan
user@switch# set interfaces xe-0/0/31 unit 0 family ethernet-switching port-mode tagged-access vlan members fcoe_vlan
user@switch# set interfaces xe-0/0/32 unit 0 family ethernet-switching port-mode tagged-access vlan members fcoe_vlan
user@switch# set interfaces xe-0/0/33 unit 0 family ethernet-switching port-mode tagged-access vlan members fcoe_vlan
```

13. Set the MTU to **2180** for the LAG and FCoE access interfaces. 2180 bytes is the minimum size required to handle FCoE packets because of the payload and header sizes; you can configure the MTU to a higher number of bytes if desired, but not less than 2180 bytes:

```
[edit interfaces]
user@switch# set ae1 mtu 2180
user@switch# set xe-0/0/30 mtu 2180
user@switch# set xe-0/0/31 mtu 2180
user@switch# set xe-0/0/32 mtu 2180
user@switch# set xe-0/0/33 mtu 2180
```

14. Set the LAG interface as an FCoE trusted port. Ports that connect to other switches should be trusted and should not perform FIP snooping:

```
[edit]
user@switch# set ethernet-switching-options secure-access-port interface ae1 fcoe-trusted
```

NOTE: Access ports xe-0/0/30, xe-0/0/31, xe-0/0/32, and xe-0/0/33 are not configured as FCoE trusted ports. The access ports remain in the default state as untrusted ports because they connect directly to FCoE devices and must perform FIP snooping to ensure network security.

15. Enable FIP snooping on the FCoE VLAN to prevent unauthorized FCoE network access (this example uses VN2VN_Port FIP snooping; the example is equally valid if you use VN2VF_Port FIP snooping):

```
[edit]
user@switch# set ethernet-switching-options secure-access-port vlan fcoe_vlan examine-fip examine-vn2vn beacon-period 90000
```

Results

Display the results of the CoS configuration on MC-LAG Switch S1 and on MC-LAG Switch S2 (the results on both switches are the same):

```
user@switch> show configuration class-of-service
```



```
traffic-control-profiles {
   fcoe-tcp {
      scheduler-map fcoe-map;
      shaping-rate percent 100;
      guaranteed-rate 3000000000;
   }
}
forwarding-class-sets {
   fcoe-pg {
      class fcoe;
   }
}
congestion-notification-profile {
   fcoe-cnp {
      input {
         ieee-802.1 {
            code-point 011 {
               pfc;
            }
         }
      }
   }
}
interfaces {
   ae0 {
      forwarding-class-set {
         fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
         }
      }
      congestion-notification-profile fcoe-cnp;
   }
   ae1 {
      forwarding-class-set {
         fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
         }
      }
      congestion-notification-profile fcoe-cnp;
   }
}
scheduler-maps {
   fcoe-map {
      forwarding-class fcoe scheduler fcoe-sched;
   }
}
schedulers {
   fcoe-sched {
      transmit-rate 3000000000;
      shaping-rate percent 100;
      priority low;
   }
}
```

NOTE: The forwarding class and classifier configurations are not shown because the show command does not display default portions of the configuration.

For MC-LAG verification commands, see "Example: Configuring Multichassis Link Aggregation" on page 39.

Display the results of the CoS configuration on FCoE Transit Switch TS1 and on FCoE Transit Switch TS2 (the results on both transit switches are the same):

```
user@switch> show configuration class-of-service
traffic-control-profiles {
  fcoe-tcp {
    scheduler-map fcoe-map;
    shaping-rate percent 100;
    guaranteed-rate 3000000000;
  }
}
forwarding-class-sets {
  fcoe-pg {
    class fcoe;
  }
}
congestion-notification-profile {
  fcoe-cnp {
    input {
      ieee-802.1 {
        code-point 011 {
          pfc;
        }
      }
    }
  }
}
interfaces {
  xe-0/0/30 {
    forwarding-class-set {
      fcoe-pg {
        output-traffic-control-profile fcoe-tcp;
      }
    }
    congestion-notification-profile fcoe-cnp;
  }
  xe-0/0/31 {
    forwarding-class-set {
      fcoe-pg {
        output-traffic-control-profile fcoe-tcp;
      }
    }
    congestion-notification-profile fcoe-cnp;
  }
  xe-0/0/32 {
```



```
        forwarding-class-set {
            fcoe-pg {
                output-traffic-control-profile fcoe-tcp;
            }
        }
        congestion-notification-profile fcoe-cnp;
    }
    xe-0/0/33 {
        forwarding-class-set {
            fcoe-pg {
                output-traffic-control-profile fcoe-tcp;
            }
        }
        congestion-notification-profile fcoe-cnp;
    }
    ae1 {
        forwarding-class-set {
            fcoe-pg {
                output-traffic-control-profile fcoe-tcp;
            }
        }
        congestion-notification-profile fcoe-cnp;
    }
}
scheduler-maps {
    fcoe-map {
        forwarding-class fcoe scheduler fcoe-sched;
    }
}
schedulers {
    fcoe-sched {
        transmit-rate 3000000000;
        shaping-rate percent 100;
        priority low;
    }
}
```

NOTE: The forwarding class and classifier configurations are not shown because the show command does not display default portions of the configuration.

Verification

To verify that the CoS components and FIP snooping have been configured and are operating properly, perform these tasks. Because this example uses the default **fcoe** forwarding class and the default IEEE 802.1p trusted classifier, the verification of those configurations is not shown:

- Verifying That the Output Queue Schedulers Have Been Created on page 328
- Verifying That the Priority Group Output Scheduler (Traffic Control Profile) Has Been Created on page 329

Verifying That the Output Queue Schedulers Have Been Created

Purpose Verify that the output queue scheduler for FCoE traffic has the correct bandwidth parameters and priorities, and is mapped to the correct forwarding class (output queue). Queue scheduler verification is the same on each of the four switches.

Action List the scheduler map using the operational mode command **show class-of-service scheduler-map fcoe-map**:

```
user@switch> show class-of-service scheduler-map fcoe-map
Scheduler map: fcoe-map, Index: 9023

  Scheduler: fcoe-sched, Forwarding class: fcoe, Index: 37289
    Transmit rate: 3000000000 bps, Rate Limit: none, Buffer size: remainder,
    Buffer Limit: none, Priority: low
    Excess Priority: unspecified
    Shaping rate: 100 percent,
    drop-profile-map-set-type: mark
    Drop profiles:
      Loss priority   Protocol    Index    Name
      Low             any             1    <default-drop-profile>
      Medium high     any             1    <default-drop-profile>
      High            any             1    <default-drop-profile>
```

Meaning The **show class-of-service scheduler-map fcoe-map** command lists the properties of the scheduler map **fcoe-map**. The command output includes:

- The name of the scheduler map (**fcoe-map**)
- The name of the scheduler (**fcoe-sched**)
- The forwarding classes mapped to the scheduler (**fcoe**)
- The minimum guaranteed queue bandwidth (transmit rate **3000000000 bps**)
- The scheduling priority (**low**)
- The maximum bandwidth in the priority group the queue can consume (shaping rate **100 percent**)
- The drop profile loss priority for each drop profile name. This example does not include drop profiles because you do not apply drop profiles to FCoE traffic.

Verifying That the Priority Group Output Scheduler (Traffic Control Profile) Has Been Created

Purpose Verify that the traffic control profile **fcoe-tcp** has been created with the correct bandwidth parameters and scheduler mapping. Priority group scheduler verification is the same on each of the four switches.

Action List the FCoE traffic control profile properties using the operational mode command **show class-of-service traffic-control-profile fcoe-tcp**:

```
user@switch> show class-of-service traffic-control-profile fcoe-tcp
Traffic control profile: fcoe-tcp, Index: 18303
  Shaping rate: 100 percent
  Scheduler map: fcoe-map
  Guaranteed rate: 3000000000
```

Meaning The **show class-of-service traffic-control-profile fcoe-tcp** command lists all of the configured traffic control profiles. For each traffic control profile, the command output includes:

- The name of the traffic control profile (**fcoe-tcp**)
- The maximum port bandwidth the priority group can consume (shaping rate **100 percent**)
- The scheduler map associated with the traffic control profile (**fcoe-map**)
- The minimum guaranteed priority group port bandwidth (guaranteed rate **3000000000** in bps)

Verifying That the Forwarding Class Set (Priority Group) Has Been Created

Purpose Verify that the FCoE priority group has been created and that the **fcoe** priority (forwarding class) belongs to the FCoE priority group. Forwarding class set verification is the same on each of the four switches.

Action List the forwarding class sets using the operational mode command **show class-of-service forwarding-class-set fcoe-pg**:

```
user@switch> show class-of-service forwarding-class-set fcoe-pg
Forwarding class set: fcoe-pg, Type: normal-type, Forwarding class set index:
31420
  Forwarding class                       Index
  fcoe                                     1
```

Meaning The **show class-of-service forwarding-class-set fcoe-pg** command lists all of the forwarding classes (priorities) that belong to the **fcoe-pg** priority group, and the internal index number of the priority group. The command output shows that the forwarding class set **fcoe-pg** includes the forwarding class **fcoe**.

Verifying That Priority-Based Flow Control Has Been Enabled

Purpose Verify that PFC is enabled on the FCoE code point. PFC verification is the same on each of the four switches.

Action List the FCoE congestion notification profile using the operational mode command **show class-of-service congestion-notification fcoe-cnp**:

```
user@switch> show class-of-service congestion-notification fcoe-cnp
Type: Input, Name: fcoe-cnp, Index: 6879
Cable Length: 100 m
  Priority      PFC          MRU
  000           Disabled
  001           Disabled
  010           Disabled
  011           Enabled      2500
  100           Disabled
  101           Disabled
  110           Disabled
  111           Disabled
Type: Output
  Priority      Flow-Control-Queues
  000
                0
  001
                1
  010
                2
  011
                3
  100
                4
  101
                5
  110
                6
  111
                7
```

Meaning The **show class-of-service congestion-notification fcoe-cnp** command lists all of the IEEE 802.1p code points in the congestion notification profile that have PFC enabled. The command output shows that PFC is enabled on code point **011** (**fcoe** queue) for the **fcoe-cnp** congestion notification profile.

The command also shows the default cable length (100 meters), the default maximum receive unit (2500 bytes), and the default mapping of priorities to output queues because this example does not include configuring these options.

Verifying That the Interface Class of Service Configuration Has Been Created

Purpose Verify that the CoS properties of the interfaces are correct. The verification output on MC-LAG Switches S1 and S2 differs from the output on FCoE Transit Switches TS1 and TS2.

Action List the interface CoS configuration on MC-LAG Switches S1 and S2 using the operational mode command **show configuration class-of-service interfaces**:

```
user@switch> show configuration class-of-service interfaces
ae0 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}

ae1 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
```

List the interface CoS configuration on FCoE Transit Switches TS1 and TS2 using the operational mode command **show configuration class-of-service interfaces**:

```
user@switch> show configuration class-of-service interfaces
xe-0/0/30 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
xe-0/0/31 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
xe-0/0/32 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
xe-0/0/33 {
    forwarding-class-set {
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
ae1 {
    forwarding-class-set {
```

```
        fcoe-pg {
            output-traffic-control-profile fcoe-tcp;
        }
    }
    congestion-notification-profile fcoe-cnp;
}
```

Meaning The **show configuration class-of-service interfaces** command lists the class of service configuration for all interfaces. For each interface, the command output includes:

- The name of the interface (for example, **ae0** or **xe-0/0/30**)
- The name of the forwarding class set associated with the interface (**fcoe-pg**)
- The name of the traffic control profile associated with the interface (output traffic control profile, **fcoe-tcp**)
- The name of the congestion notification profile associated with the interface (**fcoe-cnp**)

NOTE: Interfaces that are members of a LAG are not shown individually. The LAG or MC-LAG CoS configuration is applied to all interfaces that are members of the LAG or MC-LAG. For example, the interface CoS configuration output on MC-LAG Switches S1 and S2 shows the LAG CoS configuration but does not show the CoS configuration of the member interfaces separately. The interface CoS configuration output on FCoE Transit Switches TS1 and TS2 shows the LAG CoS configuration but also shows the configuration for interfaces xe-0/0/30, xe-0/0/31, xe-0/0/32, and xe-0/0/33, which are not members of a LAG.

Verifying That the Interfaces Are Correctly Configured

Purpose Verify that the LAG membership, MTU, VLAN membership, and port mode of the interfaces are correct. The verification output on MC-LAG Switches S1 and S2 differs from the output on FCoE Transit Switches T1 and T2.

Action List the interface configuration on MC-LAG Switches S1 and S2 using the operational mode command **show configuration interfaces**:

```
user@switch> show configuration interfaces
xe-0/0/10 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/11 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/0/20 {
    ether-options {
```



```
            802.3ad ae1;
        }
    }
    xe-0/0/21 {
        ether-options {
            802.3ad ae1;
        }
    }
    ae0 {
        mtu 2180;
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }
    ae1 {
        mtu 2180;
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }
```

List the interface configuration on FCoE Transit Switches TS1 and TS2 using the operational mode command **show configuration interfaces**:

```
user@switch> show configuration interfaces
xe-0/0/25 {
    ether-options {
        802.3ad ae1;
    }
}
xe-0/0/26 {
    ether-options {
        802.3ad ae1;
    }
}
xe-0/0/30 {
    mtu 2180;
    unit 0 {
        family ethernet-switching {
            port-mode tagged-access;
            vlan {
                members fcoe_vlan;
            }
        }
    }
}
xe-0/0/31 {
    mtu 2180;
    unit 0 {
        family ethernet-switching {
```

```
                port-mode tagged-access;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }
    xe-0/0/32 {
        mtu 2180;
        unit 0 {
            family ethernet-switching {
                port-mode tagged-access;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }
    xe-0/0/33 {
        mtu 2180;
        unit 0 {
            family ethernet-switching {
                port-mode tagged-access;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }

    ae1 {
        mtu 2180;
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members fcoe_vlan;
                }
            }
        }
    }
```

Meaning The **show configuration interfaces** command lists the configuration of each interface by interface name.

For each interface that is a member of a LAG, the command lists only the name of the LAG to which the interface belongs.

For each LAG interface and for each interface that is not a member of a LAG, the command output includes:

- The MTU (**2180**)
- The unit number of the interface (**0**)
- The port mode (**trunk** mode for interfaces that connect two switches, **tagged-access** mode for interfaces that connect to FCoE hosts)
- The name of the VLAN in which the interface is a member (**fcoe_vlan**)

Verifying That FIP Snooping Is Enabled on the FCoE VLAN on FCoE Transit Switches TS1 and TS2 Access Interfaces

Purpose Verify that FIP snooping is enabled on the FCoE VLAN access interfaces. FIP snooping is enabled only on the FCoE access interfaces, so it is enabled only on FCoE Transit Switches TS1 and TS2. FIP snooping is not enabled on MC-LAG Switches S1 and S2 because FIP snooping is done at the Transit Switch TS1 and TS2 FCoE access ports.

Action List the port security configuration on FCoE Transit Switches TS1 and TS2 using the operational mode command **show configuration ethernet-switching-options secure-access-port**:

```
user@switch> show configuration ethernet-switching-options secure-access-port
interface ae1.0 {
    fcoe-trusted;
}
vlan fcoe_vlan {
    examine-fip {
        examine-vn2vn {
            beacon-period 90000;
        }
    }
}
```

Meaning The **show configuration ethernet-switching-options secure-access-port** command lists port security information, including whether a port is trusted. The command output shows that:

- LAG port **ae1.0**, which connects the FCoE transit switch to the MC-LAG switches, is configured as an FCoE trusted interface. FIP snooping is not performed on the member interfaces of the LAG (**xe-0/0/25** and **xe-0/0/26**).
- FIP snooping is enabled (**examine-fip**) on the FCoE VLAN (**fcoe_vlan**), the type of FIP snooping is VN2VN_Port FIP snooping (**examine-vn2vn**) and the beacon period is set to 90000 milliseconds. On Transit Switches TS1 and TS2, all interface members of the FCoE VLAN perform FIP snooping unless the interface is configured as FCoE trusted. On Transit Switches TS1 and TS2, interfaces **xe-0/0/30**, **xe-0/0/31**, **xe-0/0/32**, and **xe-0/0/33** perform FIP snooping because they are not configured as FCoE trusted. The interface members of LAG **ae1** (**xe-0/0/25** and **xe-0/0/26**) do not perform FIP snooping because the LAG is configured as FCoE trusted.

Verifying That the FIP Snooping Mode Is Correct on FCoE Transit Switches TS1 and TS2

Purpose Verify that the FIP snooping mode is correct on the FCoE VLAN. FIP snooping is enabled only on the FCoE access interfaces, so it is enabled only on FCoE Transit Switches TS1 and TS2. FIP snooping is not enabled on MC-LAG Switches S1 and S2 because FIP snooping is done at the Transit Switch TS1 and TS2 FCoE access ports.

Action List the FIP snooping configuration on FCoE Transit Switches TS1 and TS2 using the operational mode command **show fip snooping brief**:

```
user@switch> show fip snooping brief
VLAN: fcoe_vlan,    Mode: VN2VN Snooping
  FC-MAP: 0e:fd:00
...
```

NOTE: The output has been truncated to show only the relevant information.

Meaning The **show fip snooping brief** command lists FIP snooping information, including the FIP snooping VLAN and the FIP snooping mode. The command output shows that:

- The VLAN on which FIP snooping is enabled is **fcoe_vlan**
- The FIP snooping mode is VN2VN_Port FIP snooping (**VN2VN Snooping**)

Verifying That IGMP Snooping Is Disabled on the FCoE VLAN

Purpose Verify that IGMP snooping is disabled on the FCoE VLAN on all four switches.

Action List the IGMP snooping protocol information on each of the four switches using the **show configuration protocols igmp-snooping** command:

```
user@switch> show configuration protocols igmp-snooping
vlan fcoe_vlan {
    disable;
}
```

Meaning The **show configuration protocols igmp-snooping** command lists the IGMP snooping configuration for the VLANs configured on the switch. The command output shows that IGMP snooping is disabled on the FCoE VLAN (**fcoe_vlan**).

Related Documentation

- Example: Configuring Multichassis Link Aggregation on page 39
- *Configuring Link Aggregation*
- *Example: Configuring CoS PFC for FCoE Traffic*
- *Example: Configuring CoS Hierarchical Port Scheduling (ETS)*
- *Understanding Multichassis Link Aggregation*
- Understanding MC-LAGs on an FCoE Transit Switch on page 309

PART 3

Troubleshooting

CHAPTER 6

Troubleshooting Multichassis Link Aggregation

Troubleshooting Multichassis Link Aggregation

Supported Platforms EX4600, QFX Series standalone switches

Use the following information to troubleshoot multichassis link aggregation configuration issues:

- Layer 3 Traffic Sent to the Standby MC-LAG Peer Is Not Redirected to Active MC-LAG Peer on page 344
- Aggregated Ethernet Interfaces Go Down on page 344
- Flooding of Upstream Traffic on page 344

MAC Addresses Learned on Multichassis Aggregated Ethernet Interfaces Are Not Removed from the MAC Address Table

Problem **Description:** When both of the mulitchassis aggregated Ethernet interfaces on both connected multichassis link aggregation group (MC-LAG) peers are down, the MAC addresses learned on the multichassis aggregated Ethernet interfaces are not removed from the MAC address table.

For example, if you disable the multichassis aggregated Ethernet interface (ae0) on both MC-LAG peers by issuing the **set interfaces ae0 disable** command and commit the configuration, the MAC table still shows the MAC addresses as being learned on the multichassis aggregated Ethernet interfaces of both MC-LAG peers.

```
user@switchA> show ethernet-switching table
Ethernet-switching table: 6 entries, 2 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v10                *                 Flood          - All-members
  v10                00:10:94:00:00:01 Learn(L)     3:55 ae0.0 (MCAE)
  v10                00:10:94:00:00:02 Learn(R)        0 xe-0/0/9.0
  v20                *                 Flood          - All-members
  v30                *                 Flood          - All-members
  v30                84:18:88:de:b1:2e Static         - Router
```

```
user@switchB> show ethernet-switching table
Ethernet-switching table: 6 entries, 2 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v10                *                 Flood          - All-members
  v10                00:10:94:00:00:01 Learn(R)        0 ae0.0 (MCAE)
  v10                00:10:94:00:00:02 Learn          40 xe-0/0/10.0
  v20                *                 Flood          - All-members
  v30                *                 Flood          - All-members
  v30                84:18:88:df:83:0a Static         - Router
```

Solution This is expected behavior.

MC-LAG Peer Does Not Go into Standby Mode

Problem **Description:** A multichassis link aggregation group (MC-LAG) peer does not go into standby mode if the MC-LAG peer IP address specified in the Inter-Chassis Control Protocol (ICCP) configuration and the IP address specified in the multichassis protection configuration are different.

Solution To prevent failure to enter standby mode, make sure that the peer IP address in the ICCP configurations and the IP address in multichassis protection configurations are the same.

Secondary MC-LAG Peer with Status Control Set to Standby Becomes Inactive

Problem **Description:** When the interchassis control link-protection link (ICL-PL) and multichassis aggregated Ethernet interfaces go down on the primary multichassis link aggregation group (MC-LAG) peer, the secondary MC-LAG peer's multichassis aggregated Ethernet interfaces with status control set to standby become inactive instead of active.

Solution This is expected behavior.

Redirect Filters Take Priority over User-Defined Filters

Problem **Description:** Multichassis link aggregation group (MC-LAG) implicit failover redirection filters take precedence over user-configured explicit filters.

Solution This is expected behavior.

Operational Command Output Is Wrong

Problem **Description:** After you deactivate Inter-Chassis Control Protocol (ICCP), the **show iccp** operational command output still shows registered client daemons, such as mcsnoopd, lacpd, and eswd.

For example:

```
user@switch> show iccp
Client Application: MCSNOOPD
  Redundancy Group IDs Joined: None

Client Application: lacpd
  Redundancy Group IDs Joined: 1

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

The **show iccp** command output always shows registered modules regardless of whether or not ICCP peers are configured.

Solution This is expected behavior.

ICCP Connection Might Take Up to 60 Seconds to Become Active

Problem **Description:** When the Inter-Chassis Control Protocol (ICCP) configuration and the routed VLAN interface (RVI) configuration are committed together, the ICCP connection might take up to 60 seconds to become active.

Solution This is expected behavior.

MAC Address Age Learned on a Multichassis Aggregated Ethernet Interface Is Reset to Zero

Problem **Description:** When you activate and then deactivate an interchassis control link-protection link (ICL-PL), the MAC address age learned on the multichassis aggregated Ethernet interface is reset to zero. The next-hop interface changes trigger MAC address updates in the hardware, which then triggers aging updates in the Packet Forwarding Engine. The result is that the MAC address age is updated to zero.

For example, the ICL-PL has been deactivated, and the **show ethernet-switching table** command output shows that the MAC addresses have an age of 0.

```
user@switch> show ethernet-switching table
Ethernet-switching table: 3 entries, 2 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  v100              *                 Flood          - All-members
  v100              00:10:00:00:00:01 Learn(L)     0 ae0.0 (MCAE)
  v100              00:10:00:00:00:02 Learn(L)     0 ae0.0 (MCAE)
```

Solution This is expected behavior.

MAC Address Is Not Learned Remotely in a Default VLAN

Problem **Description:** If a multichassis link aggregation group (MC-LAG) peer learns a MAC address in the default VLAN, the Inter-Chassis Control Protocol (ICCP) does not synchronize the MAC address with the MAC address of the other MC-LAG peer.

Solution This is expected behavior.

Snooping Entries Learned on Multichassis Aggregated Ethernet Interfaces Are Not Removed

Problem **Description:** When multichassis aggregated Ethernet interfaces are configured on a VLAN that is enabled for multicast snooping, the membership entries learned on the multichassis aggregated Ethernet interfaces on the VLAN are not cleared when the multichassis aggregated Ethernet interfaces go down. This is done to speed up convergence time when the interfaces come up, or come up and go down.

Solution This is expected behavior.

ICCP Does Not Come Up After You Add or Delete an Authentication Key

Problem **Description:** The Inter-Chassis Control Protocol (ICCP) connection is not established when you add an authentication key and then delete it only at the global ICCP level. However, authentication works correctly at the ICCP peer level.

Solution Delete the ICCP configuration, and then add the ICCP configuration.

Local Status Is Standby When It Should Be Active

Problem **Description:** If the multichassis aggregated Ethernet interface is down when the state machine is in a synchronized state, the multichassis link aggregation group (MC-LAG) peer local status is standby. If the multichassis aggregated Ethernet interface goes down after the state machine is in an active state, then the local status remains active, and the local state indicates that the interface is down.

Solution This is expected behavior.

Packets Loop on the Server When ICCP Fails

Problem **Description:** When you enable backup liveness detection for a multichassis link aggregation group (MC-LAG), and the backup liveness detection packets are lost because of a temporary failure on the MC-LAG, then both of the peers in the MC-LAG remain active. If this happens, both of the MC-LAG peers send packets to the connected server.

Solution This is expected behavior.

Both MC-LAG Peers Use the Default System ID After a Reboot or an ICCP Configuration Change

Problem **Description:** After a reboot or after a new Inter-Chassis Control Protocol (ICCP) configuration has been committed, and the ICCP connection does not become active, the Link Aggregation Control Protocol (LACP) messages transmitted over the multichassis aggregated Ethernet interfaces use the default system ID. The configured system ID is used instead of the default system ID only after the MC-LAG peers synchronize with each other.

Solution This is expected behavior.

No Commit Checks Are Done for ICL-PL Interfaces

Problem **Description:** There are no commit checks on the interface being configured as an inter-chassis link-protection link (ICL-PL), so you must provide a valid interface name for the ICL-PL.

Solution This is expected behavior.

Double Failover Scenario

Problem **Description:** If the following events happen in this exact order—Inter-Chassis Control Protocol (ICCP) goes down, and the multichassis aggregated Ethernet interface on the multichassis link aggregation group (MC-LAG) peer in active mode goes down—a double failover occurs. In this scenario, the MC-LAG peer in standby mode does not detect what happens on the active MC-LAG peer. The MC-LAG peer in standby mode operates as if the multichassis aggregated Ethernet interface on the MC-LAG in active mode were up and blocks the inter-chassis link-protection link (ICL-PL) traffic. The ICL-PL traffic is not forwarded.

Solution This is expected behavior.

Multicast Traffic Floods the VLAN When the ICL-PL Interface Goes Down and Up

Problem **Description:** When interchassis control link-protection link (ICL-PL) goes down and comes up, multicast traffic is flooded to all of the interfaces in the VLAN. The Packet Forwarding Engine flag Ip4McastFloodMode for the VLAN is changed to MCAST_FLOOD_ALL. This problem only occurs when a multichassis link aggregation group (MC-LAG) is configured for Layer 2.

Solution This is expected behavior.

Layer 3 Traffic Sent to the Standby MC-LAG Peer Is Not Redirected to Active MC-LAG Peer

Problem **Description:** When Inter-chassis Control Protocol (ICCP) is down, the status of a remote MC-LAG peer is unknown. Even if the MC-LAG peer is configured as standby, the traffic is not redirected to this peer because it is assumed that this peer is down.

Solution This is expected behavior.

Aggregated Ethernet Interfaces Go Down

Problem **Description:** When a multichassis aggregated Ethernet interface is converted to an aggregated Ethernet (AE) interface, it retains some multichassis aggregated Ethernet interface properties. For example, the aggregated Ethernet interface might retain the administrative key of the multichassis aggregated Ethernet. When this happens, the aggregated Ethernet interface goes down.

Solution Restart the Link Aggregation Control Protocol (LACP) on the multichassis link aggregation group (MC-LAG) peer hosting the AE interface to bring up the AE interface. Restarting LACP removes the multichassis aggregated Ethernet properties of the AE interface.

Flooding of Upstream Traffic

Problem **Description:** When MAC synchronization is enabled, the multichassis link aggregation group (MC-LAG) peer can resolve Address Resolution Protocol (ARP) entries for the MC-LAG routed VLAN interface (RVI) with either of the MC-LAG peer MAC addresses. If the downstream traffic is sent with one MAC address (MAC1) but the peer has resolved the MAC address with a different MAC address (MAC2), the MAC2 address might not be learned by any of the access layer switches. Flooding of the upstream traffic for the MAC2 address might then occur.

Solution Make sure that downstream traffic is sent from the MC-LAG peers periodically to prevent the MAC addresses from aging out.

Related Documentation

- *Understanding Multichassis Link Aggregation*
- Example: Configuring Multichassis Link Aggregation on page 39
- Configuring Multichassis Link Aggregation on page 35

CHAPTER 7

Interface Diagnostics

Interface Diagnostics Tools

Supported Platforms ACX Series, EX Series, J Series, M Series, MX Series, PTX Series, QFX Series, T Series

You can use two diagnostic tools to test the physical layer connections of interfaces: loopback testing and bit error rate test (BERT) testing. Loopback testing enables you to verify the connectivity of a circuit. BERT testing enables you to identify poor signal quality on a circuit. This section contains the following topics:

Configuring Loopback Testing

Loopback testing allows you to verify the connectivity of a circuit. You can configure any of the following interfaces to execute a loopback test: aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, E1, E3, *N*xDS0, serial, SONET/SDH, T1, and T3.

The physical path of a network data circuit usually consists of segments interconnected by devices that repeat and regenerate the transmission signal. The transmit path on one device connects to the receive path on the next device. If a circuit fault occurs in the form of a line break or a signal corruption, you can isolate the problem by using a loopback test. Loopback tests allow you to isolate segments of the circuit and test them separately.

To do this, configure a *line loopback* on one of the routers. Instead of transmitting the signal toward the far-end device, the line loopback sends the signal back to the originating router. If the originating router receives back its own Data Link Layer packets, you have verified that the problem is beyond the originating router. Next, configure a line loopback farther away from the local router. If this originating router does not receive its own Data Link Layer packets, you can assume that the problem is on one of the segments between the local router and the remote router's interface card. In this case, the next troubleshooting step is to configure a line loopback closer to the local router to find the source of the problem.

Thefollowing types of loopback testing are supported by the Junos OS:

- DCE local—Loops packets back on the local data circuit-terminating equipment (DCE).
- DCE remote—Loops packets back on the remote DCE.
- Local—Useful for troubleshooting physical PIC errors. Configuring local loopback on an interface allows transmission of packets to the channel service unit (CSU) and then to the circuit toward the far-end device. The interface receives its own transmission, which includes data and timing information, on the local router's PIC. The data received from the CSU is ignored. To test a local loopback, issue the **show interfaces *interface-name*** command. If PPP keepalives transmitted on the interface are received by the PIC, the **Device Flags** field contains the output **Loop-Detected**.
- Payload—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A payload loopback loops data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated.
- Remote—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A remote loopback loops packets, including both data and timing information, back on the remote router's interface card. A router at one end of the circuit initiates a remote loopback toward its remote partner. When you configure a remote loopback, the packets received from the physical circuit and CSU are received by the interface. Those packets are then retransmitted by the PIC back toward the CSU and the circuit. This loopback tests all the intermediate transmission segments.

Table 17 on page 348 shows the loopback modes supported on the various interface types.

Table 17: Loopback Modes by Interface Type

Interface	Loopback Modes	Usage Guidelines
Aggregated Ethernet, Fast Ethernet, Gigabit Ethernet	Local	*Configuring Ethernet Loopback Capability*
Circuit Emulation E1	Local and remote	*Configuring E1 Loopback Capability*
Circuit Emulation T1	Local and remote	*Configuring T1 Loopback Capability*
E1 and E3	Local and remote	*Configuring E1 Loopback Capability* and *Configuring E3 Loopback Capability*
*N*xDS0	Payload	*Configuring Channelized E1 IQ and IQE Interfaces*, *Configuring T1 and NxDS0 Interfaces*, *Configuring Channelized OC12/STM4 IQ and IQE Interfaces (SONET Mode)*, *Configuring Channelized STM1 IQ and IQE Interfaces*, and *Configuring Channelized T3 IQ Interfaces*
Serial (V.35 and X.21)	Local and remote	*Configuring Serial Loopback Capability*

Table 17: Loopback Modes by Interface Type *(continued)*

Interface	Loopback Modes	Usage Guidelines
Serial (EIA-530)	DCE local, DCE remote, local, and remote	*Configuring Serial Loopback Capability*
SONET/SDH	Local and remote	*Configuring SONET/SDH Loopback Capability*
T1 and T3	Local, payload, and remote	*Configuring T1 Loopback Capability* and *Configuring T3 Loopback Capability* See also *Configuring the T1 Remote Loopback Response*

To configure loopback testing, include the **loopback** statement:

loopback *mode*;

You can include this statement at the following hierarchy levels:

- **[edit interfaces** ***interface-name*** **aggregated-ether-options]**
- **[edit interfaces** ***interface-name*** **ds0-options]**
- **[edit interfaces** ***interface-name*** **e1-options]**
- **[edit interfaces** ***interface-name*** **e3-options]**
- **[edit interfaces** ***interface-name*** **fastether-options]**
- **[edit interfaces** ***interface-name*** **gigether-options]**
- **[edit interfaces** ***interface-name*** **serial-options]**
- **[edit interfaces** ***interface-name*** **sonet-options]**
- **[edit interfaces** ***interface-name*** **t1-options]**
- **[edit interfaces** ***interface-name*** **t3-options]**

BERT Testing

A bit error rate test (BERT) allows you to troubleshoot problems by checking the quality of links. You can configure any of the following interfaces to execute a BERT when the interface receives a request to run this test: E1, E3, T1, T3; the channelized DS3, OC3, OC12, and STM1 interfaces; and the channelized DS3 IQ, E1 IQ, and OC12 IQ interfaces.

A BERT test requires a line loop to be in place on either the transmission devices or the far-end router. The local router generates a known bit pattern and sends it out the transmit path. The received pattern is then verified against the sent pattern. The higher the bit error rate of the received pattern, the worse the noise is on the physical circuit. As you move the position of the line loop increasingly downstream toward the far-end router, you can isolate the troubled portion of the link.

To configure BERT, you must configure the duration of the test, the bit pattern to send on the transmit path, and the error rate to monitor when the inbound pattern is received.

To configure the duration of the test, the pattern to send in the bit stream, and the error rate to include in the bit stream, include the **bert-period**, **bert-algorithm**, and **bert-error-rate** statements, respectively, at the **[edit interfaces *interface-name interface-type*-options]** hierarchy level:

[edit interfaces *interface-name interface-type*-options]
bert-algorithm *algorithm*;
bert-error-rate *rate*;
bert-period *seconds*;

By default, the BERT period is 10 seconds. You can configure the BERT period to last from 1 through 239 seconds on some PICs and from 1 through 240 seconds on other PICs.

rate is the bit error rate. This can be an integer from 0 through 7, which corresponds to a bit error rate from 10^{-0} (1 error per bit) to 10^{-7} (1 error per 10 million bits).

algorithm is the pattern to send in the bit stream. For a list of supported algorithms, enter a **?** after the **bert-algorithm** statement; for example:

```
[edit interfaces t1-0/0/0 t1-options]

user@host# set bert-algorithm ?
Possible completions:
  pseudo-2e11-o152     Pattern is 2^11 -1 (per 0.152 standard)
  pseudo-2e15-o151     Pattern is 2^15 - 1 (per 0.152 standard)
  pseudo-2e20-o151     Pattern is 2^20 - 1 (per 0.151 standard)
  pseudo-2e20-o153     Pattern is 2^20 - 1 (per 0.153 standard)
        ...
```

For specific hierarchy information, see the individual interface types.

NOTE: The four-port E1 PIC supports only the following algorithms:

```
pseudo-2e11-o152     Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151     Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151     Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e23-o151     Pattern is 2^23 (per 0.151 standard)
```

When you issue the **help** command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: The 12-port T1/E1 Circuit Emulation (CE) PIC supports only the following algorithms:

```
all-ones-repeating   Repeating one bits
all-zeros-repeating  Repeating zero bits
alternating-double-ones-zeros  Alternating pairs of ones and zeros
alternating-ones-zeros  Alternating ones and zeros
pseudo-2e11-o152     Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151     Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151     Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e7           Pattern is 2^7 - 1
pseudo-2e9-o153      Pattern is 2^9 - 1 (per 0.153 standard)
repeating-1-in-4     1 bit in 4 is set
repeating-1-in-8     1 bit in 8 is set
repeating-3-in-24    3 bits in 24 are set
```

When you issue the **help** command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: The IQE PICs support only the following algorithms:

```
all-ones-repeating   Repeating one bits
all-zeros-repeating  Repeating zero bits
alternating-double-ones-zeros  Alternating pairs of ones and zeros
alternating-ones-zeros  Alternating ones and zeros
pseudo-2e9-o153      Pattern is 2^9  -1 (per 0.153 (511 type) standard)
pseudo-2e11-o152    Pattern is 2^11 -1 (per 0.152 and 0.153 (2047 type)
 standards)
pseudo-2e15-o151     Pattern is 2^15 -1 (per 0.151 standard)
pseudo-2e20-o151     Pattern is 2^20 -1 (per 0.151 standard)
pseudo-2e20-o153     Pattern is 2^20 -1 (per 0.153 standard)
pseudo-2e23-o151     Pattern is 2^23 -1 (per 0.151 standard)
repeating-1-in-4     1 bit in 4 is set
repeating-1-in-8     1 bit in 8 is set
repeating-3-in-24    3 bits in 24 are set
```

When you issue the **help** command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: BERT is supported on the PDH interfaces of the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP and the DS3/E3 MIC. The following BERT algorithms are supported:

```
all-ones-repeating            Repeating one bits
all-zeros-repeating           Repeating zero bits
alternating-double-ones-zeros Alternating pairs of ones and zeros
alternating-ones-zeros        Alternating ones and zeros
repeating-1-in-4              1 bit in 4 is set
repeating-1-in-8              1 bit in 8 is set
repeating-3-in-24             3 bits in 24 are set
pseudo-2e9-o153               Pattern is 2^9 - 1 (per 0.153 standard)
pseudo-2e11-o152              Pattern is 2^11 - 1 (per 0.152 standard)
pseudo-2e15-o151              Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151              Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e20-o153              Pattern is 2^20 - 1 (per 0.153 standard)
pseudo-2e23-o151              Pattern is 2^23 (per 0.151 standard)
```

Table 18 on page 352 shows the BERT capabilities for various interface types.

Table 18: BERT Capabilities by Interface Type

Interface	T1 BERT	T3 BERT	Comments
12-port T1/E1 Circuit Emulation	Yes (ports 0–11)	—	• Limited algorithms
4-port Channelized OC3/STM1 Circuit Emulation	Yes (port 0–3)	—	• Limited algorithms
E1 or T1	Yes (port 0–3)	Yes (port 0–3)	• Single port at a time • Limited algorithms
E3 or T3	Yes (port 0–3)	Yes (port 0–3)	• Single port at a time
Channelized OC12	-—	Yes (channel 0–11)	• Single channel at a time • Limited algorithms • No bit count
Channelized STM1	Yes (channel 0–62)	—	• Multiple channels • Only one algorithm • No error insert • No bit count
Channelized T3 and Multichannel T3	Yes (channel 0–27)	Yes (port 0–3 on channel 0)	• Multiple ports and channels • Limited algorithms for T1 • No error insert for T1 • No bit count for T1

These limitations do not apply to channelized IQ interfaces. For information about BERT capabilities on channelized IQ interfaces, see *Channelized IQ and IQE Interfaces Properties*.

Starting and Stopping a BERT Test

Before you can start the BERT test, you must disable the interface. To do this, include the **disable** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
disable;
```

After you configure the BERT properties and commit the configuration, begin the test by issuing the **test interface *interface-name* *interface-type*-bert-start** operational mode command:

```
user@host> test interface interface-name interface-type-bert-start
```

The test runs for the duration you specify with the **bert-period** statement. If you want to terminate the test sooner, issue the **test interface *interface-name* *interface-type*-bert-stop** command:

```
user@host> test interface interface-name interface-type-bert-stop
```

For example:

```
user@host> test interface t3-1/2/0 t3-bert-start
user@host> test interface t3-1/2/0 t3-bert-stop
```

To view the results of the BERT test, issue the **show interfaces extensive | find BERT** command:

```
user@host> show interfaces interface-name extensive | find BERT
```

For more information about running and evaluating the results of the BERT procedure, see the CLI Explorer.

NOTE: To exchange BERT patterns between a local router and a remote router, include the **loopback remote** statement in the interface configuration at the remote end of the link. From the local router, issue the **test interface** command.

Example: Configuring Bit Error Rate Testing

Configure a BERT test on a T3 interface. In this example, the run duration lasts for 120 seconds. The configured error rate is 0, which corresponds to a bit error rate of 10^{-0} (1 error per bit). The configured bit pattern of **all-ones-repeating** means that every bit the interface sends is set to a value of 1.

```
[edit interfaces]
t3-1/2/0 {
  t3-options {
    bert algorithm all-ones-repeating;
    bert-error-rate 0;
    bert-period 120;
```



```
  }
}
```

PART 4

Configuration Statements and Operational Commands

CHAPTER 8

Configuration Statements

authentication-key (ICCP)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax authentication-key *key*;

Hierarchy Level [edit protocols iccp],
[edit protocols iccp peer *peer-IP-address*]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Specify the authentication key (password). The QFX3500 and MX Series devices use this password to verify the authenticity of packets sent from the peers hosting a multichassis link aggregation group (MC-LAG). Peer-level authentication takes precedence over global-level authentication.

Inter-Chassis Control Protocol (ICCP) uses MD5 authentication.

Options ***key***—Authentication password. It can be 1 through 16 contiguous digits or letters. Separate decimal digits with periods. Separate hexadecimal digits with periods and precede the string with 0x. If you include spaces in the password, enclose the entire password in quotation marks (" ").

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

backup-liveness-detection

Supported Platforms EX Series, QFX Series standalone switches

Syntax

```
backup-liveness-detection {
  backup-peer-ip ipv4-address;
}
```

Hierarchy Level [edit protocols iccp peer]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2R1 for EX Series switches.

Description Backup liveness detection determines the peer status (whether it is up or down) by exchanging keep alive messages (UDP-based packets) over the management link between the two Inter-Chassis Control Protocol (ICCP) peers. When an ICCP connection is operationally down, the status of the peers hosting a multichassis link aggregation group (MC-LAG) is detected by sending liveness detection requests to each other. Peers must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, the liveness detection check fails, and a failure action is implemented. Backup liveness detection must be configured on both peers hosting the MC-LAG.

The remaining statement is explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

backup-peer-ip

Supported Platforms EX Series, QFX Series standalone switches

Syntax backup-peer-ip *ipv4-address*;

Hierarchy Level [edit protocols iccp peer backup-liveness-detection]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2R1 for EX Series switches.

Description Specify the IP address of the peer being used as a backup peer in the Bidirectional Forwarding Detection (BFD) configuration.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

detection-time (Liveness Detection)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax

```
detection-time {
  threshold milliseconds;
}
```

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description The Bidirectional Forwarding Detection (BFD) timers are adaptive and can be adjusted to be faster or slower.

The remaining statement is explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

iccp

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
iccp {
  authentication-key string;
  local-ip-addr local-ip-addr;
  peer ip-address{
    authentication-key string;
    backup-liveness-detection {
      backup-peer-ip ip-address;
    }
    liveness-detection {
      detection-time {
        threshold milliseconds;
      }
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    local-ip-addr ipv4-address;
    session-establishment-hold-time seconds;
  }
  session-establishment-hold-time seconds;
  traceoptions {
    file <filename> <files number> <match regular-expression> <microsecond-stamp>
      <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure Inter-Chassis Control Protocol (ICCP) between the multichassis link aggregation group (MC-LAG) peers. ICCP replicates forwarding information, validates configurations, and propagates the operational state of the MC-LAG members.

NOTE: Backup liveness detection is not supported on MX Series routers.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

interface (Multichassis Protection)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax interface *interface-name*;

Hierarchy Level [edit multi-chassis multi-chassis-protection peer]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the name of the interface that is being used as an interchassis link-protection link (ICL-PL). The two switches hosting a multichassis link aggregation group (MC-LAG) use this link to pass Inter-Chassis Control Protocol (ICCP) and data traffic.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

local-ip-addr (ICCP)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax local-ip-addr *local-ip-address*;

Hierarchy Level [edit protocols iccp],
[edit protocols iccp peer *peer-IP-address*]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the local IP address of the interchassis link (ICL) interface that Inter-Chassis Control Protocol (ICCP) uses to communicate to the peers that host a multichassis link aggregation group (MC-LAG).

Options ***local-ip-address***—Default local IP address to be used by all peers.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

mc-ae

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
mc-ae {
  chassis-id chassis-id;
    events {
      iccp-peer-down;
        force-icl-down;
      prefer-status-control-active;
      }
      init-delay-time seconds;
      mc-ae-id mc-ae-id;
      mode (active-active | active-standby);
      redundancy-group group-id;
      status-control (active | standby);
    switchover-mode (non-revertive |revertive);
  }
```

Hierarchy Level [edit interfaces ae*X* aggregated-ether-options],
[edit logical-systems *logical-system-name interfaces* ae*X* aggregated-ether-options]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series routers.
events statement introduced in Junos OS Release 11.4R4 for MX Series routers.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
prefer-status-control-active statement introduced in Junos OS Release 13.2R1 for EX Series switches.
init-delay-time *seconds* statement introduced in Junos OS Release 13.2R3 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for the QFX Series. Only the **chassis-id**, **mc-ae-id**, **mode active-active**, and **status-control (active | standby)** options are supported on QFX Series devices.

Description Enable multichassis link aggregation groups (MC-LAGs), which enables one device to form a logical LAG interface with two or more other devices.

Options

chassis-id *chassis-id*—Specify the chassis ID for Link Aggregation Control Protocol (LACP) to calculate the port number of MC-LAG physical member links.

Values: 0 or 1

events—Specify an action if a specific MC-LAG event occurs.

iccp-peer-down—Specify an action if the ICCP peer of this node goes down.

force-icl-down—If the node's ICCP peer goes down, bring down the interchassis-link logical interface.

prefer-status-control-active—Specify that the node configured as **status-control active** become the active node if the peer of this node goes down.

NOTE: The **prefer-status-control-active** statement can be configured with the **status-control standby** statement to prevent the LACP MC-LAG system ID from reverting to the default LACP system ID on ICCP failure. Use this statement only if you can ensure that ICCP will not go down unless the router or switch is down. You must also configure the **hold-time down** value (at the **[edit interfaces** ***interface-name*****]** hierarchy level) for the interchassis link with the **status-control standby** configuration to be higher than the ICCP BFD timeout. This configuration prevents data traffic loss by ensuring that when the router or switch with the **status-control active** configuration goes down, the router or switch with the **status-control standby** statement does not go into standby mode.

To make the **prefer-status-control-active** statement work with the **status-control standby** statement when an interchassis-link logical interface is configured on a aggregate Ethernet interface, you must either configure the **lacp periodic** ***interval*** statement at the **[edit interface** ***interface-name*** **aggregated-ether-options]** hierarchy level as slow or configure the **detection-time threshold** statement at the **[edit protocols iccp peer liveness-detection]** hierarchy level as less than 3 seconds.

init-delay-time ***seconds***—To minimize traffic loss, specify the number of seconds in which to delay bringing the multichassis aggregated Ethernet interface back to the up state when you reboot an MC-LAG peer.

mc-ae-id ***mc-ae-id***—Specify the identification number of the MC-LAG device. The two MC-LAG network devices that manage a given MC-LAG must have the same identification number.

Range: 1 through 65,535

mode (active-active | active-standby)—Specify whether the MC-LAG is in active-active or active-standby mode.

NOTE: You can configure IPv4 (inet) and IPv6 (inet6) addresses on **mc-ae** interfaces when the **active-standby** mode is configured.

redundancy-group ***group-id***—Specify the redundancy group identification number. The Inter-Chassis Control Protocol (ICCP) uses the redundancy group ID to associate multiple chassis that perform similar redundancy functions.

Range: 1 through 4,294,967,294

revert-time—Wait interval (in minutes) before the switchover to the preferred node is performed when the **switchover-mode** is configured as revertive.

Range: 1 through 10

status-control (active | standby)—Specify whether the chassis becomes active or remains in standby mode when an interchassis link failure occurs.

switchover-mode (non-revertive | revertive)—Specify whether Junos OS should trigger a link switchover to the preferred node when the active node is available.

NOTE: **For revertive mode to automatically switch over to the preferred node, the status-control statement needs to be configured as active.**

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Active-Active Bridging and VRRP over IRB Functionality on MX Series Routers Overview on page 63
- Configuring Multichassis Link Aggregation on MX Series Routers on page 27
- Configuring Multichassis Link Aggregation on EX Series Switches on page 32

minimum-interval (Liveness Detection)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax minimum-interval *milliseconds*;

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information

Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure simultaneously the minimum interval at which the peer transmits liveness detection requests and the minimum interval at which the peer expects to receive a reply from a peer with which it has established a Bidirectional Forwarding Detection (BFD) session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately by using the **transmit-interval minimal-interval** and **minimum-receive-interval** statements, respectively.

Options

milliseconds—Specify the minimum interval value for Bidirectional Forwarding Detection (BFD).

Range: 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

minimum-receive-interval (Liveness Detection)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax minimum-receive-interval *milliseconds*;

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure the minimum interval at which the peer must receive a reply from a peer with which it has established a Bidirectional Forwarding Detection (BFD) session.

Options ***milliseconds***—Specify the minimum interval value.

Range: 1 through 255,000

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

multiplier (Liveness Detection)

Supported Platforms EX4600, QFX Series standalone switches

Syntax multiplier *number*;

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the number of liveness detection requests not received by the peer before Bidirectional Forwarding Detection (BFD) declares the peer is down.

Options ***number***—Maximum allowable number of liveness detection requests missed by the peer.

Range: 1 through 255

Default: 3

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

multi-chassis

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
multi-chassis {
  multi-chassis-protection peer-ip-address {
    interface interface-name;
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure an interchassis link-protection link (ICL-PL) between the two peers that host a multichassis link aggregation group (MC-LAG). You can configure either an aggregated Ethernet interface or a 10-Gigabit Ethernet interface to be an ICL-PL.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

multi-chassis-protection

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
multi-chassis-protection peer-ip-address {
  interface interface-name;
}
```

Hierarchy Level [edit multi-chassis]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure multichassis link protection between the two peers that host a multichassis link aggregation group (MC-LAG). If the Interchassis Control Protocol (ICCP) connection is up and the interchassis link (ICL) comes up, the peer configured as standby brings up the multichassis aggregated Ethernet interfaces shared with the peer. Multichassis protection must be configured on one interface for each peer.

The remaining statement is explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

no-adaptation (Liveness Detection)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax

```
no-adaptation;
```

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

peer (ICCP)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
peer ip-address {
  authentication-key string;
  backup-liveness-detection {
    backup-peer-ip ip-address;
  }
  liveness-detection {
    detection-time {
      threshold milliseconds;
    }
    minimum-intervalmilliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version (1 | automatic);
  }
  local-ip-addr ipv4-address;
  session-establishment-hold-time seconds;
}
```

Hierarchy Level [edit protocols iccp]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure the peers that host a multichassis link aggregation group (MC-LAG). You must configure Inter-Chassis Control Protocol (ICCP) for both peers that host the MC-LAG.

NOTE: Backup liveness detection is not supported on MX Series routers.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

peer (Multichassis)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax

```
peer ip-address {
  interface interface-name;
}
```

Hierarchy Level [edit multi-chassis]

Release Information Statement introduced in Junos OS Release 9.6 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the IP address of the peer that is part of the interchassis link-protection link (ICL-PL). If Inter-Chassis Control Protocol (ICCP) is up and the interchassis link (ICL) comes up, the peer configured as standby will bring up the multichassis aggregated Ethernet interfaces shared with the active peer specified by the **peer** statement. You must specify the physical interface of the peer.

The remaining statement is explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

session-establishment-hold-time

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax session-establishment-hold-time *seconds*;

Hierarchy Level [edit protocols iccp],
[edit protocols iccp peer]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Specify the time during which an Inter-Chassis Control Protocol (ICCP) connection must be established between peers.

Options *seconds*—Time (in seconds) within which a successful ICCP connection must be established.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

threshold (Detection Time)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax threshold *milliseconds*;

Hierarchy Level [edit protocols iccp peer liveness-detection detection-time]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Specify the threshold for the adaptation of the detection time for a Bidirectional Forwarding Detection (BFD) session. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

NOTE: **The threshold time must be greater than or equal to the minimum-interval or the minimum-receive-interval values.**

Options *milliseconds*— Value for the detection time adaptation threshold.

Range: 1 through 255,000

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

transmit-interval (Liveness Detection)

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax

```
transmit-interval {
  minimum-interval milliseconds;
  threshold milliseconds;
}
```

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure the Bidirectional Forwarding Detection (BFD) transmit interval. The negotiated transmit interval for a peer is the interval between the sending of BFD liveness detection requests to peers. The receive interval for a peer is the minimum interval between receiving packets sent from its peer; the receive interval is not negotiated between peers. To determine the transmit interval, each peer compares its configured minimum transmit interval with its peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

version (Liveness Detection)

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax version (1 | automatic);

Hierarchy Level [edit protocols iccp peer liveness-detection]

Release Information Statement introduced in Junos OS Release 10.0 for MX Series routers.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description Configure the Bidirectional Forwarding Detection (BFD) protocol version to detect.

Options **1**—Use BFD protocol version 1.

automatic—Autodetect the BFD protocol version.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

CHAPTER 9

Operational Commands

show iccp

Supported Platforms EX4600, MX Series, QFX Series standalone switches

Syntax

show iccp <brief | detail>
logical-system [*system-name* | all]

Release Information Command introduced in Junos OS Release 10.0 for the MX Series.
Support for logical systems added in Junos OS Release 14.1 for MX Series routers.
Command introduced in Junos OS Release 12.2 for the QFX Series.

Description Display Inter-Chassis Control Protocol (ICCP) information about the multichassis link aggregation group (MC-LAG) peers, including the state of the TCP connection, Bidirectional Forwarding Detection protocol, backup liveness peer status, and MCSNOOPD, LACPD, and ESWD applications.

Options

none—Display ICCP information about the MC-LAG peers, including the state of the TCP connection and Bidirectional Forwarding Detection protocol, and MCSNOOPD, LACP, and ESWD applications.

brief—Display brief ICCP information about the MC-LAG peers, including the state of the TCP connection and Bidirectional Forwarding Detection protocol, and MCSNOOPD, LACP, and ESWD applications.

detail—Display detailed ICCP information about the MC-LAG peers, including the state of the TCP connection and Bidirectional Forwarding Detection protocol, and MCSNOOPD , LACP, and ESWD applications.

logical-system [*system-name* | all]—(Optional) Display information for a specified logical system or all systems.

Required Privilege Level view

Related Documentation

- iccp on page 361
- *Understanding Multichassis Link Aggregation*

List of Sample Output

show iccp (QFX Series) on page 375
show iccp (MX Series) on page 375

Output Fields Table 19 on page 374 lists the output fields for the **show iccp** command. Output fields are listed in the approximate order in which they appear.

Table 19: show iccp Output Fields

Field Name	Field Description
Redundancy Group Information for peer	Aggregated Ethernet interface name.
TCP Connection	Specifies if the TCP connection between the peers hosting the MC-LAG is up or down.

Table 19: show iccp Output Fields *(continued)*

Field Name	Field Description
Liveness Detection	Specifies if liveness detection, also known as Bidirectional Forwarding Detection (BFD), is up or down.
Client Application	Specifies information regarding the state of the MCSNOOPD and client applications.

Sample Output

show iccp (QFX Series)

```
user@switch> show iccp
Redundancy Group Information for peer 3.3.3.2
  TCP Connection       : Established
  Liveliness Detection : Up

Client Application: MCSNOOPD

Client Application: eswd
```

show iccp (MX Series)

```
user@host> show iccp
Logical system :LS1
    Redundancy Group Information for peer 16.1.1.1
       TCP Connection       : Established
       Liveliness Detection : Up
       Redundancy Group ID          Status
         2                           Up
         12                         Up

Client Application: lacpd
Redundancy Group IDs Joined:  1
Redundancy Group IDs Joined:  2

Client Application: l2ald_iccpd_client
 Redundancy Group IDs Joined:  1
 Redundancy Group IDs Joined:  2
```

show interfaces mc-ae

Supported Platforms EX Series, MX Series, QFX Series standalone switches

Syntax **show interfaces mc-ae id *identifier* unit *number***

Release Information Command introduced in Junos OS Release 9.6 for the MX Series.
Command introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description On peers with multichassis aggregated Ethernet (**mc-ae*X***) interfaces, use this command to display information about the multichassis aggregated Ethernet interfaces.

Options **id *identifier***—(Optional) Specify the name of the multichassis aggregated Ethernet interface.

unit *number*—(Optional) Specify the logical interface by unit number.

Required Privilege Level view

Related Documentation

- *Understanding Multichassis Link Aggregation* (QFX Series Switches)
- *Understanding Multichassis Link Aggregation* (EX Series Switches)
- Configuring Multichassis Link Aggregation on page 35 (QFX Series Switches)
- Configuring Multichassis Link Aggregation on EX Series Switches on page 32 (EX Series Switches)
- Example: Configuring Multichassis Link Aggregation on page 39 (QFX Series Switches)
- Example: Configuring Multichassis Link Aggregation with Layer 3 MAC Address Synchronization on page 170 (QFX Series Switches)
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast using MAC Address Synchronization on page 193 (QFX Series Switches)
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on page 208 (QFX Series Switches)
- Example: Configuring Multichassis Link Aggregation for Layer 3 Unicast Using VRRP on EX9200 Switches on page 152 (EX Series Switches)
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on page 235 (QFX Series Switches)
- Example: Configuring Multichassis Link Aggregation for Layer 3 Multicast Using VRRP on EX9200 Switches on page 130 (EX Series Switches)

List of Sample Output
show interfaces mc-ae (QFX Series Switch) on page 377
show interfaces mc-ae (MX Series) on page 377
show interfaces mc-ae (Active/Active Bridging and VRRP over IRB on MX Series) on page 378

Output Fields Table 20 on page 377 lists the output fields for the **show interfaces mc-ae** command. Output fields are listed in the approximate order in which they appear.

Table 20: show interfaces mc-ae Output Fields

Output Field Name	Field Description
Current State Machine's State	Specifies the state of the MC-LAG initialization state machine.
Member Link	Specifies the identifiers of the configured multichassis link aggregated interface members.
Local Status	Specifies the status of the local link: **active** or **standby**.
Peer Status	Specifies the status of the peer link: **active** or **standby**.
Peer State	Specifies the status of the local and peer links in an **active/active** MC-LAG configuration.
Logical Interface	Specifies the identifier and unit of the AE interface.
Topology Type	Specifies the bridge configured on the AE.
Local State	Specifies if the local device is up or down.
Peer State	Specifies if the peer device is up or down.
Peer Ip/MCP/State	Specifies the multichassis protection (MCP) link or the interchassis link-protection link (ICL-PL) for all of the multichassis aggregated Ethernet interfaces that are part of the peer.

Sample Output

show interfaces mc-ae (QFX Series Switch)

```
user@host> show interfaces mc-ae ae1 512
Member Link                   : ae0
 Current State Machine's State: mcae active state
 Local Status                  : active
 Local State                   : up
 Peer Status                   : active
 Peer State                    : up
     Logical Interface         : ae0.0
     Topology Type             : bridge
     Local State               : up
     Peer State                : up
     Peer Ip/MCP/State         : 3.3.3.2 ae1.0 up
```

show interfaces mc-ae (MX Series)

```
user@host> show interfaces mc-ae ae0 unit 512
  Member Links    : ae0
  Local Status    : active
  Peer Status     : active
```



```
 Logical Interface        : ae0.512
 Core Facing Interface : Label Ethernet Interface
 ICL-PL         : Label Ethernet Interface
```

show interfaces mc-ae (Active/Active Bridging and VRRP over IRB on MX Series)

```
user@host# show interfaces mc-ae ge-0/0/0.0
 Member Link                   : ae0
 Current State Machine's State: active
 Local Status                  : active
 Local State                   : up
 Peer Status                   : active
 Peer State                    : up
     Logical Interface         : ae0.0
     Topology Type             : bridge
     Local State               : up
     Peer State                : up
     Peer Ip/ICL-PL/State      : 192.168.100.10 ge-0/0/0.0 up
```


PART 2

Index

Index

V