This chapter provides an overview and discusses various topologies of Extreme’s Automatic Protection Switching (EAPS) feature. The chapter offers configuration and monitoring details, and also provides configuration examples.

**EAPS Protocol Overview**

The EAPS protocol provides fast protection switching to Layer 2 switches interconnected in an Ethernet ring topology, such as a Metropolitan Area Network (MAN) or large campus (see the following figure).

**EAPS Benefits**

EAPS offers the following benefits:
• **Fast Recovery time for link or node failures**—When a link failure or switch failure occurs, EAPS provides fast recovery times. EAPS provides resiliency for voice, video and data services.

• **Scalable network segmentation and fault isolation**—EAPS domains can protect groups of multiple VLANs, allowing scalable growth and broadcast loop protection. EAPS domains provide logical and physical segmentation, which means the failures in one EAPS ring do not impact network service for other rings and VLANs.

• **Resilient foundation for non-stop IP routing services**—EAPS provides a resilient foundation for upper level routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), minimizing route-flapping and dropped neighbors within the routed IP network.

• **Predictable convergence regardless of failure location**—EAPS provides consistent and predictable recovery behavior regardless of where link failures occur. The simple blocking architecture and predictable performance of EAPS allows for enforceable Service Level Agreements (SLAs). This allows easier network troubleshooting and failure scenario analysis without lengthy testing or debugging on live production networks.

EAPS protection switching is similar to what can be achieved with the Spanning Tree Protocol (STP), but EAPS offers the advantage of converging in less than one second when a link in the ring breaks.

An Ethernet ring built using EAPS can have resilience comparable to that provided by SONET rings, at a lower cost and with fewer restraints (such as ring size). The EAPS technology developed by Extreme Networks to increase the availability and robustness of Ethernet rings is described in RFC 3619: Extreme Networks’ Ethernet Automatic Protection Switching (EAPS) Version 1.

**EAPS Single Ring Topology**

The simplest EAPS configuration operates on a single ring.

This section describes how this type of EAPS configuration operates. Later sections describe more complex configurations.

An EAPS domain consists of one master node and one or more transit nodes (see the following figure), and includes one control VLAN and one or more protected VLANs.

A domain is a single instance of the EAPS protocol that defines the scope of protocol operation. A single logical EAPS domain typically exists on a given physical ring topology (fiber or copper).
A protected VLAN is a user data VLAN that uses the ring for a protected connection between all edge ports. The protected VLAN uses 802.1q trunking on the ring ports and supports tagged and untagged edge ports.

One ring port of the master node is designated the master node’s primary port (P), and another port is designated as the master node’s secondary port (S) to the ring. In normal operation, the master node blocks the secondary port for all protected VLAN traffic, thereby preventing a loop in the ring. (The spanning tree protocol, STP, provides the same type of protection.) Traditional Ethernet bridge learning and forwarding database mechanisms direct user data around the ring within the protected VLANs.

Although primary and secondary ports are configured on transit nodes, both port types operate identically as long as the transit node remains a transit node. If the transit node is reconfigured as a master node, the configured states of the primary and secondary ports apply.

The control VLAN is a dedicated 802.1q tagged VLAN that is used to transmit and receive EAPS control frames on the ring. The control VLAN can contain only two EAPS ring ports on each node. Each EAPS domain has a unique control VLAN, and control traffic is not blocked by the master node at any time. The control VLAN carries the following EAPS control messages around the ring:

- Health-check messages, which are sent from the master node primary port. Transit nodes forward health-check messages toward the master node secondary port on the control VLAN. When the master node receives a health check message on the secondary port, the EAPS ring is considered intact.
- Link-down alert messages, which are sent from a transit node to the master node when the transit node detects a local link failure.
- Flush-FDB messages, which are sent by the master node to all transit nodes when ring topology changes occur. Upon receiving this control frame, the transit node clears its MAC address forwarding table (FDB) and relearns the ring topology.
When the master node detects a failure, due to an absence of health-check messages or a received link-down alert, it transitions the EAPS domain to the Failed state and unblocks its secondary port to allow data connectivity in the protected VLANs.

### EAPS Multiple Ring Topology

EAPS works with multiple ring networks to support more complex topologies for interconnecting multiple EAPS domains. This allows larger EAPS end-to-end networks to be built from edge to core.

**Note**

Minimal EAPS support is provided at all license levels. EAPS multiple ring topologies and common link topologies are supported at higher license levels as described in Feature License Requirements.

The simplest multiple ring topology uses a single switch to join two EAPS rings.

The common link feature uses two switches, which share a common link, to provide redundancy and link multiple EAPS rings.

**Two Rings Connected by One Switch**

The following figure shows how a data VLAN can span two rings interconnected by a common switch—a figure eight topology.

![Figure 125: Two Rings Interconnected by One Switch](image)

A data VLAN that spans multiple physical rings or EAPS domains and is protected by EAPS is called an overlapping VLAN. An overlapping VLAN requires loop protection for each EAPS domain to which it belongs.

In the following figure, there is an EAPS domain with its own control VLAN running on ring 1 and another EAPS domain with its own control VLAN running on ring 2. A data VLAN that spans both rings is added as a protected VLAN to both EAPS domains to create an overlapping VLAN. Switch SS has two instances of EAPS domains running on it, one for each ring.
### Multiple Rings Sharing an EAPS Common Link

#### EAPS Common Link Operation

The following figure shows an example of a multiple ring topology that uses the EAPS common link feature to provide redundancy for the switches that connect the rings.

![Multiple Rings Sharing a Common Link](image)

**Figure 126: Multiple Rings Sharing a Common Link**

An EAPS common link is a physical link that carries overlapping VLANs that are protected by more than one EAPS domain.

In the example shown earlier in the preceding figure, switch S5 could be a single point of failure. If switch S5 were to go down, users on Ring 1 would not be able to communicate with users on Ring 2. To make the network more resilient, you can add another switch. A second switch, S10, connects to both rings and to S5 through a common link, which is common to both rings.

The EAPS common link in the following figure requires special configuration to prevent a loop that spans both rings. The software entity that requires configuration is the eaps shared-port, so the common link feature is sometimes called the *shared port* feature.

**Note**

If the shared port is not configured and the common link goes down, a superloop between the multiple EAPS domains occurs.

The correct EAPS common link configuration requires an EAPS shared port at each end of the common link. The role of the shared port (and switch) at each end of the common link must be configured as either controller or partner. Each common link requires one controller and one partner for each EAPS domain. Typically the controller and partner nodes are distribution or core switches. A controller or partner can also perform the role of master or transit node within its EAPS domain.

During normal operation, the master node on each ring protects the ring as described in [*EAPS Single Ring Topology*](#) on page 951. The controller and partner nodes work together to protect the overlapping VLANs from problems caused by a common link failure or a failed controller (see the following figure).
Figure 127: Master Node Operation in a Multiple Ring Topology

If a link failure occurs in one of the outer rings, only a single EAPS domain is affected. The EAPS master detects the failure in its domain, and converges around the failure. In this case, the controller does not take any blocking action, and EAPS domains on other rings are not affected. Likewise, when the link is restored, only the local EAPS domain is affected. The controller and any EAPS domains on other rings are not affected, and continue forwarding traffic normally.

To detect common-link faults, the controller and partner nodes send segment health check messages at one-second intervals to each other through each segment. A segment is the ring communication path between the controller and partner. The common link completes the ring, but it is a separate entity from the segment. To discover segments and their up or down status, segment health-check messages are sent from controller to partner, and also from partner to controller (see the following figure).

Figure 128: Segment Health-Check Messages

Common Link Fault Detection and Response

With one exception, when a common link fails, each master node detects the failure and unblocks its secondary port, as shown in the following figure.
Because the secondary port of each master node is now unblocked, the new topology introduces a broadcast loop spanning the outer rings.

The controller and partner nodes immediately detect the loop, and the controller does the following:
- Selects an active-open port for protected VLAN communications.
- Blocks protected VLAN communications on all segment ports except the active-open port.

**Note**
When a controller goes into or out of the blocking state, the controller sends a flush-fdb message to flush the FDB in each of the switches in its segments. In a network with multiple EAPS ports in the blocking state, the flush-fdb message gets propagated across the boundaries of the EAPS domains.

The exception mentioned above occurs when the partner node is also a master node, and the shared port that fails is configured as a primary port. In this situation, the master node waits for a link-down PDU from the controller node before opening the secondary port. This delay prevents a loop that might otherwise develop if the master/partner node detects the link failure before the controller node.

**Note**
If the common link and a ring link fail, and if the common link restores before the ring link, traffic down time can be as long as three seconds. This extended delay is required to prevent loops during the recovery of multiple failed links.

The master node selects the active-open port differently for the following EAPS configurations:
- Multiple ring topology without a PBBN
- Multiple ring topology with a PBBN

When no PBBN is present and the common link fails, the controller node selects the active-open port by choosing the lowest port number from the group of segment ports in the Up state. If the active-open port fails, the controller selects another active-open port using the same criteria. If the original active-open port recovers, the controller does not revert back to that port. When planning your
configuration, you might want to plan your port configurations so that the desired active-open port (for example, a high bandwidth link) has a lower port number than other segment ports.

**Note**

The order that you add EAPS domains to EAPS shared ports is relevant if the EAPS domains have matching ring ports and participate in spatial reuse. In this case, the `show eaps shared-port {port} {detail}` command displays the newly added EAPS domain after all other existing EAPS domains with the same matching ring port.

When the topology supports both EAPS and a PBBN (as shown in the following figure), the controller node automatically learns the relationship between the access VLANs (CVLANs or SVLANs) and the core VLAN (BVLAN). If the common link fails in this configuration, the master node selects the port leading to the BVLAN as the active-open port, providing priority support for protected VLANs on the core network. (For an example, see **Example EAPS and PBB Configuration** on page 1001.)

**Figure 130: Combined EAPS and PBBN Topology**

In the figure above, for example, the BVLAN EAPS ring protects the core network, which is made up of switches S1, S2, S3, and S4. Switch S2 is the master for this ring and blocks the secondary port to prevent a network loop. A common link between switches S1 and S3 supports the BVLAN, SVLAN1, and SVLAN2 EAPS rings.

If the common link between S1 and S3 fails, switches S2, S5, and S6 unblock their secondary EAPS ports to maintain connectivity to all devices on each ring. To prevent a super loop and give priority to the core network, the S1 controller declares the port leading to switch S2 as the active-open port and blocks protected VLAN communications on the segment ports leading to switches S5 and S6. If the active-open port fails, the controller selects another segment port as the active-open port. If the original active-open port recovers, the controller reverts back to the original active-open port.

If you have an EAPS configuration with multiple common links and a second common link fails, the controllers continue to take steps to prevent a superloop. In addition to having one controller with an active-open port, the controller with the smallest link ID becomes the root blocker. There can be only one root blocker in the network.

**Common Link Recovery**

When a common link recovers, each master node detects that the ring is complete and immediately blocks their secondary ports. The controller also detects the recovery and puts its shared port to the common link into a temporary blocking state called pre-forwarding as shown in the following figure.
Because the topology has changed, the EAPS nodes must learn the new traffic paths. Each master node notifies all switches in their domain to clear their FDB tables, and traditional Ethernet bridge learning and forwarding mechanisms establish the new traffic paths. Once the controller receives flush-fdb messages for all of its connected EAPS domains, the controller shared-port state for the common link changes to forwarding, the controller state changes to Ready, and traffic flows normally as shown in the following figure.

**Figure 132: Common-Link Restored**

**Controller and Partner Node States**

EAPS controller and partner nodes can be in the following states:
- **Ready**—Indicates that the EAPS domains are running, the common-link neighbor can be reached through segment health-checks, and the common link is up.
- **Blocking**—Indicates that the EAPS domains are running, the common-link neighbor can be reached through segment health-checks, but the common-link is down. Only the controller node (and not the partner) performs blocking.
- **Preforwarding**—Indicates the EAPS domain was in a blocking state, and the common link was restored. The controller port is temporarily blocked to prevent a loop during state transition from Blocking to Ready.
- **Idle**—Indicates the EAPS common-link neighbor cannot be reached through segment health-check messages.

**Spatial Reuse with an EAPS Common Link**

The common-link topology supports multiple EAPS domains (spatial reuse) on each ring as shown in the following figure.

**Figure 133: EAPS Common Link Topology with Spatial Reuse**

---

**Note**

If you are using the older method of enabling STP instead of EAPSv2 to block the super loop in a shared-port environment, you can continue to do so. In all other scenarios, we recommend that you do not use both STP and EAPS on the same port.

**Additional Common Link Topology Examples**

**Basic Core Topology**

The following figure shows a core topology with two access rings. In this topology, there are two EAPS common links.
Figure 134: Basic Core Topology

Right-Angle Topology

In the right-angle topology, there are still two EAPS common links, but the common links are adjacent to each other.

To configure a right-angle topology, there must be two common links configured on one of the switches. The following figure shows a right-angle topology.

Figure 135: Right-Angle Topology

Combined Basic Core and Right-Angle Topology

The following figure shows a combination basic core and right-angle topology.
Figure 136: Basic Core and Right Angle Topology

The following figure shows an extension of the basic core and right angle configuration.

Figure 137: Advanced Basic Core and Right Angle Topology

Large Core and Access Ring Topology

The following figure shows a single large core ring with multiple access rings hanging off of it.

This is an extension of a basic core configuration.
Fast Convergence

The fast convergence mode allows EAPS to converge more rapidly. In EAPS fast convergence mode, the link filters on EAPS ring ports are turned off. In this case, an instant notification is sent to the EAPS process if a port’s state transitions from up to down or vice-versa.

You must configure fast convergence for the entire switch, not by EAPS domain.

EAPS and Hitless Failover--Modular Switches and SummitStack Only

When you install two Management Switch Fabric Modules (MSMs) or Management Modules (MMs) in a BlackDiamond chassis or use redundancy in a SummitStack, one MSM/MM (node) assumes the role of primary and another node assumes the role of backup.

The primary node executes the switch’s management functions, and the backup node acts in a standby role. Hitless failover transfers switch management control from the primary to the backup and maintains the state of EAPS. EAPS supports hitless failover. You do not explicitly configure hitless failover support; rather, if you have two MSMs/MMs installed in a chassis or you are operating with redundancy in a SummitStack, hitless failover is available.

Note
Not all platforms support hitless failover in the same software release. To verify if the software version you are running supports hitless failover, see the following table in Managing the Switch on page 44. For more information about protocol, platform, and MSM/MM support for hitless failover, see Understanding Hitless Failover Support on page 64.
To support hitless failover, the primary node replicates all EAPS PDUs to the backup, which allows the backup to be aware of the EAPS domain state. Since both nodes receive EAPS PDUs, each node maintains equivalent EAPS states.

By knowing the state of the EAPS domain, the EAPS process running on the backup node can quickly recover after a primary node failover. Although both nodes receive EAPS PDUs, only the primary transmits EAPS PDUs to neighboring switches and actively participates in EAPS.

**Note**
For instructions on how to manually initiate hitless failover, see Relinquishing Primary Status on page 61.

### EAPS Licensing

Different EAPS features are offered at different license levels.

For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for these features, see Feature License Requirements.

### Configuring EAPS

**Single Ring Configuration Tasks**

To configure and enable an EAPS protected ring, do the following on each ring node:

1. Create an EAPS domain and assign a name to the domain as described in Creating and Deleting an EAPS Domain on page 964.
2. Create and add the control VLAN to the domain as described in Adding the EAPS Control VLAN on page 964.
3. Create and add the protected VLAN(s) to the domain as described in Adding Protected VLANs on page 965.
4. Configure the EAPS mode (master or transit) for the switch in the domain as described in Defining the Switch Mode (Master or Transit) on page 965.
5. Configure the EAPS ring ports, including the master primary and secondary ring ports, as described in Configuring the Ring Ports on page 966.
6. If desired, configure the polling timers and timeout action as described in Configuring the Polling Timers and Timeout Action on page 966.*
7. Enable EAPS for the entire switch as described in Enabling and Disabling EAPS on the Switch on page 967.
8 If desired, enable Fast Convergence as described in Enabling and Disabling Fast Convergence on page 968.*
9 Enable EAPS for the specified domain as described in Enabling and Disabling an EAPS Domain on page 968.

**Note**
If you configure a VMAN on a switch running EAPS, make sure you configure the VMAN attributes on all of the switches that participate in the EAPS domain. For more information about VMANs, see VMAN (PBN) and PBBN.

---

**Creating and Deleting an EAPS Domain**

Each EAPS domain is identified by a unique domain name.

- To create an EAPS domain, use the following command:
  ```
  create eaps name
  ```
- To delete an EAPS domain, use the following command:
  ```
  delete eaps name
  ```

**Adding the EAPS Control VLAN**

You must create and configure one control VLAN for each EAPS domain. For instructions on creating a VLAN, see VLANs on page 503.

- To configure EAPS to use a VLAN as the EAPS control VLAN for a domain, use the following command:
  ```
  configure eaps name add control {vlan} vlan_name
  ```

**Note**
A control VLAN cannot belong to more than one EAPS domain. If the domain is active, you cannot delete the domain or modify the configuration of the control VLAN.

The control VLAN must NOT be configured with an IP address. In addition, only ring ports may be added to this control VLAN. No other ports can be members of this VLAN. Failure to observe these restrictions can result in a loop in the network.

The ring ports of the control VLAN must be tagged.

By default, EAPS PDUs are automatically assigned to QoS profile QP8. This ensures that the control VLAN messages reach their intended destinations. You do not need to configure a QoS profile for the control VLAN.
Adding Protected VLANs

You must add one or more protected VLANs to each EAPS domain. The protected VLANs are the data-carrying VLANs.

**Note**
When you configure a protected VLAN, the ring ports of the protected VLAN must be tagged (except in the case of the default VLAN).

For instructions on creating a VLAN, see VLANs on page 503.

- To configure a VLAN as an EAPS protected VLAN, use the following command:
  ```
  configure eaps name add protected {vlan} vlan_name
  ```

Configuring the EAPS Domain Priority

The EAPS domain priority feature allows you to select the EAPS domains that are serviced first when a break occurs in an EAPS ring. For example, you might set up a network topology with two or more domains on the same physical ring, such as in spatial reuse. In this topology, you could configure one domain as high priority and the others as normal priority. You would then add a small subset of the total protected VLANs to the high priority domain, and add the rest of the protected vlans to the normal priority domain. The secondary port of the normal and high priority domains can be the same, or as is typically the case of spatial reuse, opposite. If a ring fault occurs in this topology, the protected VLANs in the high priority domain are the first to recover.

- To configure the EAPS domain priority, use the following command:
  ```
  configure eaps name priority {high | normal}
  ```

Defining the Switch Mode (Master or Transit)

We recommend keeping the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary.

1. Configure the EAPS switch mode for a domain using the following command:
   ```
   configure eaps name mode [master | transit]
   ```
   One switch on the ring must be configured as the master node for the specified domain; all other switches on the same ring and domain are configured as transit nodes.

   If you configure a switch to be a transit node for an EAPS domain, the default switch configuration displays the following message and prompts you to confirm the command:
   **WARNING:** Make sure this specific EAPS domain has a Master node in the ring. If you change this node from EAPS master to EAPS transit, you could cause a loop in the network. Are you sure you want to change mode to transit? (y/n)

2. When prompted, do one of the following:
   - Enter **y** to identify the switch as a transit node.
   - Enter **n** or press [Return] to cancel the command.

For more information see, Disabling EAPS Loop Protection Warning Messages on page 969.
Configuring the Ring Ports

Each node on the ring connects to the ring through two ring ports. The ports that you choose on each switch should be tagged and added to the control VLAN and all protected VLANs. For information on adding tagged ports to a VLAN, see VLANs on page 503.

On the master node, one ring port must be configured as the primary port, and the other must be configured as the secondary port.

We recommend that you keep the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary.

1 To configure a node port as primary or secondary, use the following command:

   \texttt{configure eaps name [primary | secondary] port ports}

   If you attempt to add an EAPS ring port to a VLAN that is not protected by EAPS, the default switch configuration prompts you to confirm the command with the following message:
   
   \texttt{Make sure <vlan_name> is protected by EAPS. Adding EAPS ring ports to a VLAN could cause a loop in the network. Do you really want to add these ports (y/n)}

2 When prompted, do one of the following:
   - Enter \texttt{y} to identify the switch as a transit node.
   - Enter \texttt{n} or press [Return] to cancel the command.

For information on configuring a VLAN for EAPS, see the following sections:

- Adding the EAPS Control VLAN on page 964
- Adding Protected VLANs on page 965

For more information see, Disabling EAPS Loop Protection Warning Messages on page 969.

Configuring the Polling Timers and Timeout Action

The polling timers provide an alternate way to detect ring breaks. In a ring that uses only Extreme Networks switches, the master switch learns about a ring break by receiving a link-down PDU. When the ring uses only Extreme networks switches, the polling timers are not needed and can remain configured for the default values.

In a ring that contains switches made by other companies, the polling timers provide an alternate way to detect ring breaks. The master periodically sends hello PDUs at intervals determined by the hello PDU timer and waits for a reply. If a hello PDU reply is not received before the failtime timer expires, the switch detects a failure and responds by either sending an alert or opening the secondary port. The response action is defined by a configuration command.

- Set the polling timer values the master node uses for detecting ring failures.

   \texttt{configure eaps name hellotime seconds milliseconds}
configure eaps name failtime seconds milliseconds

Note
These commands apply only to the master node. If you configure the polling timers for a transit node, they are ignored. If you later reconfigure that transit node as the master node, the polling timer values are used as the current values.

Use the **hellotime** keyword and its associated parameters to specify the amount of time the master node waits between transmissions of health check messages on the control VLAN. The combined value for seconds and milliseconds must be greater than 0. The default value is 1 second.

Use the **failtime** keyword and its associated parameters to specify the amount of time the master node waits before the failtimer expires. The combined value for seconds and milliseconds must be greater than the configured value for **hellotime**. The default value is 3 seconds.

Note
Increasing the failtime value increases the time it takes to detect a ring break using the polling timers, but it can also reduce the possibility of incorrectly declaring a failure when the network is congested.

- Configure the action taken when a ring break is detected.

```
configure eaps name failtime expiry-action [open-secondary-port | send-alert]
```

Use the send-alert parameter to send an alert when the failtimer expires. Instead of going into a failed state, the master node remains in a Complete or Init state, maintains the secondary port blocking, and writes a critical error message to syslog warning the user that there is a fault in the ring. An SNMP trap is also sent.

Use the open-secondary-port parameter to open the secondary port when the failtimer expires.

**Enabling and Disabling EAPS on the Switch**

We recommend that you keep the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary.

- To enable the EAPS function for the entire switch, use the following command:

```
enable eaps
```

- To disable the EAPS function for the entire switch, use the following command:

```
disable eaps
```

If you enter the command to disable EAPS, the default switch configuration displays the following warning message and prompts you to confirm the command:

```
WARNING: Disabling EAPS on the switch could cause a loop in the network! Are you sure you want to disable EAPS? (y/n)
```

- When prompted, do one of the following:
  a. Enter **y** to disable EAPS for the entire switch.
  b. Enter **n** or press [Return] to cancel the command.

For more information see, [Disabling EAPS Loop Protection Warning Messages](#) on page 969.
Enabling and Disabling Fast Convergence

You can enable or disable fast convergence for the entire switch to improve EAPS convergence times.

**Note**
Possible factors affecting EAPS fast convergence time:

- The medium type of the link being flapped (Fiber link-down events are detected faster than copper, causing better convergence).
- Number of VLANs protected by the EAPS domain (convergence time increases with the number of protected VLANs).
- Number of FDB entries present during the switch over (convergence time increases with the number of FDBs learned).
- Topology change event (link down or link up) causes the master node to send an FDB flush to all transits. In the event of a shared port failure, FDB is flushed twice, causing an increase in convergence time.
- Number of hops between the switch where the link flap happens and the master node (convergence increases with the number of hops).

- To enable or disable fast convergence on the switch, use the following command:
  ```
  configure eaps fast-convergence [off | on]
  ```

Enabling and Disabling an EAPS Domain

We recommend that you keep the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary.

- To enable a specific EAPS domain, use the following command:
  ```
  enable eaps {name}
  ```
- To disable a specific EAPS domain, use the following command:
  ```
  disable eaps {name}
  ```

If you enter the `disable eaps` command, the default switch configuration displays the following warning message and prompts you to confirm the command:

**WARNING:** Disabling specific EAPS domain could cause a loop in the network! Are you sure you want to disable this specific EAPS domain? (y/n)

- When prompted, do one of the following:
  a. Enter `y` to disable EAPS for the specified domain.
  b. Enter `n` or press [Return] to cancel the command.

For more information see, [Disabling EAPS Loop Protection Warning Messages](#) on page 969.
Configuring EAPS Support for Multicast Traffic

The ExtremeXOS software provides several commands for configuring how EAPS supports multicast traffic after an EAPS topology change.

**Note**

EAPS multicast flooding must be enabled before the add-ring-ports feature will operate. For information on enabling EAPS multicast flooding, see the command:

```bash
configure eaps multicast temporary-flooding [on | off]
```

Unconfiguring an EAPS Ring Port

Unconfiguring an EAPS port sets its internal configuration state to INVALID, which causes the port to appear in the Idle state with a port status of Unknown. This occurs when you use the `show eaps {eapsDomain} {detail}` command to display the status information about the port.

We recommend that you keep the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary.

1. To unconfigure an EAPS primary or secondary ring port for an EAPS domain, use the following command:

   ```bash
   unconfigure eaps eapsDomain [primary | secondary] port
   ```

   To prevent loops in the network, the switch displays by default a warning message and prompts you to unconfigure the specified EAPS primary or secondary ring port.

2. When prompted, do one of the following:
   a. Enter `y` to unconfigure the specified port.
   b. Enter `n` or press `[Return]` to cancel this action.

   The following command example unconfigures this node’s EAPS primary ring port on the domain “eaps_1”:

   ```bash
   unconfigure eaps eaps_1 primary port
   ```

   Warning: Unconfiguring the Primary port from the EAPS domain could cause a loop in The network! Are you sure you want to unconfigure the Primary EAPS Port? (y/n)

3. Enter `y` to continue and unconfigure the EAPS primary ring port. Enter `n` to cancel this action.

   The switch displays a similar warning message if you unconfigure the secondary EAPS port.

   For more information see, **Disabling EAPS Loop Protection Warning Messages** on page 969.

Disabling EAPS Loop Protection Warning Messages

The switch displays by default loop protection messages when configuring the following EAPS parameters:

- Adding EAPS primary or secondary ring ports to a VLAN
- Deleting a protected VLAN
- Disabling the global EAPS setting on the switch
• Disabling an EAPS domain
• Configuring an EAPS domain as a transit node
• Unconfiguring EAPS primary or secondary ring ports from an EAPS domain

We recommend keeping the loop protection warning messages enabled. If you have considerable knowledge and experience with EAPS, you might find the EAPS loop protection warning messages unnecessary. For example, if you use a script to configure your EAPS settings, disabling the warning messages allows you to configure EAPS without replying to each interactive yes/no question.

• To disable loop protection messages, use the following command:
  ```
  configure eaps config-warnings off
  ```
• To re-enable loop protection messages, use the following command:
  ```
  configure eaps config-warnings on
  ```

Common Link Topology Configuration Tasks

To create a common link topology, you must configure the shared ports at each end of the common link.

**EAPS Shared Port Configuration Rules**

The following rules apply to EAPS shared port configurations:

• Each common link in the EAPS network must have a unique link ID, which is configured at the shared port at each end of the link.
• The shared port mode configured on each side of a common link must be different from the other; one must be a controller and one must be a partner.
• The controller and partner shared ports on either side of a common link must have the same link ID. The common link is established only when the shared ports at each end of the common link have the same link ID.
• There can be up to two shared ports per switch.
• There cannot be more than one controller on a switch.

Valid combinations on any one switch are:

• 1 controller
• 1 partner
• 1 controller and 1 partner
• 2 partners
• A shared port cannot be configured on an EAPS master’s secondary port.

**Note**

When a common link fails, one of the segment ports becomes the active-open port, and all other segment ports are blocked to prevent a loop for the protected VLANs. For some topologies, you can improve network performance during a common link failure by selecting the port numbers to which segments connect. For information on how the active-open port is selected, see Common Link Fault Detection and Response.
Common Link Configuration Overview

To configure and enable a common link to serve multiple rings, do the following on the controller and partner nodes:

1. Create a shared port for the common link as described in Creating and Deleting a Shared Port on page 971.
2. Configure the shared port as either a controller or a partner as described in Defining the Mode of the Shared Port on page 971.
3. Configure the link ID on the shared port as described in Configuring the Link ID of the Shared Port on page 971.
4. If desired, configure the polling timers and timeout action as described in Configuring the Shared Port Timers and Timeout Action on page 972. This step can be configured at any time, even after the EAPS domains are running.
5. Configure EAPS on each ring as described in Single Ring Configuration Tasks on page 963.

Creating and Deleting a Shared Port

To configure a common link, you must create a shared port on each switch belonging to the common link.

- To create a shared port, use the following command:

  `create eaps shared-port ports`

  Where `ports` is the common link port.

  **Note**

  A switch can have a maximum of two shared ports.

- To delete a shared port on the switch, use the following command:

  `delete eaps shared-port ports`

Defining the Mode of the Shared Port

The shared port on one end of the common link must be configured to be the controller. This is the end responsible for blocking ports when the common link fails, thereby preventing the superloop.

The shared port on the other end of the common link must be configured to be the partner. This end does not participate in any form of blocking. It is responsible for only sending and receiving health-check messages.

- To configure the mode of the shared port, use the following command:

  `configure eaps shared-port ports mode controller | partner`

Configuring the Link ID of the Shared Port

Each common link in the EAPS network must have a unique link ID. The controller and partner shared ports that belong to the same common link must have matching link IDs. No other instance in the network should have that link ID.
If you have multiple adjacent common links, we recommend that you configure the link IDs in ascending order of adjacency. For example, if you have an EAPS configuration with three adjacent common links, moving from left to right of the topology, configure the link IDs from the lowest to the highest value.

- To configure the link ID of the shared port, use the following command:
  
  ```
  configure eaps shared-port ports link-id id
  ```

  The link ID range is 1–65534.

**Configuring the Shared Port Timers and Timeout Action**

- To configure the shared port timers, use the following commands:
  
  ```
  configure eaps shared-port port common-path-timers {[health-interval | timeout] seconds}
  ```

  ```
  configure eaps shared-port port segment-timers health-interval seconds
  ```

  ```
  configure eaps shared-port port segment-timers timeout seconds
  ```

- To configure the time out action for segment timers, use the following command:

  ```
  configure eaps shared-port port segment-timers expiry-action [segment-down | send-alert]
  ```

**Unconfiguring an EAPS Shared Port**

- To unconfigure a link ID on a shared port, use the following command:

  ```
  unconfigure eaps shared-port ports link-id
  ```

- To unconfigure the mode on a shared port, use the following command:

  ```
  unconfigure eaps shared-port ports mode
  ```

- To delete a shared port, use the following command:

  ```
  delete eaps shared-port ports
  ```

**Clearing the EAPS Counters**

The EAPS counters continue to increment until you explicitly clear the information. By clearing the counters, you can see fresh statistics for the time period you are monitoring.

- To clear the counters used by EAPS, use the following commands:

  ```
  clear counters
  ```

  ```
  clear eaps counters
  ```

**Displaying EAPS Information**
Displaying Single Ring Status and Configuration Information

- To display EAPS status and configuration information, use the following command:

  ```
  show eaps {eapsDomain} {detail}
  ```

  **Note**
  You might see a slightly different display, depending on whether you enter the command on the master node or the transit node.

If you specify a domain with the optional `eapsDomain` parameter, the command displays status information for a specific EAPS domain.

The display from the `show eaps detail` command shows all the information shown in the `show eaps eapsDomain` command for all configured EAPS domains.

Displaying Domain Counter Information

- To display EAPS counter information for one or all domains, use the following command:

  ```
  show eaps counters [eapsDomain | global]
  ```

If you specify the name of an EAPS domain, the switch displays counter information related to only that domain.

If you specify the `global` keyword, the switch displays a list of the counter totals for all domains. To see the counters for a specific domain, you must specify the domain name.

  **Note**
  If a PDU is received, processed, and consumed, only the Rx counter increments. If a PDU is forwarded in slow path, both the Rx counter and Fw counter increment.

Displaying Common Link Status and Configuration Information

Each controller and partner node can display status and configuration information for the shared port or ports on the corresponding side of the common link.

- To display EAPS common link information, use the following command:

  ```
  show eaps shared-port {port} {detail}
  ```

If you enter the `show eaps shared-port` command without an argument or keyword, the command displays a summary of status information for all configured EAPS shared ports on the switch.

If you specify a shared port, the command displays information about that specific port.

You can use the `detail` keyword to display more detailed status information about the segments and VLANs associated with each shared port.
Displaying Common Link Counter Information

Each controller and partner node can display counter information for the shared port or ports through which the switch connects to a common link.

- To display EAPS shared port counter information, use the following command:
  
  ```
  show eaps counters shared-port [global | port {segment-port segport {eapsDomain}}]
  ```

  If you specify the `global` keyword, the switch displays a list of counters that show the totals for all shared ports together. To view the counters for a single shared port, enter the command with the port number.

  If you specify a particular EAPS segment port, the switch displays counter information related to only that segment port for the specified EAPS domain.

Configuration Examples

Migrating from STP to EAPS

This section explains how to migrate or reconfigure an existing STP network to an EAPS network.

Note

Actual implementation steps on a production network may differ based on the physical topology, switch models, and software versions deployed.

The sample STP network is a simple two-switch topology connected with two Gigabit Ethernet trunk links, which form a broadcast loop. Both Extreme Networks switches are configured for 802.1D mode STP running on a single data VLAN named Data. The sample STP network for migration to EAPS is shown in the following figure.

![Figure 139: Sample STP Network for Migration to EAPS](image)

Creating and Configuring the EAPS Domain

- The first step in the migration process is to create an EAPS Domain and configure the EAPS mode, then define the primary and secondary ports for the domain. Follow this step for both switches.

  Switch2 is configured as EAPS Master to ensure the same port blocking state is maintained as in the original STP topology.

  Switch 1 EAPS domain configuration:

  ```
  * SWITCH#1.1 # create eaps new-eaps
  * SWITCH#1.2 # configure new-eaps mode transit
  ```
* SWITCH#1.3 # configure new-eaps primary port 4:1
* SWITCH#1.4 # configure new-eaps secondary port 4:2

Switch 2 EAPS domain configuration:

* SWITCH#2.1 # create eaps new-eaps
* SWITCH#2.2 # configure new-eaps mode master
* SWITCH#2.3 # configure new-eaps primary port 4:1
* SWITCH#2.4 # configure new-eaps secondary port 4:2

Creating and Configuring the EAPS Control VLAN

1. You must create the EAPS control VLAN and configure the 802.1q tag and ring ports.
2. Configure the control VLANs as part of the EAPS domain. Do this for both switches.

Switch 1 control VLAN configuration:

* SWITCH#1.5 # create vlan control-1
* SWITCH#1.6 # configure vlan control-1 tag 4001
* SWITCH#1.8 # configure vlan control-1 add port 4:1,4:2 tagged
* SWITCH#1.9 # configure eaps new-eaps add control vlan control-1

Switch 2 control VLAN configuration:

* SWITCH#2.5 # create vlan control-1
* SWITCH#2.6 # configure vlan control-1 tag 4001
* SWITCH#2.8 # configure vlan control-1 add port 4:1,4:2 tagged
* SWITCH#2.9 # configure eaps new-eaps add control vlan control-1

Enabling EAPS and Verify EAPS Status

1. Enable the EAPS protocol and the EAPS domain.
2. Confirm that the master node is in Complete state and its secondary port is blocking.

Switch 1 commands to enable EAPS and the domain:

* SWITCH#1.10 # enable eaps
* SWITCH#1.11 # enable eaps new-eaps

Switch 2 commands to enable EAPS and verify status:

* SWITCH#2.10 # enable eaps
* SWITCH#2.11 # enable eaps new-eaps
* SWITCH#2.12 # show eaps

EAPS Enabled: Yes
EAPS Fast-Convergence: Off
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1

# EAPS domain configuration :

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mo</th>
<th>En</th>
<th>Pri</th>
<th>Sec</th>
<th>Control-Vlan VID</th>
<th>Count</th>
</tr>
</thead>
</table>

---

ExtremeXOS Concepts Guide for Release 15.4 975
Configuring the STP Protected VLAN as an EAPS Protected VLAN

Configure the data VLAN (currently protected by STP as an untagged VLAN) as an EAPS protected VLAN.

1. Assign an 802.1q tag to the data VLAN, as this might not be required with the previous STP configuration.
2. Next, the data VLAN is added to the EAPS domain as a protected VLAN.
3. Configure the VLAN port changes at the end to prevent any broadcast loop from forming during the transition from STP to EAPS protection.
   A warning message is displayed on the CLI, but this can be ignored, as it is just a reminder that the ring ports have not been added to the protected VLAN yet.
4. Change the port membership for the data VLAN from untagged to 802.1q tagged trunk ports.

Switch#2 commands to add EAPS protected VLAN and tagged ports:

* SWITCH#2.13 # configure vlan data tag 1000
* SWITCH#2.14 # configure new-eaps add protect vlan data
WARNING: Primary port [4:1] is not tagged on vlan "data", EAPS="new-eaps"
WARNING: Secondary port [4:2] is not tagged on vlan "data", EAPS="new-eaps"
* SWITCH#2.15 # configure data add port 4:1,4:2 tagged

Switch#1 commands to add EAPS protected VLAN and tagged ports:

* SWITCH#1.13 # configure vlan data tag 1000
* SWITCH#1.14 # configure new-eaps add protect vlan data
WARNING: Primary port [4:1] is not tagged on vlan "data", EAPS="new-eaps"
WARNING: Secondary port [4:2] is not tagged on vlan "data", EAPS="new-eaps"
* SWITCH#1.15 # configure data add port 4:1,4:2 tagged

Verifying the EAPS Blocking State for the Protected VLAN

• To ensure there is no potential for a broadcast storm, confirm that EAPS is successfully blocking the protected VLAN, as shown in the following example:

* SWITCH#2.16 # show new-eaps
Name: new-eaps
State: Complete Running: Yes
Enabled: Yes Mode: Master
Primary port: 4:1 Port status: Up Tag status: Tagged
Secondary port: 4:2 Port status: Blocked Tag status: Tagged
Hello timer interval: 1 sec 0 millisec
Fail timer interval: 3 sec
Fail Timer expiry action: Send alert
Last valid EAPS update: From Master Id 00:04:96:10:51:50, at Fri Sep 10 13:38:39 2004
EAPS Domain’s Controller Vlan: control-1 4001
EAPS Domain’s Protected Vlan(s): data 1000
Number of Protected Vlans: 1
After you verify that EAPS is protecting the data VLAN, you can safely remove the STP configuration.

### Verifying the STP Status and Disabling STP

Once you have successfully verified that EAPS has taken over loop prevention for the data VLAN, you no longer need the STP configuration.

Now, verify whether the data VLAN is removed from the STP domain, and then disable the STP protocol.

Switch 2 commands to verify STP status and disable STP:

```
* SWITCH#2.17 # show stp s0
  Stpd: s0                Stp: ENABLED            Number of Ports: 0
  Rapid Root Failover: Disabled
  Operational Mode: 802.1D            Default Binding Mode: 802.1D
  802.1Q Tag: (none)
  Ports: (none)
  Participating Vlans: (none)
  Auto-bind Vlans: Default
  Bridge Priority: 32768
  BridgeID:               80:00:00:04:96:10:51:50
  Designated root:        80:00:00:04:96:10:51:50
  RootPathCost: 0         Root Port: ----
  MaxAge: 20s             HelloTime: 2s           ForwardDelay: 15s
  CfgBrMaxAge: 20s        CfgBrHelloTime: 2s       CfgBrForwardDelay: 15s
  Topology Change Time: 35s         Hold time: 1s
  Topology Change Detected: FALSE   Topology Change: FALSE
  Number of Topology Changes: 4
  Time Since Last Topology Change: 1435s
* SWITCH#2.18 # show s0 port
* SWITCH#2.19 # disable stp
```

Switch 1 commands to verify STP status and disable STP:

```
* SWITCH#1.16 # show stp s0
  Stpd: s0                Stp: ENABLED            Number of Ports: 0
  Rapid Root Failover: Disabled
  Operational Mode: 802.1D            Default Binding Mode: 802.1D
  802.1Q Tag: (none)
  Ports: (none)
  Participating Vlans: (none)
  Auto-bind Vlans: Default
  Bridge Priority: 1
  BridgeID:               00:01:00:04:96:10:30:10
  Designated root:        00:01:00:04:96:10:30:10
  RootPathCost: 0         Root Port: ----
  MaxAge: 20s             HelloTime: 2s           ForwardDelay: 15s
  CfgBrMaxAge: 20s        CfgBrHelloTime: 2s       CfgBrForwardDelay: 15s
  Topology Change Time: 35s         Hold time: 1s
  Topology Change Detected: FALSE   Topology Change: FALSE
  Number of Topology Changes: 2
  Time Since Last Topology Change: 11267s
* SWITCH#1.17 # show stp s0 po
```
The network should now be successfully migrated from STP to EAPS.

Designing and Implementing a Highly Resilient Enterprise Network Using EAPS

Network managers can design and employ a highly resilient end-to-end enterprise network using the Extreme Networks switching platform and the EAPS protocol as shown in the following figure.

Figure 140: Extreme Networks EAPS Everywhere

EAPS can be used in the network edge to provide link resiliency for Ethernet and IP services in a partial-meshed design. In the aggregation layer, EAPS interconnects multiple edge and core domains. When combined with VRRP and OSPF in the aggregation layer, EAPS provides the foundation for highly resilient IP routing by protecting against link and switch failures.
In the network core, EAPS is used with OSPF to provide a high-performance IP routing backbone with zero downtime or route flaps. Using EAPS and dual-homed server farms in the data center provides high availability for mission-critical server resources.

The collapsed core/aggregation layer and data center also make use of EAPS resilient ring topology to ensure network availability to all critical sources.

*Designing and Configuring the Unified Access Layer*

The unified access network layer makes use of EAPS in a partial-meshed ring topology for maximum resiliency. The edge of the network is the first point of entry for client devices such as PCs, servers, VoIP phones, wireless devices, and printers.

Utilizing EAPS and redundant uplink ports on edge switches increases network resiliency and availability. Edge switches connect their primary and secondary uplink trunk ports to one or more switches in the aggregation network layer (as shown in the following figure). If the primary uplink port fails, traffic can use the alternate secondary uplink.

---

**Figure 141: Converged Network Edge (Unified Access Layer)**

In this sample network, each edge switch is configured with a unique EAPS domain and control VLAN. Protected VLANs can overlap across multiple EAPS domains, or remain local to their own domain.

By putting each edge switch and VLAN into a separate EAPS domain, you gain resiliency and management benefits. First, any link or switch failures in one ring do not affect the other edge switches. Also, this type of modular design allows you to add edge switches easily without impacting other parts...
of the network. Troubleshooting becomes easier as the scope of failures can be quickly isolated to a specific EAPS ring or switch.

This section describes how to design the access edge network switches as EAPS transit nodes to provide Ethernet L2 connectivity services. In this example, upstream aggregation switches perform Layer 3 (L3) inter-VLAN routing functions. Although not discussed in the scope of this section, the edge switches could also be configured with additional routing, QoS, WLAN, or security features.

Creating and Configuring the EAPS Domain

- Create the EAPS domain, configure the switch as a transit node, and define the EAPS primary and secondary ports as shown in the following example:
  - Edge-Switch#1:1 # create eaps e1-domain
  - Edge-Switch#1:2 # configure eaps e1-domain mode transit
  - Edge-Switch#1:3 # configure eaps e1-domain primary port 49
  - Edge-Switch#1:4 # configure eaps e1-domain secondary port 50

Creating and Configuring the EAPS Control VLAN

1. Create the EAPS control VLAN and configure its 802.1q tag and ring ports.
2. Configure the control VLAN as part of the EAPS domain. The control VLAN only contains the EAPS primary and secondary ports configured earlier. The following commands accomplish these tasks:
  - Edge-Switch#1:5 # create vlan control-1
  - Edge-Switch#1:6 # configure vlan control-1 tag 4000
  - Edge-Switch#1:8 # configure vlan control-1 add port 49,50 tagged
  - Edge-Switch#1:9 # configure eaps e1-domain add control vlan control-1

Creating and Configuring EAPS Protected VLANs

1. Create at least one EAPS protected VLAN, and configure its 802.1q tag and ports.
2. Configure the protected VLAN as part of the EAPS domain.
   The Protect VLAN contains the EAPS primary and secondary ports as tagged VLAN ports. Additional VLAN ports connected to client devices such as a PC could be untagged or tagged. The following commands accomplish these tasks and should be repeated for all additional protected VLANs:
   - Edge-Switch#1:10 # create vlan purple-1
   - Edge-Switch#1:11 # configure purple-1 tag 1
   - Edge-Switch#1:12 # configure purple-1 add port 49,50 tagged
   - Edge-Switch#1:13 # configure purple-1 add port 1 untagged
   - Edge-Switch#1:14 # configure eaps e1-domain add protect vlan purple-1

Enabling the EAPS Protocol and EAPS Domain

- Enable EAPS to run on the domain as shown in the following example:
  - Edge-Switch#1:15 # enable eaps
  - Edge-Switch#1:16 # enable eaps e1-domain
Verifying the EAPS Configuration and Status

- The command in the following example allows you to verify that the EAPS configuration is correct and that the EAPS state is Links-Up.

  Both ring ports must be plugged in to see the Links-Up state.

* Edge-Switch#1:17 # show eaps el-domain detail
Name: "el-domain" (instance=0) Priority: High
State: Links-Up                  Running: Yes
Enabled: Yes                    Mode: Transit
Primary port: 49                Port status: Up   Tag status: Tagged
Secondary port: 50              Port status: Up   Tag status: Tagged
Hello Timer interval: 1 sec     0 millisec
Fail Timer interval: 3 sec
Preforwarding Timer interval: 0 sec
Last valid EAPS update: From Master Id 00:04:96:10:51:50, at Sun Sep 5
23:20:10 2004
EAPS Domain has following Controller Vlan:
Vlan Name             VID
"control-1"            4000
EAPS Domain has following Protected Vlan(s):
Vlan Name             VID
"purple-1"             0001
Number of Protected Vlans: 1

Designing and Configuring the Aggregation Layer

The network switches in the aggregation layer provide additional resiliency benefits.

In the following example, aggregation switches are typically deployed in pairs that protect against single switch failures. Each aggregation switch is physically connected to all edge switches and participates in multiple EAPS domains. The aggregation switches can serve a different role within each EAPS domain, with one switch acting as a transit node and the other as a master node.

In this example, we have a common link with overlapping domains (and protected VLANs), which includes an EAPS controller and partner configuration. The result is a partial-mesh network design of EAPS from the access edge to the aggregation layer (see the following figure).
The aggregation switches are configured to act as multi-function EAPS nodes to provide L2 connectivity services. After EAPS and L2 connectivity is configured, additional L3 routing configuration can be added.

Using redundant aggregation switches helps protect against a single point of failure at the switch level, while EAPS domains provide fault isolation and minimize the impact that failures have on the network. With shared port configurations, the partial-mesh physical design is maintained without broadcast loops, regardless of where a failure might occur.

To configure the L2 aggregate switches, complete the tasks described in the following sections on all aggregate switches:

1. Create and configure the EAPS domains.
2. Create and configure the EAPS control VLANs.
3. Create and configure the EAPS shared ports.
4. Enable the EAPS protocol and EAPS domain.
5. Create and configure the EAPS protected VLANs.
6. Verify the EAPS configuration and operating state.

Creating and Configuring the EAPS Domains

- Create the EAPS domains for each ring (one domain for one edge switch) and configure the EAPS mode.

Define the primary and secondary ports for each domain. In this example, however, the primary port is the same as the common link. One aggregation switch has EAPS mode configured as master and partner, while the other aggregation switch is configured as transit and controller.

EAPS master node configuration:

* AGG-SWITCH#2.1 # create eaps e1-domain
* AGG-SWITCH#2.2 # create eaps e2-domain
* AGG-SWITCH#2.3 # create eaps e3-domain
* AGG-SWITCH#2.4 # create eaps e4-domain
* AGG-SWITCH#2.5 # configure eaps e1-domain mode master
* AGG-SWITCH#2.6 # configure eaps e2-domain mode master
* AGG-SWITCH#2.7 # configure eaps e3-domain mode master
* AGG-SWITCH#2.8 # configure eaps e4-domain mode master
* AGG-SWITCH#2.9 # configure eaps e1-domain primary port 2:1
* AGG-SWITCH#2.10 # configure eaps e1-domain secondary port 1:1
* AGG-SWITCH#2.11 # configure eaps e2-domain primary port 2:1
* AGG-SWITCH#2.12 # configure eaps e2-domain secondary port 1:4
* AGG-SWITCH#2.13 # configure eaps e3-domain primary port 2:1
* AGG-SWITCH#2.14 # configure eaps e3-domain secondary port 3:1
* AGG-SWITCH#2.15 # configure eaps e4-domain primary port 2:1
* AGG-SWITCH#2.16 # configure eaps e4-domain secondary port 3:2

EAPS transit node configuration:

* AGG-SWITCH#1.1 # create eaps e1-domain
* AGG-SWITCH#1.2 # create eaps e2-domain
* AGG-SWITCH#1.3 # create eaps e3-domain
* AGG-SWITCH#1.4 # create eaps e4-domain
* AGG-SWITCH#1.5 # configure eaps e1-domain mode transit
* AGG-SWITCH#1.6 # configure eaps e2-domain mode transit
* AGG-SWITCH#1.7 # configure eaps e3-domain mode transit
* AGG-SWITCH#1.8 # configure eaps e4-domain mode transit
* AGG-SWITCH#1.9 # configure eaps e1-domain primary port 2:1
* AGG-SWITCH#1.10 # configure eaps e1-domain secondary port 1:1
* AGG-SWITCH#1.11 # configure eaps e2-domain primary port 2:1
* AGG-SWITCH#1.12 # configure eaps e2-domain secondary port 1:4
* AGG-SWITCH#1.13 # configure eaps e3-domain primary port 2:1
* AGG-SWITCH#1.14 # configure eaps e3-domain secondary port 3:1
* AGG-SWITCH#1.15 # configure eaps e4-domain primary port 2:1
* AGG-SWITCH#1.16 # configure eaps e4-domain secondary port 3:2
Creating and Configuring the EAPS Control VLANs

1. Create the EAPS control VLANs (one for each domain) and configure the 802.1q tag and ring ports for each.
2. Configure the control VLANs as part of their respective EAPS domain.

The control VLAN only contains the EAPS primary and secondary ports configured earlier. The following commands are entered on both aggregate switches:

* AGG-SWITCH.17 # create vlan control-1
* AGG-SWITCH.18 # create vlan control-2
* AGG-SWITCH.19 # create vlan control-3
* AGG-SWITCH.20 # create vlan control-4
* AGG-SWITCH.21 # configure vlan control-1 tag 4001
* AGG-SWITCH.22 # configure vlan control-2 tag 4002
* AGG-SWITCH.23 # configure vlan control-3 tag 4003
* AGG-SWITCH.24 # configure vlan control-4 tag 4004
* AGG-SWITCH.29 # configure vlan control-1 add port 2:1,1:1 tagged
* AGG-SWITCH.30 # configure vlan control-2 add port 2:1,1:4 tagged
* AGG-SWITCH.31 # configure vlan control-3 add port 2:1,3:1 tagged
* AGG-SWITCH.32 # configure vlan control-4 add port 2:1,3:2 tagged
* AGG-SWITCH.33 # configure eaps e1-domain add control vlan control-1
* AGG-SWITCH.34 # configure eaps e2-domain add control vlan control-2
* AGG-SWITCH.35 # configure eaps e3-domain add control vlan control-3
* AGG-SWITCH.36 # configure eaps e4-domain add control vlan control-4

Creating and Configuring the EAPS Shared Ports

- Create the EAPS shared ports, which are used to connect a common-link between the aggregate switches.

On the first switch, define the shared port mode as partner, and define the link ID. Repeat this step on the other aggregate switch, but configure the shared port mode as controller. The link ID matches the value configured for the partner.

The following shows an example configuration for the partner:

* AGG-SWITCH#2.37 # create eaps shared-port 2:1
* AGG-SWITCH#2.38 # configure eaps shared-port 2:1 mode partner
* AGG-SWITCH#2.39 # configure eaps shared-port 2:1 link-id 21

Enabling the EAPS Protocol and EAPS Domain

- Enable the EAPS protocol on the switch, and enable EAPS to run on each domain created.

The following commands are entered on both aggregate switches.

* AGG-SWITCH.40 # enable eaps
* AGG-SWITCH.41 # enable eaps e1-domain
* AGG-SWITCH.42 # enable eaps e2-domain
* AGG-SWITCH.43 # enable eaps e3-domain
* AGG-SWITCH.44 # enable eaps e4-domain

Creating and Configuring the EAPS Protected VLANs

1. Create the EAPS protected VLANs for each domain.
2 Configure an 802.1q tag and the ports for each protected VLAN.

3 Configure each protected VLAN as part of the EAPS domain.

Depending on the scope of the VLAN, it could be added to multiple EAPS domains. This type of VLAN is referred to as an *overlapping protected VLAN*, and requires shared port configurations.

In this example, there is one overlapping protected VLAN, purple-1, while all other VLANs are isolated to a single EAPS domain (VLANs green-1, orange-1, and red-1). Protected VLAN configuration, such as 802.1q tagging, must match on the edge switch. The commands in the following example are entered on both aggregate switches.

This procedure can also be repeated for additional protected VLANs as needed:

```
* AGG-SWITCH.44 # create vlan purple-1
* AGG-SWITCH.45 # create vlan green-1
* AGG-SWITCH.46 # create vlan orange-1
* AGG-SWITCH.47 # create vlan red-1
* AGG-SWITCH.48 # configure purple-1 tag 1
* AGG-SWITCH.49 # configure green-1 tag 2
* AGG-SWITCH.50 # configure orange-1 tag 3
* AGG-SWITCH.51 # configure red-1 tag 4
* AGG-SWITCH.52 # configure eaps e1-domain add protect vlan purple-1
* AGG-SWITCH.53 # configure eaps e2-domain add protect vlan purple-1
* AGG-SWITCH.54 # configure eaps e3-domain add protect vlan purple-1
* AGG-SWITCH.55 # configure eaps e4-domain add protect vlan purple-1
* AGG-SWITCH.56 # configure eaps e2-domain add protect vlan green-1
* AGG-SWITCH.57 # configure eaps e3-domain add protect vlan orange-1
* AGG-SWITCH.58 # configure eaps e4-domain add protect vlan red-1
* AGG-SWITCH.59 # configure vlan purple-1 add port 2:1,1:1,1:4,3:1,3:2
tagged
* AGG-SWITCH.60 # configure vlan green-1 add port 2:1,1:4 tagged
* AGG-SWITCH.61 # configure vlan orange-1 add port 2:1,3:1 tagged
* AGG-SWITCH.62 # configure vlan red-1 add port 2:1,3:2 tagged
```

**Verifying the EAPS Configuration and Operating State**

1. When the configuration is complete, confirm that the EAPS domain and shared port configuration is correct.
2. Verify whether the EAPS state is Complete and the shared port status is Ready.

Both ring ports must be plugged in to see the Links-Up state. This verification is performed on both aggregate switches.

EAPS master and partner node status verification example:

```
* AGG-SWITCH#2.63 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: Off
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 4
# EAPS domain configuration:
```

---
### Domain State

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mode</th>
<th>Priority</th>
<th>Secondary</th>
<th>Control</th>
<th>Vlan</th>
<th>VID</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>e1-domain</td>
<td>Complete</td>
<td>M</td>
<td>Y</td>
<td>2:1</td>
<td>1:1</td>
<td>control-1 (4001)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>e2-domain</td>
<td>Complete</td>
<td>M</td>
<td>Y</td>
<td>2:1</td>
<td>1:4</td>
<td>control-2 (4002)</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>e3-domain</td>
<td>Complete</td>
<td>M</td>
<td>Y</td>
<td>2:1</td>
<td>3:1</td>
<td>control-3 (4003)</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>e4-domain</td>
<td>Complete</td>
<td>M</td>
<td>Y</td>
<td>2:1</td>
<td>3:2</td>
<td>control-4 (4004)</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

* AGG-SWITCH#2.64 # show eaps shared-port
EAPS shared-port count: 1

### Link Domain Vlan RB RB

<table>
<thead>
<tr>
<th>Shared-port Mode</th>
<th>Id</th>
<th>Up State</th>
<th>count</th>
<th>Nbr State</th>
<th>Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:1 Partner</td>
<td>21</td>
<td>Y</td>
<td>Ready</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

### EAPS transit and controller node status verification example:

* AGG-SWITCH#1.63 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: Off
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 4
# EAPS domain configuration :

### Designing and Configuring L3 Services on top of EAPS

This section explains how to run L3 routing services on top of EAPS as a foundation.
In this example, OSPF is used as the dynamic IP routing protocol to communicate between different VLANs. To provide redundancy at the router level, VRRP is used to protect against an aggregation switch failure. VRRP allows one aggregation switch to route IP traffic, and if it fails the other aggregation switch takes over the IP routing role. Each EAPS protected VLAN provides L3 connectivity to the clients by configuring IP addressing, OSPF routing, and VRRP on the aggregation switches.

**Figure 143: L2 and L3 Aggregation Network Layer**

IP routing is added to the design on the access network switches by configuring each EAPS protected VLAN as an OSPF interface. Because these are broadcast OSPF interfaces, we need to specify a Designated Router (DR) and Backup Designated Router (BDR). While the EAPS transit and controller node is not blocking any ports, it is configured as the OSPF DR.

The EAPS master and partner node is then configured as the BDR. Similarly, the EAPS transit and controller node is also configured as the VRRP master, which provides L3 routing to the hosts. The EAPS master and partner node is configured as the VRRP backup router for redundancy.
Using redundant aggregation switches with VRRP protects against a single point of failure at the switch level. Client devices receive non-stop IP routing services in the event of link or aggregation switch failure without any reconfiguration. OSPF provides fast convergence from any routing failures. EAPS provides the resilient L2 foundation and minimizes the occurrence of routing interface flaps or dropped OSPF neighbor adjacencies.

To configure L3 on the aggregation switches, complete the tasks described in the following sections:

1. Configure OSPF on the EAPS protected VLANs.
2. Configure OSPF on the EAPS protected VLANs.
3. Configure VRRP on the EAPS protected VLANs.
4. Verify OSPF and VRRP configuration status.

**Configuring IP Addresses on the EAPS Protected VLANs**

Client host stations need the IP address configuration to match their protected VLANs. The edge switches do not require IP addresses, but this could optionally be done for management or troubleshooting purposes.

The following example shows IP address configuration:

* AGG-SWITCH#1.1 # configure vlan green-1 ipaddress 172.16.1.1/24
* AGG-SWITCH#1.2 # configure vlan purple-1 ipaddress 172.16.2.1/24
* AGG-SWITCH#1.3 # configure vlan orange-1 ipaddress 172.16.3.1/24
* AGG-SWITCH#1.4 # configure vlan red-1 ipaddress 172.16.4.1/24
* AGG-SWITCH#2.1 # configure vlan green-1 ipaddress 172.16.1.2/24
* AGG-SWITCH#2.2 # configure vlan purple-1 ipaddress 172.16.2.2/24
* AGG-SWITCH#2.3 # configure vlan orange-1 ipaddress 172.16.3.2/24
* AGG-SWITCH#2.4 # configure vlan red-1 ipaddress 172.16.4.2/24

**Configuring OSPF on the EAPS Protected VLANs**

Because OSPF broadcast networks are being used, configure the DR and BDR for each VLAN. Configure the EAPS transit and controller as the DR by using a higher OSPF priority value since it is not performing L2 blocking. The EAPS master and partner switch is configured as the BDR. In this example, all edge EAPS protected VLANs are placed in the OSPF backbone area, but another OSPF area could be created if desired.

Example OSPF DR configuration:

* AGG-SWITCH#1.5 # enable ipforwarding vlan green-1
* AGG-SWITCH#1.6 # enable ipforwarding vlan purple-1
* AGG-SWITCH#1.7 # enable ipforwarding vlan orange-1
* AGG-SWITCH#1.8 # enable ipforwarding vlan red-1
* AGG-SWITCH#1.9 # configure ospf routerid 172.16.1.1
* AGG-SWITCH#1.10 # configure ospf add vlan green-1 area 0.0.0.0
* AGG-SWITCH#1.11 # configure ospf add vlan purple-1 area 0.0.0.0
* AGG-SWITCH#1.12 # configure ospf add vlan orange-1 area 0.0.0.0
* AGG-SWITCH#1.13 # configure ospf add vlan red-1 area 0.0.0.0
* AGG-SWITCH#1.14 # configure ospf vlan green-1 priority 110
* AGG-SWITCH#1.15 # configure ospf vlan purple-1 priority 110
* AGG-SWITCH#1.16 # configure ospf vlan orange-1 priority 110
Example OSPF BDR configuration:

```
* AGG-SWITCH#2.5 # enable ipforwarding vlan green-1
* AGG-SWITCH#2.6 # enable ipforwarding vlan purple-1
* AGG-SWITCH#2.7 # enable ipforwarding vlan orange-1
* AGG-SWITCH#2.8 # enable ipforwarding vlan red-1
* AGG-SWITCH#2.9 # configure ospf routerid 172.16.1.2
* AGG-SWITCH#2.10 # configure ospf add vlan green-1 area 0.0.0.0
* AGG-SWITCH#2.11 # configure ospf add vlan purple-1 area 0.0.0.0
* AGG-SWITCH#2.12 # configure ospf add vlan orange-1 area 0.0.0.0
* AGG-SWITCH#2.13 # configure ospf add vlan red-1 area 0.0.0.0
* AGG-SWITCH#2.14 # configure ospf vlan green-1 priority 100
* AGG-SWITCH#2.15 # configure ospf vlan purple-1 priority 100
* AGG-SWITCH#2.16 # configure ospf vlan orange-1 priority 100
* AGG-SWITCH#2.17 # configure ospf vlan red-1 priority 100
* AGG-SWITCH#2.18 # enable ospf
```

Configuring VRRP on the EAPS Protected VLANS

The VRRP virtual router is configured with the virtual IP address of 172.16.x.254 for each VLAN (example VLAN green-1 = 172.16.1.254). The VRRP virtual router IP address is configured as the default gateway of each client machine. Since it is not performing L2 blocking, configure the EAPS transit and controller as VRRP master router by using a higher priority value. The EAPS master and partner switch is configured as the VRRP backup router.

Example VRRP master router configuration:

```
* AGG-SWITCH#1.19 # create vrrp vlan green-1 vrid 1
* AGG-SWITCH#1.20 # configure vrrp vlan green-1 vrid 1 priority 110
* AGG-SWITCH#1.21 # configure vrrp vlan green-1 vrid 1 add 172.16.1.254
* AGG-SWITCH#1.22 # enable vrrp vlan green-1 vrid 1
* AGG-SWITCH#1.23 # create vrrp vlan purple-1 vrid 1
* AGG-SWITCH#1.24 # configure vrrp vlan purple-1 vrid 1 priority 110
* AGG-SWITCH#1.25 # configure vrrp vlan purple-1 vrid 1 add 172.16.2.254
* AGG-SWITCH#1.26 # enable vrrp vlan purple-1 vrid 1
* AGG-SWITCH#1.27 # create vrrp vlan orange-1 vrid 1
* AGG-SWITCH#1.28 # configure vrrp vlan orange-1 vrid 1 priority 110
* AGG-SWITCH#1.29 # configure vrrp vlan orange-1 vrid 1 add 172.16.3.254
* AGG-SWITCH#1.30 # enable vrrp vlan orange-1 vrid 1
* AGG-SWITCH#1.31 # create vrrp vlan red-1 vrid 1
* AGG-SWITCH#1.32 # configure vrrp vlan red-1 vrid 1 priority 110
* AGG-SWITCH#1.33 # configure vrrp vlan red-1 vrid 1 add 172.16.4.254
* AGG-SWITCH#1.34 # enable vrrp vlan red-1 vrid 1
```

Example VRRP backup router configuration:

```
* AGG-SWITCH#2.19 # create vrrp vlan green-1 vrid 1
* AGG-SWITCH#2.20 # configure vrrp vlan green-1 vrid 1 priority 100
* AGG-SWITCH#2.21 # configure vrrp vlan green-1 vrid 1 add 172.16.1.254
* AGG-SWITCH#2.22 # enable vrrp vlan green-1 vrid 1
* AGG-SWITCH#2.23 # create vrrp vlan purple-1 vrid 1
```
Verifying OSPF and VRRP Configuration Status

1. Verify the OSPF neighbor adjacencies are established and that the DR and BDR status is correct.
2. Verify that the VRRP virtual router is running and the VRRP master/backup status is correct.

OSPF and VRRP verification example:

* AGG-SWITCH#1.35 # show ospf neighbor

Neighbor ID Pri State Up/Dead Time Address Interface
172.16.1.2 100 FULL /BDR 00:18:01:08/00:00:00:03 172.16.3.2 orange-1
172.16.1.2 100 FULL /BDR 00:18:01:08/00:00:00:03 172.16.4.2 red-1
172.16.1.2 100 FULL /BDR 00:17:54:17/00:00:00:03 172.16.1.2 green-1
172.16.1.2 100 FULL /BDR 00:17:54:07/00:00:00:03 172.16.2.2 purple-1

* AGG-SWITCH#1.36 # show vrrp

VLAN Name VRID Pri Virtual IP Addr State Master Mac Address TP/TR/TV/P/T
green-1(En) 0001 110 172.16.1.254 MSTR 00:00:5e:00:01:01 0 0 0 Y 1
purple-(En) 0001 110 172.16.2.254 MSTR 00:00:5e:00:01:01 0 0 0 Y 1
orange-(En) 0001 110 172.16.3.254 MSTR 00:00:5e:00:01:01 0 0 0 Y 1
red-1(En) 0001 110 172.16.4.254 MSTR 00:00:5e:00:01:01 0 0 0 Y 1
En-Enabled, Ds-Disabled, Pri-Priority, T-Advert Timer, P-Preempt
TP-Tracked Pings, TR-Tracked Routes, TV-Tracked VLANs

* AGG-SWITCH#2.35 # show ospf neighbor

Neighbor ID Pri State Up/Dead Time Address Interface
172.16.1.1 110 FULL /DR 00:18:01:08/00:00:00:03 172.16.3.1 orange-1
172.16.1.1 110 FULL /DR 00:18:01:08/00:00:00:03 172.16.4.1 red-1
172.16.1.1 110 FULL /DR 00:17:54:17/00:00:00:03 172.16.1.1 green-1
172.16.1.1 110 FULL /DR 00:17:54:07/00:00:00:03 172.16.2.1 purple-1

* AGG-SWITCH#2.36 # show vrrp

VLAN Name VRID Pri Virtual IP Addr State Master Mac Address TP/TR/TV/P/T
green-1(En) 0001 100 172.16.1.254 BKUP 00:00:5e:00:01:01 0 0 0 Y 1
purple-(En) 0001 100 172.16.2.254 BKUP 00:00:5e:00:01:01 0 0 0 Y 1
orange-(En) 0001 100 172.16.3.254 BKUP 00:00:5e:00:01:01 0 0 0 Y 1
red-1(En) 0001 100 172.16.4.254 BKUP 00:00:5e:00:01:01 0 0 0 Y 1
En-Enabled, Ds-Disabled, Pri-Priority, T-Advert Timer, P-Preempt
TP-Tracked Pings, TR-Tracked Routes, TV-Tracked VLANs

Designing and Configuring the Core Layer with EAPS

The core switches provide high performance backbone routing between the edge, aggregation, data center, and external Internet networks.

An additional high availability backbone ring is built that combines EAPS and OSPF. Using EAPS and OSPF together increases the stability of IP routing tables. Since EAPS provides 50-millisecond convergence for link failures, OSPF adjacencies do not flap. In this example, the backbone ring is
formed by adding two core L2/L3 switches and connecting them to the two existing aggregation switches. The core switches also provide routing to the Internet using BGP (see the following figure).

Figure 144: Core EAPS and OSPF Network Layer

Using redundant core switches protects against a single point of failure at the switch level. OSPF provides fast convergence from any routing failures. EAPS provides the resilient L2 foundation and minimizes the occurrence of routing interface flaps or dropped OSPF neighbor adjacencies. Combining EAPS and OSPF provides the highest level of network resiliency and routing stability.

Configuring the core switches requires a new EAPS domain with a single EAPS protected VLAN with OSPF forming the backbone IP network. Additional configuration is needed on the aggregation switches to connect them to the backbone EAPS and OSPF ring. Since the steps are similar to previous configuration examples, the L2 (EAPS) and L3 (OSPF) configurations are combined. Since the BGP configuration is independent of EAPS configuration, BGP configuration is not discussed here.

To configure backbone connectivity on the core and aggregation switches, complete the tasks described in the following sections:

1. Create and configure the backbone EAPS domain.
2. Create and configure the backbone EAPS protected VLANs.
3  Configure an IP address and OSPF on the backbone VLAN.
4  Verify EAPS and OSPF configuration status.

Creating and Configuring the Backbone EAPS Domain

1  Create the backbone EAPS domains and configure the EAPS mode.
2  Define the primary and secondary ports for each domain.
   Configure on both core and aggregation switches.

Core-Switch 1 EAPS configuration:
* CORE-SWITCH#1.1 # create eaps e5-domain
* CORE-SWITCH#1.2 # configure eaps e5-domain mode transit
* CORE-SWITCH#1.3 # configure eaps e5-domain primary port 2:1
* CORE-SWITCH#1.4 # configure eaps e5-domain secondary port 2:4

Core-Switch 2 EAPS configuration:
* CORE-SWITCH#2.1 # create eaps e5-domain
* CORE-SWITCH#2.2 # configure eaps e5-domain mode master
* CORE-SWITCH#2.3 # configure eaps e5-domain primary port 2:1
* CORE-SWITCH#2.4 # configure eaps e5-domain secondary port 2:4

Agg-Switch 1 EAPS configuration:
* AGG-SWITCH#1.1 # create eaps e5-domain
* AGG-SWITCH#1.2 # configure eaps e5-domain mode transit
* AGG-SWITCH#1.3 # configure eaps e5-domain primary port 2:1
* AGG-SWITCH#1.4 # configure eaps e5-domain secondary port 2:4

Agg-Switch 2 EAPS configuration:
* AGG-SWITCH#2.1 # create eaps e5-domain
* AGG-SWITCH#2.2 # configure eaps e5-domain mode transit
* AGG-SWITCH#2.3 # configure eaps e5-domain primary port 2:1
* AGG-SWITCH#2.4 # configure eaps e5-domain secondary port 2:4

Creating and Configuring the Backbone EAPS Control VLAN

1  Create the EAPS control VLAN and configure its 802.1q tag, and ring ports.
2  Configure the control VLANs as part of the backbone EAPS domain. Enable EAPS and the backbone
   EAPS domain. Configure on both core and aggregation switches (EAPS is already enabled on
   aggregation switches).

Core-Switch#1 control VLAN configuration:
* CORE-SWITCH#1.1 # create vlan control-5
* CORE-SWITCH#1.2 # configure vlan control-5 tag 4005
* CORE-SWITCH#1.4 # configure vlan control-5 add port 2:1,2:4 tagged
* CORE-SWITCH#1.5 # configure eaps e5-domain add control vlan control-5
* CORE-SWITCH#1.6 # enable eaps
* CORE-SWITCH#1.7 # enable eaps e5-domain

Core-Switch#2 control VLAN configuration:
* CORE-SWITCH#2.1 # create vlan control-5
* CORE-SWITCH#2.2 # configure vlan control-5 tag 4005
Creating and Configuring the Backbone EAPS Protected VLANs

1. Create the EAPS protected VLAN for the backbone domain.
2. Configure the 802.1q tag and ports for the protected VLANs.
   Because this VLAN is only used for transit routing, there are no other ports besides the ring ports.
3. Configure the protected VLAN as part of the EAPS domain. Do this configuration on both the core and aggregate switches.

Core-Switch#1 protected VLAN configuration:

- CORE-SWITCH#1.8 # create vlan backbone
- CORE-SWITCH#1.9 # configure vlan backbone tag 3000
- CORE-SWITCH#1.10 # configure vlan backbone add port 2:1,2:4 tagged
- CORE-SWITCH#1.11 # configure eaps e5-domain add protect vlan backbone

Core-Switch#2 protected VLAN configuration:

- CORE-SWITCH#2.8 # create vlan backbone
- CORE-SWITCH#2.9 # configure vlan backbone tag 3000
- CORE-SWITCH#2.10 # configure vlan backbone add port 2:1,2:4 tagged
- CORE-SWITCH#2.11 # configure eaps e5-domain add protect vlan backbone

Agg-Switch#1 protected VLAN configuration:

- AGG-SWITCH#1.7 # create vlan backbone
- AGG-SWITCH#1.8 # configure vlan backbone tag 3000
- AGG-SWITCH#1.9 # configure vlan backbone add port 2:4,2:6 tagged
- AGG-SWITCH#1.10 # configure eaps e5-domain add protect vlan backbone
Agg-Switch#2 protected VLAN configuration:

* AGG-SWITCH#2.7 # create vlan backbone
* AGG-SWITCH#2.8 # configure vlan backbone tag 3000
* AGG-SWITCH#2.9 # configure vlan backbone add port 2:4,2:6 tagged
* AGG-SWITCH#2.10 # configure eaps e5-domain add protect vlan backbone

Configuring an IP Address and OSPF on the Backbone VLAN

1. Configure an IP address and enable IP forwarding (routing) on the backbone protected VLAN.
2. OSPF is configured and because an OSPF broadcast network is used, configure the designated router and backup designated router for each VLAN.

Since it is not performing L2 blocking, configure the EAPS transit core switch as the DR by using a higher OSPF priority value. The EAPS master core switch is configured as the BDR. The aggregation transit switches need not perform DR/BDR duties for the backbone VLAN, so their OSPF priority is configured at 0 to force ODR behavior.

Core-Switch#1 OSPF configuration:

* CORE-SWITCH#1.12 # configure vlan backbone ipaddress 192.168.1.1/24
* CORE-SWITCH#1.13 # enable ipforwarding vlan backbone
* CORE-SWITCH#1.14 # configure ospf routerid 192.168.1.1
* CORE-SWITCH#1.15 # configure ospf add vlan backbone area 0.0.0.0
* CORE-SWITCH#1.16 # configure ospf vlan backbone priority 110
* CORE-SWITCH#1.17 # enable ospf

Core-Switch#2 OSPF configuration:

* CORE-SWITCH#2.12 # configure vlan backbone ipaddress 192.168.1.2/24
* CORE-SWITCH#2.13 # enable ipforwarding vlan backbone
* CORE-SWITCH#2.14 # configure ospf routerid 192.168.1.2
* CORE-SWITCH#2.15 # configure ospf add vlan backbone area 0.0.0.0
* CORE-SWITCH#2.16 # configure ospf vlan backbone priority 100
* CORE-SWITCH#2.17 # enable ospf

Agg-Switch#1 OSPF configuration:

* AGG-SWITCH#1.11 # configure vlan backbone ipaddress 192.168.1.3/24
* AGG-SWITCH#1.12 # enable ipforwarding vlan backbone
* AGG-SWITCH#1.13 # configure ospf add vlan backbone area 0.0.0.0
* AGG-SWITCH#1.14 # configure ospf vlan backbone priority 0

Agg-Switch#2 OSPF configuration:

* AGG-SWITCH#2.11 # configure vlan backbone ipaddress 192.168.1.4/24
* AGG-SWITCH#2.12 # enable ipforwarding vlan backbone
* AGG-SWITCH#2.13 # configure ospf add vlan backbone area 0.0.0.0
* AGG-SWITCH#2.14 # configure ospf vlan backbone priority 0

Verifying EAPS and OSPF Configuration Status

1. Verify that the backbone EAPS domain and OSPF configuration is correct.
2 Confirm that the OSPF neighbor adjacencies and DR/BDR/ODR status are correct. Verify this status on both aggregate switches.

Core-Switch#1 EAPS and OSPF status example:

* CORE-SWITCH#1.18 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1
# EAPS domain configuration :

Domain State Mo En Pri Sec Control-Vlan VID Count
----------------------------------------------------------------------------
e5-domain Links-Up T Y 2:1 2:4 control-5 (4005) 1
----------------------------------------------------------------------------

Core-Switch#2 EAPS and OSPF status example:

* CORE-SWITCH#2.18 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1
# EAPS domain configuration :

----
Domain State Mo En Pri Sec Control-Vlan VID Count
----
e5-domain Complete T Y 2:1 2:4 control-5 (4005) 1
----

Agg-Switch#1 EAPS and OSPF status example:

* AGG-SWITCH#1.15 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 5

# EAPS domain configuration:

---

Domain State Mo En Pri Sec Control-Vlan VID Count
---

e1-domain Links-Up T Y 1:1 2:1 control-1 (4001) 2
e2-domain Links-Up T Y 1:4 2:1 control-2 (4002) 2
e3-domain Links-Up T Y 3:1 2:1 control-3 (4003) 2
e4-domain Links-Up T Y 3:2 2:1 control-4 (4004) 2
e5-domain Links-Up T Y 2:4 2:6 control-5 (4005) 1
---

* AGG-SWITCH#1.16 # show ospf neighbor
Neighbor ID Pri State Up/Dead Time Address Interface
192.168.1.1 110 FULL /DR 00:00:28:51/00:00:00:01 192.168.1.1 backbone
192.168.1.2 100 FULL /BDR 00:00:28:51/00:00:00:01 192.168.1.2 backbone
192.168.1.4 0 2WAY /DROTER00:05:45:40/00:00:00:03 192.168.1.4 backbone
172.16.1.2 18 FULL /BDR 00:18:01:08/00:00:00:00 172.16.3.2 orange-1
172.16.1.2 100 FULL /BDR 00:18:01:08/00:00:00:03 172.16.4.2 red-1
172.16.1.2 100 FULL /BDR 00:17:54:17/00:00:00:03 172.16.1.2 green-1
172.16.1.2 100 FULL /BDR 00:17:54:07/00:00:00:03 172.16.2.2 purple-1

Agg-Switch#2 EAPS and OSPF status example:

* AGG-SWITCH#2.15 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 5

# EAPS domain configuration:

---

Domain State Mo En Pri Sec Control-Vlan VID Count
---

e1-domain Complete M Y 2:1 1:1 control-1 (4001) 2
e2-domain Complete M Y 2:1 1:4 control-2 (4002) 2
e3-domain Complete M Y 2:1 3:1 control-3 (4003) 2
e4-domain Complete M Y 2:1 3:2 control-4 (4004) 2
e5-domain Links-Up T Y 2:4 2:6 control-5 (4005) 1
---

* AGG-SWITCH#2.16 # show ospf neighbor
Interface
192.168.1.1 110 FULL /DR 00:00:28:51/00:00:00:01 192.168.1.1 backbone
192.168.1.2 100 FULL /BDR 00:00:28:51/00:00:00:01 192.168.1.2 backbone
192.168.1.3 0 2WAY /DROTER00:05:45:40/00:00:00:03 192.168.1.3 backbone
172.16.1.1 110 FULL /DR 00:18:01:08/00:00:00:03 172.16.3.1 orange-1
172.16.1.1 110 FULL /DR 00:18:01:08/00:00:00:03 172.16.4.1 red-1
172.16.1.1 110 FULL /DR 00:17:54:17/00:00:00:03 172.16.1.1 green-1
172.16.1.1 110 FULL /DR 00:17:54:07/00:00:00:03 172.16.2.1 purple-1
Designing and Configuring the Data Center Switches with EAPS

Building from the network core, you can expand the network with additional EAPS rings to provide resiliency to mission-critical server farms.

The core switches provide high performance backbone routing between the data center and the rest of the network, which includes both internal and external (Internet) destinations. The core switch acts as the EAPS master node for each ring, while the data center switches act as EAPS transit nodes to complete the ring. The core switch also acts as the OSPF routing node to provide gateway routing functionality to the server-farms. For an additional level of resiliency, each server is dual-homed (dual attached) to both EAPS transit L2 switches. Even if a switch or link fails, the servers are available.

The network design and configuration is similar to the edge and aggregation EAPS and OSPF layers. The modular approach is simple and scalable, and allows additional data center rings to be added to provide room for growth. In our example, server-farms are isolated into separate categories such as external and internal service groups, which yield additional security and resiliency benefits.

To configure the data center switches, you need a new EAPS domain with a single EAPS protected VLAN to form the server-farm network. In this example, two data center switches are configured as EAPS transit nodes (L2 switch only) and attach to the existing core switch acting as the EAPS master. Each server in the server-farm is dual-homed to both EAPS transit switches in the data center for additional physical resiliency. IP routing functionality is performed by the core switch via OSPF, which provides L3 connectivity to the rest of the network.

![Figure 145: Data Center EAPS and OSPF Network Layer](image)

To configure data center connectivity, complete the tasks described in the following sections:
1 Create and configure the data center EAPS domain.
2 Create and configure the data center EAPS Control VLAN.
3 Create and configure the data center EAPS protected VLANs.
4 Configure an IP address and OSPF on the backbone VLAN.
5 Verify EAPS and OSPF configuration status.

Creating and Configuring the Data Center EAPS Domain

Create the backbone EAPS domains, configure the EAPS mode, and define the primary and secondary ports for each domain. Do this configuration on both core and aggregation switches.

Core-Switch#1 EAPS configuration:

* CORE-SWITCH#1.1 # create eaps e6-domain
* CORE-SWITCH#1.2 # configure eaps e6-domain mode master
* CORE-SWITCH#1.3 # configure eaps e6-domain primary port 4:1
* CORE-SWITCH#1.4 # configure eaps e6-domain secondary port 4:2

Data center-Switch#1 EAPS configuration:

* DC-SWITCH#1.1 # create eaps e6-domain
* DC-SWITCH#1.2 # configure eaps e6-domain mode transit
* DC-SWITCH#1.3 # configure eaps e6-domain primary port 49
* DC-SWITCH#1.4 # configure eaps e6-domain secondary port 50

Datacenter -Switch#2 EAPS configuration:

* DC-SWITCH#2.1 # create eaps e6-domain
* DC-SWITCH#2.2 # configure eaps e6-domain mode transit
* DC-SWITCH#2.3 # configure eaps e6-domain primary port 49
* DC-SWITCH#2.4 # configure eaps e6-domain secondary port 50

Creating and Configuring the Data Center EAPS Control VLAN

1 Create the EAPS control VLAN and configure its 802.1q tag, and ring ports.
2 Configure the control VLANs as part of the data center EAPS domain. Enable EAPS and the data center EAPS domain. You need to do this configuration on the core and data center L2 switches.

Core-Switch#1 control VLAN configuration:

* CORE-SWITCH#1.1 # create vlan control-6
* CORE-SWITCH#1.2 # configure vlan control-6 tag 4006
* CORE-SWITCH#1.4 # configure vlan control-6 add port 4:1,4:2 tagged
* CORE-SWITCH#1.5 # configure eaps e5-domain add control vlan control-6
* CORE-SWITCH#1.6 # enable eaps e6-domain

Data center-Switch#1 control VLAN configuration:

* DC-SWITCH#1.1 # create vlan control-6
* DC-SWITCH#1.2 # configure vlan control-6 tag 4006
* DC-SWITCH#1.4 # configure vlan control-6 add port 49,50 tagged
* DC-SWITCH#1.5 # configure eaps e6-domain add control vlan control-6
Create and Configure the Data Center EAPS Protected VLANs

1. Create the EAPS protected VLAN for the data center domain.
2. Configure the 802.1q tag and ports for the protected VLANs.
   Because each server is dual-homed to each data center switch, add a VLAN port on each switch for each server.
3. Configure the protected VLAN as part of the EAPS domain. Do this configuration on the core and data center switches.

Core-Switch#1 protected VLAN configuration:

* CORE-SWITCH#1.7 # create vlan srvfarm-1
* CORE-SWITCH#1.8 # configure vlan srvfarm-1 tag 1000
* CORE-SWITCH#1.9 # configure vlan srvfarm-1 add port 4:1,4:2 tagged
* CORE-SWITCH#1.10 # configure eaps e6-domain add protect vlan srvfarm-1

Data center-Switch#1 protected VLAN configuration:

* DC-SWITCH#1.8 # create vlan srvfarm-1
* DC-SWITCH#1.9 # configure vlan srvfarm-1 tag 1000
* DC-SWITCH#1.10 # configure vlan srvfarm-1 add port 49,50 tagged
* DC-SWITCH#1.11 # configure vlan srvfarm-1 add port 1 untagged
* DC-SWITCH#1.12 # configure eaps e6-domain add protect vlan srvfarm-1

Data center-Switch#2 protected VLAN configuration:

* DC-SWITCH#2.8 # create vlan srvfarm-1
* DC-SWITCH#2.9 # configure vlan srvfarm-1 tag 1000
* DC-SWITCH#2.10 # configure vlan srvfarm-1 add port 49,50 tagged
* DC-SWITCH#2.11 # configure vlan srvfarm-1 add port 1 untagged
* DC-SWITCH#2.12 # configure eaps e6-domain add protect vlan srvfarm-1

Configuring an IP Address and OSPF on the Backbone VLAN

Configure an IP address and enable IP forwarding (routing) on the data center protected VLAN. This step is only performed on the core switch. Servers are configured accordingly with the core switch IP address as their default gateway. Since there are no additional routers on this VLAN, configure it as an OSPF passive interface. In this example, the data center VLAN is placed on the backbone OSPF area, but additional OSPF areas can be configured if needed.
Core-Switch#1 OSPF configuration:

* CORE-SWITCH#1.11 # configure vlan srvfarm-1 ipaddress 10.10.10.10/24
* CORE-SWITCH#1.12 # enable ipforwarding vlan srvfarm-1
* CORE-SWITCH#1.13 # configure ospf add vlan srvfarm-1 area 0.0.0.0 passive

Verifying EAPS and OSPF Configuration Status

1 Verify that the data center EAPS domain and OSPF configuration is correct.
2 Verify whether the data center subnet is advertised to other routers through OSPF.

Core-Switch#2 route verification example:

* CORE-SWITCH#2.1 # show iproute 10.10.10.0/24

<table>
<thead>
<tr>
<th>Ori</th>
<th>Destination</th>
<th>Gateway</th>
<th>Mtr</th>
<th>Flags</th>
<th>VLAN</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>#oa</td>
<td>10.10.10.0/24</td>
<td>192.168.1.1</td>
<td>6</td>
<td>UG-D---um--f backbone</td>
<td>0d:0h:25m:5s</td>
<td></td>
</tr>
</tbody>
</table>

Origin(Ori): (b) BlackHole, (be) EBGP, (bg) BGP, (bi) IBGP, (bo) BOOTP (ct) CBT, (d) Direct, (df) DownIF, (dv) DVMRP, (e1) ISISL1Ext (e2) ISISL2Ext, (h) Hardcoded, (i) ICMP, (i1) ISISL1 (i2) ISISL2 (is) ISIS, (mb) MBGP, (mbe) MBGPExt, (mbi) MBGPInter, (mp) MPLS Lsp (mo) MOSPF (o) OSPF, (o1) OSPFExt1, (o2) OSPFExt2 (oa) OSPFINtra, (oe) OSPFAsExt, (or) OSPFInter, (pd) PIM-DM, (ps) PIM-SM (r) RIP, (ra) RAdvrt, (s) Static, (sv) SLB_VIP, (un) UnKnown (*: Preferred unicast route #: Preferred multicast route)

Flags: (B) BlackHole, (D) Dynamic, (G) Gateway, (H) Host Route (L) Matching LDP LSP, (l) Calculated LDP LSP, (m) Multicast (P) LPM-routing, (R) Modified, (S) Static, (s) Static LSP (T) Matching RSVP-TE LSP, (t) Calculated RSVP-TE LSP, (u) Unicast, (U) Up (f) Provided to FIB (c) Compressed Route

Mask distribution:
1 routes at length 16
1 routes at length 24
Route Origin distribution:
1 routes from OSPFINtra 1 routes from OSPFExt1
Total number of routes = 2
Total number of compressed routes = 0

Core-Switch#1 EAPS status:

* CORE-SWITCH#1.14 # show eaps

EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 2
# EAPS domain configuration:

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mo</th>
<th>En</th>
<th>Pri</th>
<th>Sec</th>
<th>Control-Vlan VID</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>e5-domain</td>
<td>Links-Up</td>
<td>T</td>
<td>Y</td>
<td>2:1</td>
<td>2:4</td>
<td>control-5 (4005)</td>
<td>1</td>
</tr>
</tbody>
</table>
Data center-Switch#1 EAPS status:

* DC-SWITCH#1.15 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1

# EAPS domain configuration:

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mo</th>
<th>En</th>
<th>Pri</th>
<th>Sec</th>
<th>Control-Vlan</th>
<th>VID</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>e6-domain</td>
<td>Links-Up</td>
<td>T</td>
<td>Y</td>
<td>49</td>
<td>50</td>
<td>control-6</td>
<td>(4006)</td>
<td>1</td>
</tr>
</tbody>
</table>

Data center-Switch#2 EAPS status:

* DC-SWITCH#2.15 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
EAPS Display Config Warnings: On
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1

# EAPS domain configuration:

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mo</th>
<th>En</th>
<th>Pri</th>
<th>Sec</th>
<th>Control-Vlan</th>
<th>VID</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>e6-domain</td>
<td>Links-Up</td>
<td>M</td>
<td>Y</td>
<td>49</td>
<td>50</td>
<td>control-6</td>
<td>(4006)</td>
<td>1</td>
</tr>
</tbody>
</table>

Example EAPS and PBB Configuration

This section provides an example of how to configure a controller node to support EAPS and PBB. The example can be modified to configure a partner node.

Note
Actual implementation steps on a production network may differ based on the physical topology, switch models, and software versions deployed.

The following figure shows a sample EAPS topology that supports PBB.
Figure 146: Sample EAPS Topology with PBB

In the figure above, the CVLANs data1, data2, and data3 are mapped to BVLANs metro1 and metro2. This example details the configuration of switch BD20K-1, which is the controller node for common link 10. To configure EAPS and PBB for switch BD20K-1, EAPS rings d1, d2, and d3 must be configured.

After configuration is complete, switch BD20K-1 recognizes that port 3:38 serves a BVLAN. If common link 10 fails, port 3:38 becomes the active-open port, and ports 3:35 and 3:36 enter the blocking state. If the link connected to port 3:38 fails, port 3:35 becomes the active-open port because it has the lowest port number. If port 3:38 recovers, it again becomes the active-open port.

The following sections list the commands required to configure EAPS and PBB for switch BD20K-1 as shown in the following figure:

1. Create and configure the EAPS control VLANs.
2. Configure the shared port.
3. Enable EAPS.

Configuring the CVLANs and BVLANs

The following commands create the CVLANs and BVLANs:

```
# Create CVLANs
create cvlan data1
configure cvlan data1 tag 1001
configure cvlan data1 add port 3:35-36 tagged
create cvlan data2
configure cvlan data2 tag 1002
configure cvlan data2 add port 3:35-36 tagged
create cvlan data3
```
configure cvlan data3 tag 1003
configure cvlan data3 add port 3:35-36 tagged

# Create BVLANs
create bvlan metro1
configure bvlan metro1 tag 2001
configure bvlan metro1 add port 3:38, 1:24 tagged
create bvlan metro2
configure bvlan metro2 tag 2002
configure bvlan metro2 add port 3:38, 1:24 tagged

# Create ISIDs
create isid is1 1000
configure isid is1 add cvlan data1
create isid is2 2000
configure isid is2 add cvlan data2
create isid is3 3000
configure isid is3 add cvlan data3

# Bind ISIDs to BVLANs
configure bvlan metro1 add isid is1
configure bvlan metro1 add isid is2
configure bvlan metro2 add isid is3

Creating and Configuring the EAPS Domains

• The following commands configure the EAPS domains:

  create eaps d1
  configure eaps d1 mode transit
  configure eaps d1 primary port 1:24
  configure eaps d1 secondary port 3:38
  configure eaps d1 add control vlan vc1
  configure eaps d1 add protected metro1
  configure eaps d1 add protected metro2
  create eaps d2
  configure eaps d2 mode transit
  configure eaps d2 primary port 1:24
  configure eaps d2 secondary port 3:36
  configure eaps d2 add control vlan vc2
  configure eaps d2 add protected data1
  configure eaps d2 add protected data2
  configure eaps d2 add protected data3
  create eaps d3
  configure eaps d3 mode transit
  configure eaps d3 primary port 1:24
  configure eaps d3 secondary port 3:35
  configure eaps d3 add control vlan vc3
  configure eaps d3 add protected data1
  configure eaps d3 add protected data2
  configure eaps d3 add protected data3

EAPS
ExtremeXOS Concepts Guide for Release 15.4
Creating and Configuring the EAPS Control VLANs

- The following commands configure the control VLANs:
  
  ```
  create vlan vc1
  configure vc1 tag 101
  configure vc1 add port 3:38,1:24 tagged
  create vlan vc2
  configure vc2 tag 102
  configure vc2 add port 3:36,1:24 tagged
  create vlan vc3
  configure vc3 tag 103
  configure vc3 add port 3:35,1:24 tagged
  ```

Configuring the Shared Port

- The following commands configure the shared port:
  
  ```
  create eaps shared-port 1:24
  configure eaps shared-port 1:24 link-id 10
  configure eaps shared-port 1:24 mode controller
  ```

Enabling EAPS

The following commands enable EAPS on the switch and on the EAPS rings:

```
enable eaps
enable eaps d1
enable eaps d2
enable eaps d3
```

Displaying the EAPS Status

- The following display commands show the example configuration and status after common link 10 fails:
  
  ```bash
  Switch.2 # sh eaps shared-port 1:24
  ------------------------------------------
  Link           Domain  Vlan   RB       RB
  Shared-port    Mode    Id   Up State  count  count Nbr State  Id
  ------------------------------------------
  1:24           Controller 10 Y  Blocking 3       5     Yes None
  None
  Segment Health Check interval: 1 sec
  Segment Timeout: 3 sec
  Segment Fail Timer expiry action: Send alert
  Common Path Health Check interval: 1 sec
  Common Path Timeout: 3 sec
  Segment Port: 3:35 Status: Up
  EAPS Domain: d3
  Vlan-port count: 3
  Adjacent Blocking Id: None
  Segment RB Id: None
  Segment Port: 3:36 Status: Up
  EAPS Domain: d2
  ```
Vlan-port count: 3
Adjacent Blocking Id: None
Segment RB Id: None
Segment Port: 3:38 Status: Up
EAPS Domain: d1
Vlan-port count: 5
Adjacent Blocking Id: None
Segment RB Id: None
Vlan: data1, Vlan-port count: 3, Active Open: 3:38 Bvlan: metro1
Vlan: data2, Vlan-port count: 3, Active Open: 3:38 Bvlan: metro1
Vlan: data3, Vlan-port count: 3, Active Open: 3:38 Bvlan: metro2
Vlan: metro1, Vlan-port count: 1, Active Open: 3:38
Vlan: metro2, Vlan-port count: 1, Active Open: 3:38

Switch.3 # sh eaps shared-port 1:24 detail

<table>
<thead>
<tr>
<th>Link</th>
<th>Domain</th>
<th>Vlan</th>
<th>RB</th>
<th>RB</th>
<th>RB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared-port</td>
<td>Mode</td>
<td>Id</td>
<td>Up State</td>
<td>count</td>
<td>count</td>
</tr>
<tr>
<td>1:24</td>
<td>Controller 10</td>
<td>Y</td>
<td>Blocking</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

Vlan: data1, Vlan-port count: 3, Active Open: 3:38
Segment Port Bvlan
3:38 metro1 Active-Open
3:35 Blocked
3:36 Blocked
Vlan: data2, Vlan-port count: 3, Active Open: 3:38
Segment Port Bvlan
3:38 metro1 Active-Open
3:35 Blocked
3:36 Blocked
Vlan: data3, Vlan-port count: 3, Active Open: 3:38
Segment Port Bvlan
3:38 metro2 Active-Open
3:35 Blocked
3:36 Blocked
Vlan: metro1, Vlan-port count: 1, Active Open: 3:38
Segment Port Bvlan
3:38 Active-Open
Vlan: metro2, Vlan-port count: 1, Active Open: 3:38
Segment Port Bvlan
3:38 Active-Open

Switch.4 # sh eaps shared-port detail
EAPS shared-port count: 1

<table>
<thead>
<tr>
<th>Link</th>
<th>Domain</th>
<th>Vlan</th>
<th>RB</th>
<th>RB</th>
<th>RB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared-port</td>
<td>Mode</td>
<td>Id</td>
<td>Up State</td>
<td>count</td>
<td>count</td>
</tr>
<tr>
<td>1:24</td>
<td>Controller 10</td>
<td>Y</td>
<td>Blocking</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

Vlan: data1, Vlan-port count: 3, Active Open: 3:38
Segment Port Bvlan
3:38 Active-Open
CFM Support in EAPS

ExtremeXOS provides Connectivity Fault Management (CFM) support within EAPS protocol.

CFM reports fault connectivity failures to EAPS, and EAPS communicates with the CFM process to set up point-to-point DOWN MEPs (Management Endpoints) to monitor link connectivity. The CFM module notifies EAPS of any link-connectivity issues, and triggers EAPS to take necessary action.

802.1ag CFM supports link monitoring. It does this by sending out PDUs at designated transmit intervals. If the CFM fails to receive PDUs, it assumes the link is out of service, and notifies its clients. In this instance, EAPS acts as a CFM client.

First, you will create a down MEP within the CFM CLI. Configure the CLI to create a MEP group that associates this down MEP with a remote MEP (RMEP). There is a 1:1 relationship between a port and the down MEP, and as such, each MEP group is tied to a single port. Using the EAPS CLI, you can add the MEP groups you wish to monitor. For each MEP group added to EAPS, EAPS will receive UP/DOWN notifications from CFM when CFM detects a MEP state change for that group. Each MEP group corresponds to an EAPS ring port. Notifications from those MEP groups that are inadvertently added, that do not correspond to an EAPS ring port, are ignored in EAPS.

The CFM configuration is independent of EAPS, and MEPs and MEP groups may use different VLANs other than the EAPS control VLAN to monitor links.

When EAPS receives a CFM notification that the link failed, EAPS blocks that port on all of the EAPS control VLANs. This prevents EAPS control PDUs from being hardware forwarded on the link, in case the link is still up. Any EAPS PDUs that are received on a CFM failed port are dropped in EAPS.

Configuring EAPS for CFM Support

- Use the following command to configure EAPS for CFM support:

```
For additional configuration details for CFM support, refer to Configuring CFM on page 396.
```
Binding to a MEP Group

- To bind to a MEP Group, use the following command:

  ```
  configure eaps cfm [add | delete] group group_name
  ```

  This command notifies CFM that EAPs is interested in notifications for this MEP and RMEP pair. This MEP should already be bound to a physical port, so when notification is received, EAPS associates that notification with a ring-port failure.

Create MPs and the CCM Transmission Interval

Within an MA, you configure the following MPs:

- Maintenance end points (MEPs), which are one of the following types:
  - UP MEPs—transmit CCMs and maintain CCM database
  - DOWN MEPs—transmit CCMs and maintain CCM database
  - Maintenance intermediate points (MIPs)—pass CCMs through

Each MEP must have an ID that is unique for that MEP throughout the MA.

- To configure UP and DOWN MEPs and its unique MEP ID, use the following command:

  ```
  configure cfm domain domain_name association association_name [ports <port_list add [end-point [up|down] mepid {group group_name}] | [intermediate-point]]
  ```

- To change the MEP ID on an existing MEP, use the following command:

  ```
  configure cfm domain domain-name association association_name ports port_list end-point [up | down] mepid mepid
  ```

- To delete UP and DOWN MEPs, use the following command:

  ```
  configure cfm domain domain-name association association_name ports port_list end-point [up | down] intermediate-point
  ```

- To configure a MIP, use the following command:

  ```
  configure cfm domain domain_name association association_name [ports <port_list add [end-point [up|down] mepid {group group_name}] | [intermediate-point]]
  ```

- To delete a MIP, use the following command:

  ```
  configure cfm domain domain_name association association_name [ports <port_list delete [end-point [up|down] mepid {group group_name}] | [intermediate-point]]
  ```

- To configure the transmission interval for the MEP to send CCMs, use the following command:

  ```
  configure cfm domain domain_name association association_name {ports port_list end-point [up | down]} transmit-interval [3 | 10 | 100 | 1000 | 10000 | 60000 | 600000]
  ```

- To unconfigure the transmission interval for the MEP to send CCMs and return it to the default, use the following command:

  ```
  unconfigure cfm domain domain_name association association_name {ports port_list end-point [up | down]} transmit-interval
  ```

- To enable or disable a MEP, use the following command:
configure cfm domain domain_name association association_name ports port_list end-point [up | down] [enable | disable]

Displaying EAPS MEP Group Bindings

- Display EAPS MEP group bindings with the command: `show eaps cfm groups`

```
X480-48t.2 # sh eaps cfm groups
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>MEP Group Name</th>
<th>Status</th>
<th>Port</th>
<th>MEP ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>eapsCfmGrp1</td>
<td>Up</td>
<td>41</td>
<td>11</td>
</tr>
<tr>
<td>eapsCfmGrp2</td>
<td>Up</td>
<td>31</td>
<td>12</td>
</tr>
</tbody>
</table>
```

Displaying EAPS Output Change

- Display EAPS output changes using the command `show eaps`

The existing output places a ! next to a CFM monitored ring port if the CFM indicates the MEP group for that port is down.

```
X480-48t.1 # sh eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: Off
EAPS Display Config Warnings: Off
EAPS Multicast Add Ring Ports: Off
EAPS Multicast Send IGMP Query: On
EAPS Multicast Temporary Flooding: Off
EAPS Multicast Temporary Flooding Duration: 15 sec
Number of EAPS instances: 1
# EAPS domain configuration :
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Mo</th>
<th>En</th>
<th>Pri</th>
<th>Sec</th>
<th>Control-Vlan VID</th>
<th>Count</th>
<th>Prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>d2</td>
<td>Failed</td>
<td>M</td>
<td>Y</td>
<td>!41</td>
<td>31</td>
<td>v2</td>
<td>(101 )</td>
<td>1</td>
</tr>
</tbody>
</table>
---------------------------------------------------------------------
Flags : (!) CFM Down
```

Configuration Example

Below is a sample configuration of CFM support in EAPS:

```
switch 1 # sh configuration cfm
#
# Module dot1ag configuration.
#
create cfm domain string "MD1" md-level 6
configure cfm domain "MD1" add association string "MD1v1" vlan "v1"
configure cfm domain "MD1" add association string "MD1v2" vlan "v2"
configure cfm domain "MD1" association "MD1v1" ports 17 add end-point down 6
configure cfm domain "MD1" association "MD1v1" ports 23 add end-point down 5
configure cfm domain "MD1" association "MD1v2" ports 17 add end-point down 13
configure cfm domain "MD1" association "MD1v1" ports 17 end-point down add group "eapsCfmGrp1"
configure cfm domain "MD1" association "MD1v1" ports 23 end-point down add
```
group "eapsCfmGrp2"
configure cfm domain "MD1" association "MD1v2" ports 31 end-point down add
group "eapsCfmGrp3"
configure cfm group "eapsCfmGrp1" add rmep 2
configure cfm group "eapsCfmGrp2" add rmep 4
configure cfm group "eapsCfmGrp3" add rmep 12
switch 2 # sh configuration "eaps"s
#
# Module eaps configuration.
#
enable eaps
create eaps d1
configure eaps d1 mode transit
configure eaps d1 primary port 17
configure eaps d1 secondary port 23
enable eaps d1
create eaps d2
configure eaps d2 mode transit
configure eaps d2 primary port 31
configure eaps d2 secondary port 23
enable eaps d2
configure eaps d1 add control vlan v1
configure eaps d1 add protected vlan pv1
configure eaps d2 add control vlan v2
configure eaps d2 add protected vlan pv2
create eaps shared-port 23
configure eaps shared-port 23 mode partner
configure eaps shared-port 23 link-id 100
configure eaps cfm add group eapsCfmGrp1
configure eaps cfm add group eapsCfmGrp2
configure eaps cfm add group eapsCfmGrp3

Limitations

CFM PDU transmit intervals are limited by the supported limits of CFM module. Platforms that do not support CFM in hardware are limited to a minimum interval of 100 ms.

The maximum number of down MEPs is limited by the CFM module. This is as low as 32 MEPs in some platforms. See CFM scaling limitations in EXOS_1AG_(CFM)_Functional_Spec.doc

Platforms Supported

All ExtremeXOS platforms support this feature; however, not all platforms support hardware-based CFM.

Platforms with no hardware-based CFM support are limited to software-based CFM transmit intervals of 100 ms or higher. Hardware-based intervals can go as low as 3.3 ms.

Currently, only the x460 and E4G platforms support hardware-based CFM.