Port Channel and Virtual Port Channel Configuration

This chapter contains the following sections:

Port Channel or Virtual Port Channel Configuration

You can configure a port channel or virtual port channel or a port channel policy using the Cisco APIC GUI, NX-OS style CLI, or REST API.

Configure a Port Channel or Virtual Port Channel Using the GUI

Use the Cisco APIC GUI to configure a port channel or virtual port channel.

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 Expand the **Interface** and **Leaf Interfaces** folders.

Step 4 Right-click the **Profiles** folder and choose **Create Leaf Interface Profile**.

Step 5 In the **Create Leaf Interface Policy** dialog box, enter a name for the policy in the **Name** field.

Step 6 In the **Interface Selectors** area, click **+** to add an access port selector.

Step 7 In the **Create Access Port Selector** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the access port.

b) In the **Interface IDs** field, enter the interface IDs where the host is located.

c) From the **Interface Policy Group** drop-down list, choose **Create PC Interface Policy Group** or **Create VPC Interface Policy Group**.

Step 8 In the **Create PC Interface Policy Group** dialog box or the **Create VPC Interface Policy Group** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the port channel.
b) From the **Port Channel Policy** drop-down list, choose **Create Port Channel Policy**.

Step 9 In the **Create Port Channel Policy** dialog box, complete the following actions:

a) In the **Name** field, enter a name for the policy.
b) In the **Mode** field, choose one of the following options appropriate to your setup:

- **Static Channel - Mode On**
- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-NIC-load**

Note LACP Passive mode is not supported for directly connected hosts. Ports using LACP Passive mode do not initiate an LACP handshake. We recommend that you always use LACP Active instead of LACP Passive. LACP Passive can be used only with Cisco ACI Virtual Edge/TOR policy groups when there is an intermediate Layer 2 device and the Layer 2 device ports are using LACP Active mode.

Note MAC Pinning-Physical-NIC-load mode is not supported for Cisco ACI Virtual Edge.

c) Click **Submit**.

Step 10 In the **Create PC Interface Policy Group** or **Create VPC Interface Policy Group** dialog box, from the **Attached Entity Profile** drop-down list, choose or create an attached entity profile, and then click **Submit**.

Step 11 In the **Create Access Port Selector** dialog box, click **OK**.

Step 12 In the **Create Leaf Interface Policy** dialog box, click **Submit**.

Configure a Port Channel Policy

You can configure one of several types of port channel policies on the Cisco ACI Virtual Edge:

- Link Aggregation Control Policy (LACP) in active mode
- Link Aggregation Control Policy (LACP) in passive mode
- Static mode
- MAC Pinning

You can configure port channel policies through the Cisco APIC GUI or the REST API. However, you can configure port channel mode using the NX-OS Style CLI.

Note When an LACP policy is applied as a vSwitch policy for the VMM domain, the LACP policy is applied only to the VMware vSphere Distributed Switch (VDS) uplinks. However, it is not applied to the Cisco ACI Virtual Edge port channel. This is expected behavior. Cisco ACI Virtual Edge does not support LACP on its uplinks because VDS does not support it for its virtual Ethernet (vEth) interfaces. So the VMM port channel policy is applied only for the VDS uplinks.

Enhanced LACP Policy Support

In Cisco Application Policy Infrastructure Controller (APIC) Release 3.2(7), you can improve uplink load balancing by applying different Link Aggregation Control Protocol (LACP) policies to different distributed virtual switch (DVS) uplink port groups.

Cisco APIC now supports VMware's Enhanced LACP feature, which is available for DVS 5.5 and later. Previously, the same LACP policy applied to all DVS uplink port groups. Before Cisco APIC Release 3.2(7), it was not possible to manage VMware link aggregation groups (LAGs) with Cisco APIC.

When you enable Enhanced LACP policy on the ACI side, it will push the configuration to DVS. Later, even if you remove the policy on the ACI side, enhanced LACP is still available on the DVS side, because after an enhanced LACP policy is enabled, it can not be reverted.

Note Enhanced LACP policy can be enabled either on the ACI or DVS side.

You can choose from up to 20 different load-balancing algorithms when you create a VMware vCenter virtual machine manager (VMM) domain for Cisco Application Centric Infrastructure (ACI) Virtual Edge or VMware VDS. You apply different policies to different uplink portgroups.

You have eight DVS uplink portgroups, and you must configure at least two uplinks in the same policy. So you can have up to four different LACP policies for each DVS. Enhanced LACP supports only active and passive LACP modes.

Note For Cisco ACI Virtual Edge VXLAN mode, it is mandatory to use a load-balancing algorithm having a UDP port. We recommend the algorithm **Source and Destination TCP/UDP Port**. In VLXAN mode, traffic is always sent between VTEP to the FTEP IP. So communication is always between one pair of IP address. So for VXLAN traffic, the only way to distinguish traffic is using the UDP port number.

The following sections provide instructions for configuring multiple LACP policies for DVS uplinks using the Cisco APIC GUI, NX-OS style CLI, or REST API.

Enhanced LACP Limitations

Be aware of the following limitations when using enhanced Link Aggregation Control Protocol (LACP) policies.

- You cannot fall back to the previous version of LACP after upgrading to enhanced LACP.
- You cannot downgrade to a version of Cisco Application Policy Infrastructure Controller (APIC) earlier than 3.2(7) without removing the enhanced LACP configuration. See the procedure Remove the Enhanced LACP Configuration Before a Downgrade, on page 6 in this guide.
- For Cisco Application Centric Infrastructure (ACI) Virtual Edge, VXLAN mode traffic always uses the source IP address as the TEP IP address. To ensure proper load balancing, we recommend the algorithm **Source and Destination TCP/UDP Port**.

- If traffic is present for a Cisco ACI Virtual Edge domain over enhanced LACP, and you increase or reduce the number of uplinks, a traffic loss of 5 or 10 seconds occurs.
- Traffic is disrupted when an enhanced LACP LAG policy name conflicts with the name of a previous enhanced LACP link aggregation group (LAG) policy uplink. If you have an enhanced LACP LAG policy that is named ELACP-DVS for a DVS domain, its uplink is automatically named ELACP-DVS-1, ELACP-DVS-2, ELACP-DVS-3, and so on, depending on the number uplinks configured in the policy.

  Traffic loss occurs if you then try to configure of add another enhanced LAG policy with a name that conflicts with a previous policy uplink name. To remedy the issue, delete the LAG policy and re-create it with a different name.

Create LAGs for DVS Uplink Port Groups Using the Cisco APIC GUI

Improve distributed virtual switch (DVS) uplink port group load balancing by putting the port groups into link aggregation groups (LAGs) and associating them with specific load-balancing algorithms. You can perform this task using the Cisco Application Policy Infrastructure Controller (APIC) GUI.

Before you begin

- You must have created a VMware vCenter virtual machine manager (VMM) domain for VMware VDS or Cisco Application Centric Infrastructure (ACI) Virtual Edge.
- If a vSwitch policy container does not exist, create one.

Note You must configure a port channel policy before you create an enhanced LAG policy. You can create a port channel policy when you create a vCenter domain profile.

Step 1 Log into the Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***domain***.

Step 3 In the work pane, choose **Policy** > **VSwitch Policy**.

Step 4 If you have not already done so, in the **Properties** area, choose a policy.

Step 5 In the **Enhanced LAG Policy** area, click the **+** (plus) icon and then complete the following steps:

a) In the **Name** field, enter the name of the LAG.
b) From the **Mode** drop-down list, choose **LACP Active** or **LACP Passive**.
c) From the **Load Balancing Mode** drop-down list, choose a load-balancing method.
d) In the **Number of Links** selector, choose how many DVS uplink port groups to include in the LAG.

   You can put two to eight uplink port groups into a LAG.

e) Click **Update** and then click **Submit**.

Step 6 Repeat Step 5 to create other LAGs for the DVS.

What to do next

If you are using VMware VDS, associate endpoint groups (EPGs) to the domain with the enhanced LACP policy. If you are using Cisco Application Centric Infrastructure (ACI) Virtual Edge, associate internally created inside and outside port groups with the enhanced LACP policy, then associate EPGs to the domain with the policy.

Associate Internal Port Groups to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI

Associate Cisco Application Centric Infrastructure (ACI) Virtual Edge internally created inside and outside port groups with a VMware vCenter domain with an enhanced LACP policy. You can perform this task using the Cisco Application Policy Infrastructure Controller (APIC) GUI.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Step 1 Log into the Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***domain***.

Step 3 In the work pane, choose **Policy** > **General**.

Step 4 From the **Enhanced LAG Policy** drop-down list, choose a policy.

Step 5 Click **Submit**.

What to do next

Associate endpoint groups (EPGs) with the VMware vCenter domain containing the enhanced LACP policy.

Associate Application EPGs to VMware vCenter Domains with Enhanced LACP Policies Using the Cisco APIC GUI

Associate application endpoint groups (EPGs) with the VMware vCenter domain with LAGs and a load-balancing algorithm. You can perform this task using the Cisco Application Policy Infrastructure Controller (APIC) GUI.

Before you begin

You must have created link aggregation groups (LAGs) for distributed virtual switch (DVS) uplink port groups and associated a load-balancing algorithm to the LAGs.

Note This procedure assumes that you have not yet associated an application EPG with a VMware vCenter domain. If you have already done so, you edit the domain association.

Step 1 Log into Cisco APIC.

Step 2 Go to **Tenants** > *tenant* > **Application Profiles** > *application_profile* > **Application EPGs** > *EPG* > **Domains (VMs and Bare-Metals)**.

Step 3 Right-click **Domains (VMs and Bare-Metals)** and choose **Add VMM Domain Association**.

Step 4 In the **Add VMM Domain Association** dialog box, complete the following steps:

a) From the **VMM Domain Profile** drop-down list, choose the domain that you want to associate the EPG to.

b) From the **Enhanced Lag Policy**, choose the policy configured for the domain that you want to apply to the EPG.

c) (Optional) In the **Delimiter** field, enter one of the following: `|`, `~`, `!`, `@`, `^`, `+`, or `=`.

If you do not enter a symbol, the system default `|` delimiter will appear in the policy.

d) Add remaining values as desired for the domain association, and then click **Submit**.

Step 5 Repeat Step 2 through Step 4 for other application EPGs in the tenant as desired.

Remove the Enhanced LACP Configuration Before a Downgrade

Before you downgrade Cisco Application Policy Infrastructure Controller (APIC) to a release earlier than 3.2(7), you must remove the enhanced LACP configuration. Complete the steps in this procedure to remove the configuration.

Step 1 Reassign uplinks on all ESXi hosts from link aggregation groups (LAGs) to normal uplinks.

Step 2 Remove LAG associations from all EPGs associated with the distributed virtual switch (DVS).

You can expect traffic loss while performing this step.

Step 3 Change port channel settings to static channel or MAC pinning, which will cause traffic to recover once the port channel is up.

Step 4 Remove all LAG-related configuration from the virtual machine manager (VMM).

Step 5 Verify that all LAG-related policies are deleted from VMware vCenter.

What to do next

Downgrade to a Cisco APIC release earlier than 3.2(7).