Node and Interface for L3Out

Modifying Interfaces for L3Out

Modifying Interfaces for L3Out Using the GUI

This procedure modifies an L3Out interface.

Before you begin

- The Cisco ACI fabric is installed, the Cisco APICs are online, and the Cisco APIC cluster is formed and healthy.
- A Cisco APIC fabric administrator account is available that enables creating the necessary fabric infrastructure configurations.
- The target leaf switches are registered in the Cisco ACI fabric and available.
- Port channels are configured when port channels are used for L3Out interfaces.

Procedure

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, expand **tenant_name** > **Networking** > **L3Outs** > ***L3Out*** > **Logical Node Profiles** > ***node_profile*** > **Logical Interface Profiles**.

Step 4 In the Navigation pane, choose the **Logical Interface Profile** that you want to modify.

Step 5 Choose the interface type tab from **Routed Sub-Interfaces**, **Routed Interfaces**, **SVI**, or **Floating SVI**.

Step 6 Double click the existing interface to modify it, or click the **Create** (+) button to add a new interface to the Logical Interface Profile.

Step 7 To add a new interface in the **Path Type** field, choose the appropriate path type.

If **Routed Sub-Interface** or **Routed Interface**, choose **Path Type** as a port or Direct Port Channel. If this is for **SVI**, choose **Path Type** from Port, Direct Port Channel, or Virtual Port Channel (vPC).

Note Direct port-channel support on routed interface and routed sub-interface was available starting with Cisco APIC release 3.2(1).

Step 8 In the **Node** field, choose a node.

Note This is applicable only for non port-channel Path Type. If you selected **Path Type** as **Port** in the previous step, then perform this step. Otherwise, proceed to the next step.

Step 9 In the **Path** field, choose the interface ID or the port-channel name from the drop-down list.

An example of an interface ID is eth 1/1. The port-channel name is the interface policy group name for each direct or virtual port-channel.

Step 10 In the **Description** field, enter a description of the L3Out interface.

Step 11 For **Routed Sub-Interfaces** or **SVI**, in the **Encap** field, choose **VLAN** from the drop-down menu, and enter an integer value for this entry.

Step 12 For **Routed Sub-Interfaces** or **SVI**, in the **Mode** field, choose the VLAN tagging mode.

Step 13 In the **IPv4 Primary / IPv6 Preferred Address** field, enter the primary IP addresses of the path attached to the Layer 3 outside profile.

Step 14 If an IPv6 address is used, in the **IPv6 DAD** field, select **disabled** or **enabled**.

For more information about this field, see the section "Configuring IPv6 Neighbor Discovery Duplicate Address Detection" in the chapter "IPv6 Neighbor Discovery".

Step 15 In the **Link-local Address** field, enter an IPv6 link-local address. This is the override of the system-generated IPv6 link-local address.

Step 16 In the **IPv4 Secondary / IPv6 Additional Addresses** field, enter the secondary IP addresses of the path attached to the Layer 3 outside profile.

Step 17 Check the **ND RA Prefix** box if you wish to enable a Neighbor Discovery Router Advertisement prefix for the interface. The ND RA Prefix Policy option appears.

When this is enabled, the routed interface is available for autoconfiguration and the prefix is sent to the host for autoconfiguration.

While ND RA Interface policies are deployed under bridge domains or Layer 3 Outs, ND prefix policies are deployed for individual subnets. The ND prefix policy is on a subnet level.

The ND RA Prefix applies only to IPv6 addresses.

Step 18 If you checked the **ND RA Prefix** box, select the ND RA Prefix policy that you want to use. You can select the default policy or you can choose to create your own ND RA prefix policy. If you choose to create your own policy, the Create ND RA Prefix Policy screen appears:

a) In the **Name** field, enter the Router Advertisement (RA) name for the prefix policy.
b) In the **Description** field, enter a description of the prefix policy.
c) In the **Controller State** field, check the desired check boxes for the controller administrative state. More than one can be specified. The default is **Auto Configuration** and **On link**.
d) In the **Valid Prefix Lifetime** field, choose the desired value for the length of time that you want the prefix to be valid. The range is from 0 to 4294967295 milliseconds. The default is 2592000.
e) In the **Preferred Prefix Lifetime** field, choose the desired value for the preferred lifetime of the prefix. The range is from 0 to 4294967295 milliseconds. The default is 604800.

f) Click **Submit**.

Step 19 In the **MAC Address** field, enter the MAC address of the path attached to the Layer 3 outside profile.

Step 20 In the **MTU (bytes)** field, set the maximum transmit unit of the external network. The range is 576 to 9216. To inherit the value, enter *inherit* in the field.

Step 21 In the **Target DSCP** field, select the target differentiated services code point (DSCP) of the path attached to the Layer 3 outside profile from the drop-down list.

Step 22 Click **Submit**.

Customizing SVI for L3Out

SVI External Encapsulation Scope

About SVI External Encapsulation Scope

In the context of a Layer 3 Out configuration, a switch virtual interfaces (SVI), is configured to provide connectivity between the ACI leaf switch and a router.

By default, when a single Layer 3 Out is configured with SVI interfaces, the VLAN encapsulation spans multiple nodes within the fabric. This happens because the ACI fabric configures the same bridge domain (VXLAN VNI) across all the nodes in the fabric where the Layer 3 Out SVI is deployed as long as all SVI interfaces use the same external encapsulation (SVI) as shown in the figure.

However, when different Layer 3 Outs are deployed, the ACI fabric uses different bridge domains even if they use the same external encapsulation (SVI) as shown in the figure:

Figure 1: Local Scope Encapsulation and One Layer 3 Out

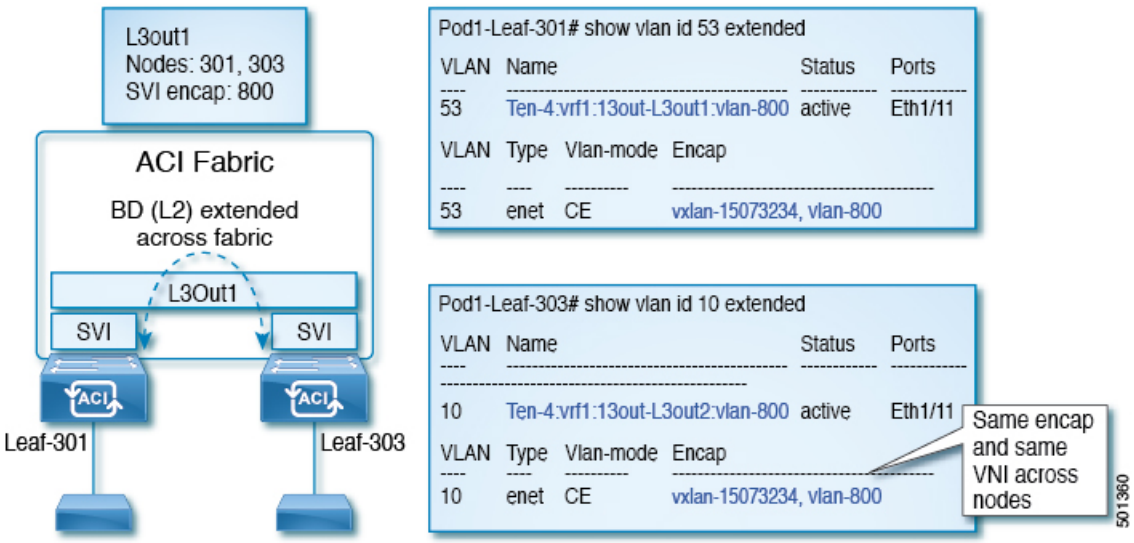
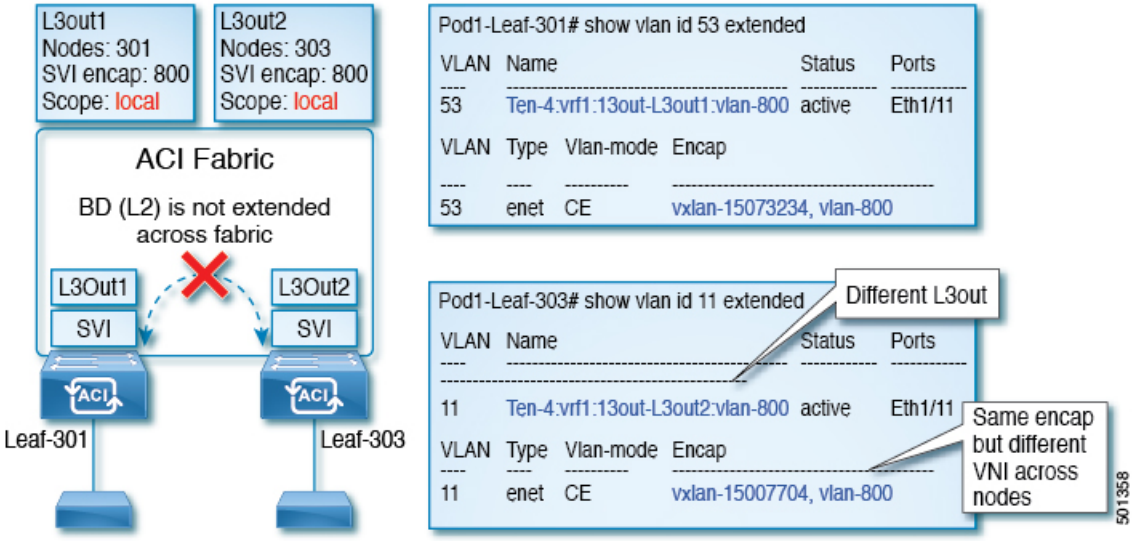


Figure 2: Local Scope Encapsulation and Two Layer 3 Outs

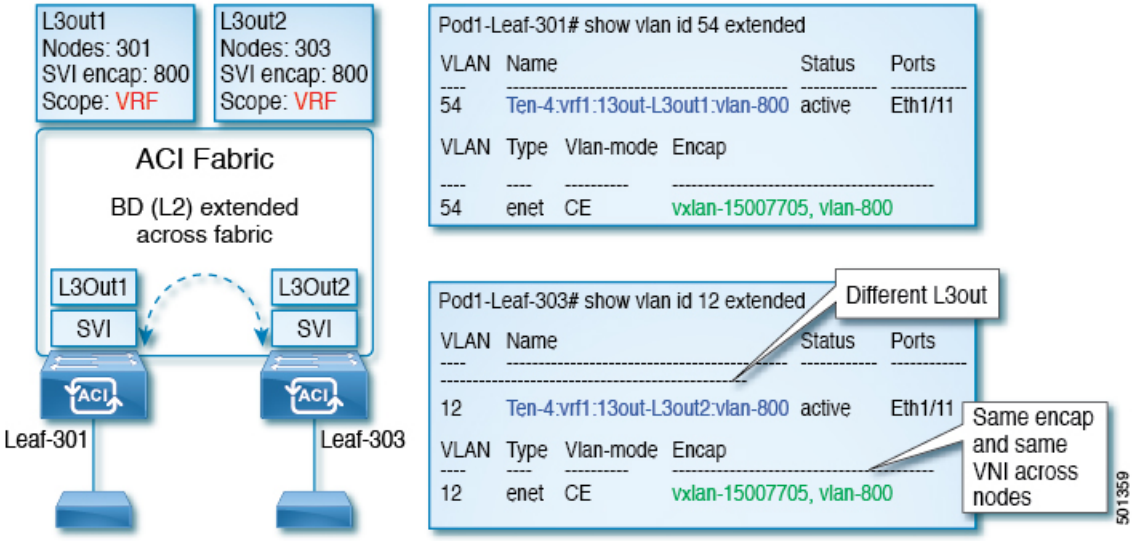


Starting with Cisco APIC release 2.3, it is now possible to choose the behavior when deploying two (or more) Layer 3 Outs using the same external encapsulation (SVI).

The encapsulation scope can now be configured as Local or VRF:

- Local scope (default): The example behavior is displayed in the figure titled *Local Scope Encapsulation and Two Layer 3 Outs*.
- VRF scope: The ACI fabric configures the same bridge domain (VXLAN VNI) across all the nodes and Layer 3 Out where the same external encapsulation (SVI) is deployed. See the example in the figure titled *VRF Scope Encapsulation and Two Layer 3 Outs*.

Figure 3: VRF Scope Encapsulation and Two Layer 3 Outs



Encapsulation Scope Syntax

The options for configuring the scope of the encapsulation used for the Layer 3 Out profile are as follows:

- **Ctx**—The same external SVI in all Layer 3 Outs in the same VRF for a given VLAN encapsulation. This is a global value.
- **Local** —A unique external SVI per Layer 3 Out. This is the default value.

The mapping among the CLI, API, and GUI syntax is as follows:

Table 1: Encapsulation Scope Syntax

CLI	API	GUI
l3out	local	Local
vrf	ctx	VRF

Note The CLI commands to configure encapsulation scope are only supported when the VRF is configured through a named Layer 3 Out configuration.

Guidelines for SVI External Encapsulation Scope

To use SVI external encapsulation scope, follow these guidelines:

- If deploying the Layer 3 Outs on the same node, the OSPF areas in both the Layer 3 Outs must be different.
- If deploying the Layer 3 Outs on the same node, the BGP peer configured on both the Layer 3 Outs must be different.

Configuring SVI External Encapsulation Scope Using the GUI

Before you begin

- The tenant and VRF configured.
- An L3Out is configured and a logical node profile under the L3Out is configured.

Procedure

Step 1 On the menu bar, click > **Tenants** > ***Tenant_name***.

Step 2 In the **Navigation** pane, click **Networking** > **L3Outs** > ***L3Out_name*** > **Logical Node Profiles** > ***LogicalNodeProfile_name*** > **Logical Interface Profiles**.

Step 3 In the **Navigation** pane, right-click **Logical Interface Profiles**, and click **Create Interface Profile**.

Step 4 In the **Create Interface Profile** dialog box, perform the following actions:

a) In the **Step 1 Identity** screen, in the **Name** field, enter a name for the interface profile.

b) In the remaining fields, choose the desired options, and click **Next**.

c) In the **Step 2 Protocol Profiles** screen, choose the desired protocol profile details, and click **Next**.
d) In the **Step 3 Interfaces** screen, click the **SVI** tab, and click the **+** icon to open the **Select SVI** dialog box.
e) In the **Specify Interface** area, choose the desired values for the various fields.
f) In the **Encap Scope** field, choose the desired encapsulation scope value. Click **OK**.

The default value is **Local**.

The SVI External encapsulation scope is configured in the specified interface.

SVI Auto State

About SVI Auto State

Note This feature is available in the APIC Release 2.2(3x) release and going forward with APIC Release 3.1(1). It is not supported in APIC Release 3.0(x).

The Switch Virtual Interface (SVI) represents a logical interface between the bridging function and the routing function of a VLAN in the device. SVI can have members that are physical ports, direct port channels, or virtual port channels. The SVI logical interface is associated with VLANs, and the VLANs have port membership.

The SVI state does not depend on the members. The default auto state behavior for SVI in Cisco APIC is that it remains in the up state when the auto state value is disabled. This means that the SVI remains active even if no interfaces are operational in the corresponding VLAN/s.

If the SVI auto state value is changed to enabled, then it depends on the port members in the associated VLANs. When a VLAN interface has multiple ports in the VLAN, the SVI goes to the down state when all the ports in the VLAN go down.

Table 2: SVI Auto State

SVI Auto State	Description of SVI State
Disabled	SVI remains in the up state even if no interfaces are operational in the corresponding VLAN/s. Disabled is the default SVI auto state value.
Enabled	SVI depends on the port members in the associated VLANs. When a VLAN interface contains multiple ports, the SVI goes into the down state when all the ports in the VLAN go down.

Guidelines and Limitations for SVI Auto State Behavior

Read the following guidelines:

- When you enable or disable the auto state behavior for SVI, you configure the auto state behavior per SVI. There is no global command.

Configuring SVI Auto State Using the GUI

Before you begin

- The tenant and VRF configured.
- An L3Out is configured and a logical node profile and a logical interface profile under the L3Out is configured.

Procedure

Step 1 On the menu bar, click > **Tenants** > ***Tenant_name***.

Step 2 In the **Navigation** pane, click **Networking** > **L3Outs** > ***L3Out_name*** > **Logical Node Profiles** > ***LogicalNodeProfile_name*** > **Logical Interface Profiles**.

Step 3 In the **Navigation** pane, expand **Logical Interface Profile**, and click the appropriate logical interface profile.

Step 4 In the Work pane, click the **SVI** tab, then click the **+** sign to display the **SVI** dialog box.

Step 5 To add an additional SVI, in the **SVI** dialog box, perform the following actions:

a) In the **Path Type** field, choose the appropriate path type.
b) In the **Path** field, from the drop-down list, choose the appropriate physical interface.
c) In the **Encap** field, choose the appropriate values.
d) In the **Auto State** field, choose the SVI in the **Work** pane, to view/change the Auto State value.

The default value is **Disabled**.

Note To verify or change the Auto State value for an existing SVI, choose the appropriate SVI and verify or change the value.

About Cisco Floating L3Outs

Beginning with the Cisco Application Policy Infrastructure Controller (APIC) release 4.2(1), you no longer need to specify multiple Layer 3 outside network connection (L3Out) logical interface paths in a virtual environment.

The floating L3Out feature enables you to configure a L3Out without specifying logical interfaces. The feature saves you from having to configure multiple L3Out logical interfaces to maintain routing when virtual machines move from one host to another. Floating L3Out is supported for VMware vSphere Distributed Switch (VDS).

Beginning with the Cisco APIC release 5.0(1), physical domains are supported.

For more information, see the *Using Floating L3Out to Simplify Outside Network Connections* knowledge base article:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Floating-L3Out.html