Configuring L4-L7 Services

Unmanaged Mode

In unmanaged mode, Cisco APIC allocates only the network resources for the service graph and programs only the fabric side during graph instantiation. You must configure the unmanaged device in an external application or tool.

When you add an unmanaged network device, Cisco APIC does not require the device package for that device.

For more information about unmanaged mode, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Setting Up an Unmanaged Device

For unmanaged devices, the Application Policy Infrastructure Controller (APIC) allocates only the network resources for the service graph and programs only the fabric side during graph instantiation. You cannot configure an unmanaged device in the APIC.

Step 1 Add an unmanaged device cluster.

See Adding an Unmanaged L4-L7 Devices, on page 3.

Step 2 Add at least one concrete device to the unmanaged device cluster.

See Adding a Concrete Device to an Unmanaged L4-L7 Device Cluster, on page 7.

Step 3 For a virtual concrete device, add at least one vNIC to the concrete interface on the device.

See Adding a vNIC to an Unmanaged Virtual Concrete Device, on page 8.

Step 4 For a physical concrete device, add at least one path to the concrete interface on the device.

See Adding a Path Interface to an Unmanaged Physical Concrete Device, on page 9.

Step 5 Add at least one logical interface to the unmanaged device cluster.

See Adding a Cluster Interface to an Unmanaged L4-L7 Device, on page 5.

Step 6 Create an L4-L7 service graph template with the configuration parameters you want to use for the device cluster.

See Creating a Service Graph Template, on page 19.

Step 7 Apply the L4-L7 service graph template to configure the device cluster.

See Applying a Service Graph Template, on page 20.

Managed Mode

By default, when a device is registered with Cisco APIC, the device is set to be in managed mode. When a device is configured as managed, Cisco APIC manages the device and programs the device during graph instantiation.

Setting Up a Managed Device

Step 1 Add a managed device cluster.

See Adding a Managed L4-L7 Device, on page 4.

Step 2 Add at least one concrete device to the managed device cluster.

See Adding a Concrete Device to a Managed L4-L7 Device Cluster, on page 7.

Step 3 For a virtual concrete device, add at least one vNIC to the concrete interface on the device.

See Adding a vNIC to a Managed Virtual Concrete Device, on page 8.

Step 4 For a physical concrete device, add at least one path to the concrete interface on the device.

See Adding a Path Interface to a Managed Physical Concrete Device, on page 9.

Step 5 Add at least one logical interface to the managed device cluster.

See Adding a Cluster Interface to a Managed Device Cluster, on page 6.

Step 6 Create an L4-L7 service graph template with the configuration parameters you want to use for the device cluster.

See Creating a Service Graph Template, on page 19.

Step 7 Apply the L4-L7 service graph template to configure the device cluster.

See Applying a Service Graph Template, on page 20.

Layer 4 to Layer 7 Device Clusters

A L4-L7 device cluster, also known as a logical device, contains one or more concrete devices that act as a single device. A L4-L7 device cluster has cluster interfaces, also known as logical interfaces, which describe the interface information for the device cluster.

L4-L7 device clusters can be managed or unmanaged.

When the Application Policy Infrastructure Controller (APIC) renders and instantiates service graph templates, it does the following:

- Associates function node connectors with the cluster interfaces.
- Allocates network resources for a function node connector, such as VLAN or Virtual Extensible Local Area Network (VXLAN) resources
- Programs those network resources onto the cluster logical interfaces

The service graph template uses a specific device that is based on a device selection policy, known as a logical device context.

Each device cluster can have a maximum of two concrete devices in active/standby mode.

Adding an Unmanaged L4-L7 Devices

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click **Add**.

Step 8 On the **Create L4-L7 Devices** screen, complete the following fields:

a) Ensure that **Managed** is not checked.

b) In the **Device Cluster** field, enter a unique name for the cluster.

c) Choose **True** from the **Promiscuous Mode** drop-down list, to enable promiscuous mode. When promiscuous mode is enabled on an interface, all packets received on the interface are sent to the central point or to the Services Processing Unit (SPU) regardless of the destination MAC address of the packet.

d) From the **Context Aware** drop-down list, choose one of the following:

- **Single**—The device cluster must be given to a specific tenant and cannot be shared across multiple tenants. This is the default value.
- **Multiple**—The device cluster can be shared across multiple tenants of a given type that you are hosting on a provider network.

e) From the **Function Type** drop-down list, choose one of the following:

- **Go To**—A Go To device has a specific destination. This is the default value.

- **Go Through**—A Go Through device is a transparent device. A packet goes through the device without being addressed to it, and the endpoints are not aware of the device.

f) From the **Service Type** drop-down list, choose one of the following:

- **ADC**—One-arm and two-arm deployment modes.
- **Firewall**—Routed and transparent deployment modes.
- **IDS/IPS**—IDS and IPS deployment modes.
- **Other**—Any other mode.

g) From the **Device Type** drop-down list, choose one of the following:

- **Physical**
- **Virtual**

h) Click **Select** and check the domain that you want to use.

The domain must be a VMM domain if the device type is Virtual, and a physical domain if the device type is Physical.

Step 9 Click **Submit**.

Adding a Managed L4-L7 Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click **Add**.

Step 8 On the **Create L4-L7 Devices** screen, complete the following fields:

a) Ensure that **Managed** is checked.
b) In the **Device Cluster** field, enter a unique name for the cluster.
c) Click **Select** and check the device package that you want to use.
d) Click **Model** and check the device package model that you want to use.
e) Choose **True** from the **Promiscuous Mode** drop-down list, to enable promiscuous mode. When promiscuous mode is enabled on an interface, all packets received on the interface are sent to the central point or to the Services Processing Unit (SPU) regardless of the destination MAC address of the packet.
f) From the **Context Aware** drop-down list, choose one of the following:

- **Single**—The device cluster must be given to a specific tenant and cannot be shared across multiple tenants. This is the default value.
- **Multiple**—The device cluster can be shared across multiple tenants of a given type that you are hosting on a provider network.

g) From the **Function Type** drop-down list, choose one of the following:

- **Go To**—A Go To device has a specific destination. This is the default value.
- **Go Through**—A Go Through device is a transparent device. A packet goes through the device without being addressed to it, and the endpoints are not aware of the device.

h) From the **Service Type** drop-down list, choose one of the following:

- **ADC**—One-arm and two-arm deployment modes.
- **Firewall**—Routed and transparent deployment modes.
- **IDS/IPS**—IDS and IPS deployment modes.
- **Other**—Any other mode.

i) From the **Device Type** drop-down list, choose one of the following:

- **Physical**
- **Virtual**

j) Click **Select** and check the domain that you want to use.

The domain must be a VMM domain if the device type is Virtual, and a physical domain if the device type is Physical.

k) From the **APIC to Device Management Connectivity** drop-down list, choose the type of connectivity. Choose **Out-of-Band** when you are connecting to a device that is outside of the fabric or **In-Band** when you are connecting to a device through the fabric.

l) Click **Select** and check the EPG that you want to use.

m) Enter the virtual IP address, port, user name, and password for the cluster management interface.

Step 9 Click **Submit**.

Cluster Interface

Adding a Cluster Interface to an Unmanaged L4-L7 Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the unmanaged L4-L7 device that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Cluster Interface**.

Step 9 Click **Add**.

Step 10 On the **Add Cluster Interface to L4-L7 Device** screen, complete the following fields:

a) Enter a unique name for the logical interface.

b) In the **Encapsulation** field, enter the traffic encapsulation identifiers for the logical interface.

The valid VLAN range for encapsulation is between 1 and 4094.

Step 11 Click **Submit**.

Adding a Cluster Interface to a Managed Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the managed L4-L7 device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Cluster Interface**.

Step 9 Click **Add**.

Step 10 On the **Add Cluster Interface to L4-L7** screen, complete the following fields:

a) Enter a unique name for the logical interface.

b) Click **Select** and check the logical interface type that you want to use for managed L4-L7 device cluster.

Step 11 Click **Submit**.

Concrete Devices

A concrete device has concrete interfaces. When a concrete device is added to a logical device cluster, concrete interfaces are mapped to the logical interfaces. During service graph template instantiation, VLANs and VXLANs are programmed on concrete interfaces that are based on their association with logical interfaces.

You can create multiple cluster interfaces on a concrete device and then specify which cluster interface will be used for the connector in the device selection policy. This cluster interface can be shared by using multiple service graph instantiations.

Adding a Concrete Device to an Unmanaged L4-L7 Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the unmanaged physical L4-L7 device cluster that you want to update and click **View Details**.

Check the **Device Type** column to determine if the device cluster is physical or virtual.

Step 8 Click **Concrete Device**.

Step 9 Click **Add**.

Step 10 On the **Add Concrete Device to L4-L7** screen, complete the following fields:

a) In the **Device Name** field, enter a unique name for the concrete device.
b) In the **Device Context Label** field, enter the label for the device cluster context.
c) For a virtual device cluster, in the **VM Name** field, enter the name of the VM where the device is hosted.
d) For a virtual device cluster, in the **vCenter Name** field, enter the name of the VMware vCenter where the VM is located.

Step 11 Click **Submit**.

Adding a Concrete Device to a Managed L4-L7 Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4 - L7 Devices**.

Step 7 Click the row with the managed physical L4-L7 device cluster where you want to create the concrete device and click **View Details**.

Check the **Device Type** column to determine if the device cluster is physical or virtual.

Step 8 Click **Concrete Device**.

Step 9 Click **Add**.

Step 10 On the **Add Concrete Device to L4-L7** screen, complete the fields, including the following:

a) In the **Device Name** field, enter a unique name for the concrete device.
b) In the **Device Context Label** field, enter the label for the device cluster context.
c) For a virtual device cluster, in the **VM Name** field, enter the name of the VM where the device is hosted.

d) For a virtual device cluster, in the **vCenter Name** field, enter the name of the VMware vCenter where the VM is located.
e) Enter the virtual IP address, port, user name, and password for the cluster management interface.

Step 11 Click **Submit**.

Adding a vNIC to an Unmanaged Virtual Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the L4-L7 device cluster that you want to update and click **View Details**.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **vNIC to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the fields, including the following:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) In the **vNIC** field, enter the vNIC assigned to this interface.
d) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

Adding a vNIC to a Managed Virtual Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the managed L4-L7 device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **vNIC to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the following fields:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) In the **vNIC** field, enter the vNIC assigned to this interface.
d) Click **Select** and check the logical interface where you want to add the path.

Adding a Path Interface to an Unmanaged Physical Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the unmanaged L4-L7 device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **Path to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the fields, including the following:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) For virtual device, enter vNIC.
d) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

Adding a Path Interface to a Managed Physical Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Devices**.

Step 7 Click the row with the managed L4-L7 device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **Path to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the following fields:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) For virtual device, enter vNIC.
d) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

APIC Function Profiles

An APIC function profile provides default values for the parameters of a particular function associated with a device package that is managed by Cisco APIC. You can then include one or more APIC function profiles in an L4-L7 service graph template. For example, you can create a function profile that provides default values for the Cisco ASA firewall function.

In Cisco UCS Director, you create APIC function profiles within function profile groups.

Function profile groups organize function profiles to make it easier to identify the profiles that you want to include in a specific service graph template.

Note Cisco UCS Director supports only the configuration of Cisco ASA devices through APIC function profiles and service graphs. You can create service graph template and function profile with load balancer service. But the parameters that are added for the function profile through individual workflow task, user interface action, and REST API in Cisco UCS Director, are supported for firewall service alone.

Creating an APIC Function Profile Group

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click **Add**.

Step 8 On the **Add Function Profile Group** screen, enter a name and description for the group and click **Submit**.

What to do next

Add one or more APIC function profiles to the function profile group.

Creating an APIC Function Profile

Note Cisco UCS Director supports only the configuration of Cisco ASA devices through APIC function profiles and service graphs.

Before you begin

- Create an APIC function profile group.
- Create an APIC firewall policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to add a function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 Click **Add**.

Step 10 On the **Create Function Profile** screen, complete the following fields:

a) Add a unique name and description for the function profile.

b) Click **Select** and check the row with the APIC account, device, and function that you want to use.

For example, to configure a firewall for a Cisco ASA 1.2, check a row that has a Device Package Name of CISCO-ASA-1.2 and a Function of Firewall. After you validate your selection, the function displays next to **Function Name**.

c) If you chose a load balancing function, in the **Load Balancer Parameters** area, complete the following fields:

- **External ID**
- **External Netmask**
- **Internal ID**
- **Internal Netmask**
- **Services**—Use a comma-separated list to include multiple services.

- **LB IPv4 IP**

d) Optional. If you chose a firewall function, click **Select** and check the APIC firewall policy that you want to assign to this function profile.

If the list does not include the firewall policy you need, click **Add** to create a new policy.

Alternately, navigate to **Policy** > **Resource Groups** > **APIC Firewall Policy**, and then click **Add** to create a firewall policy.

e) Click **Submit**.

What to do next

Click **View Details** and add one or more parameters to the function profile from **Function Profile Parameters**. After you add the parameters, they are displayed on either **L4L7 Function Profile Parameters** or **Function Profile Function Parameters**.

Adding ACL Parameters to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameter**.

Step 11 Choose **Add ACL to Function Profile**.

Step 12 On the **Add ACL to Function Profile** screen, complete the following fields:

a) In the **ACL List Name** field, enter the name of the Access Control List.

b) In the **ACE Name** field, enter the name of the Access Control Entry in the ACL to specify the permit or deny rule for packets.

c) From the **Protocol** drop-down list, choose one of the following protocols:

- **ip**
- **tcp**
- **udp**
- **icmp**

d) Check **Source Any** if you want the ACL to apply to any source IP address.

If you do not check this box, enter a single IP address, an IP address range, or a network address or subnet address in the **Source Address** field.

e) Check **Destination Any** if you want the ACL to apply to any destination IP address.

If you do not check this box, you can enter a single IP address, an IP address range, or a network address or subnet address in the **Destination Address** field.

f) From the **Action** drop-down list, choose one of the following:

- **deny** if you want this ACL to drop the packet.
- **allow** if you want this ACL to forward the packet. The ACL denies all packets that you do not specifically allow.

g) In the **Order** field, enter the order of this entry in the ACL.

Step 13 Click **Submit**.

Adding an Interface to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Interface to Function Profile**.

Step 12 On the **Add Interface to Function Profile** screen, complete the following fields:

a) Enter a unique name for the interface.

b) From the **Type** drop-down list, choose one of the following:

- **External**
- **Internal**

c) In the **IPv4 Address** field, enter the IPv4 address for the interface.

d) In the **Security Level** field, enter the security level for the interface.

The security level can be from 0 (lowest) to 100 (highest). The Cisco ASA uses the security level to determine the type of traffic allowed to and from the interface. For example, you can assign a higher security level to an interface that handles internal traffic and a lower security level to an interface that handles external traffic.

e) Click **Select** and check the bridge group that you want to use for this interface.

f) Click **Select** and check the ACL that you want to use for inbound traffic.

g) Click **Select** and check the ACL that you want to use for outbound traffic.

Step 13 Click **Submit**.

Adding a Bridge Group Interface to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Bridge Group Interface to Function Profile**.

Step 12 On the **Add Bridge Group Interface to Function Profile** screen, complete the following fields:

- **Bridge Group ID**—Enter an integer between 1 and 100.
- **IPv4 Address Value**—Enter the IPv4 address for the bridge group interface.

Step 13 Click **Submit**.

Adding a Static Route to an Interface on an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Static Route to Interface on APIC Function Profile**.

Step 12 On the **Add Static Route to Interface on APIC Function Profile** screen, complete the following fields:

a) Click **Select** and check the interface you want to update.

b) From the **Type** drop-down list, choose either **IPv4** or **IPv6**.

c) If you chose **IPv4**, complete the following fields:

- **Gateway Address**
- **Network Mask**
- **Network**
- **Metric**

d) If you chose **IPv6**, complete the following fields:

- **Gateway Address**
- **Hop Count**
- **Prefix**
- **Tunneled**

Step 13 Click **Submit**.

Adding a Network Object to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameter**.

Step 11 Choose **Add Network Object to Function Profile**.

Step 12 On the **Add Network Object to Function Profile** screen, complete the following fields:

a) In the **Network Object Name** field, enter a unique name for the network object.

b) From the **Network Object Type** drop-down list, choose one of the following types:

- **FQDN**
- **Host IP Address**
- **IP Address Range**

- **Network IP Address**

c) If you chose **FQDN**, enter the fully qualified domain name for this network object.
d) If you chose **Host IP Address**, enter the IP address that you want to use for this network object.
e) If you chose **IP Address Range**, enter the range of IP addresses that you want to use for this network object.
f) If you chose **Network IP Address**, enter the IP address that you want to use for this network object.

Step 13 Click **Submit**.

Adding a Service Object to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Service Object to Function Profile**.

Step 12 On the **Add Service Object to Function Profile** screen, complete the following fields:

a) In the **Service Object Name** field, enter a unique name for the service object.
b) Enter a description of the service object.
c) In the **Protocol Type** field, enter the IP protocol name or number for the service object.
d) From the **Service Object Type** drop-down list, choose one of the following types:

- **icmp**
- **icmp6**
- **tcp**
- **udp**

After you choose the type, you are prompted to enter additional parameters for that type.

e) If you chose **icmp**, enter the **Code** and **Type** for the service object.
f) If you chose **icmp6**, enter the **Code** and **Type** for the service object.
g) If you chose **tcp**, enter the **High Port**, **Low Port**, and **Operator** for the following fields:

- **TCP Destination**
- **TCP Source**

h) If you chose **udp**, enter the **High Port**, **Low Port**, and **Operator** for the following fields:

- **UDP Destination**—
- **UDP Source**—Enter the **High Port**, **Low Port**, and **Operator**.

Step 13 Click **Submit**.

Creating a NAT Rule for an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Create NAT Rule**.

Step 12 On the **Create NAT Rule** screen, complete the following fields:

a) Enter a unique name for the NAT rule.

b) Click **Select** and check the source real object that you want to use.

c) Click **Select** and check the source mapped object that you want to use.

d) From the **Type** drop-down list, choose one of the following:

- **Static**
- **Dynamic**

e) Click **Select** and check the destination real object that you want to use.

f) Click **Select** and check the destination mapped object that you want to use.

g) Click **Select** and check the service real object that you want to use.

h) Click **Select** and check the service mapped object that you want to use.

i) In the **DNS** field, enter the IP address or the fully qualified domain name (FQDN) of the DNS server that you want to use.

j) In the **Order** field, enter the order of the rule in an access list.

The order of the rules in an access list determines how traffic is handled and which rule the Cisco ASA applies to the traffic. For an access list with multiple rules, the Cisco ASA goes through the rules in order and applies the first rule that matches the traffic.

k) In the **Uni-Direction** field, enter unidirectional so that the destination addresses cannot initiate traffic to the source addresses.

l) Click **Select** and check the source interface that you want to use.

m) Click **Select** and check the destination interface that you want to use.

Step 13 Click **Submit**.

Adding a Network Object Group to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 From **More Actions** drop-down list, choose **Add Network Object Group to Function Profile**.

Step 12 On the **Add Network Object Group to Function Profile** screen, complete the following fields:

a) Enter a unique name and description for the network object group.

b) From the **Network Object Group Type** drop-down list, choose one of the following:

- **Host IP Address**
- **Network Address**
- **Network Object**

c) If you chose **Host IP Address**, enter an IPv4 or IPv6 address for the host.

d) If you chose **Network Address**, enter one of the following:

- An IPv4 address with netmask in the following format: 10.10.10.10/255.255.255.255
- An IPv6 address with prefix in the following format: X:X:X:X:X:X/<0-128>

e) If you chose **Network Object**, click **Select** and check the network objects that you want to include.

Step 13 Click **Submit**.

Service Graph Templates

A service graph template contains configuration parameters, which you can specify through one or more of the following:

- Device package
- EPG

- Application profile
- Tenant context

You can apply a service graph template to multiple devices and ensure that all of those devices have the same configuration.

A function node within a service graph template can require one or more configuration parameters. You can lock the parameter values to prevent any additional changes.

The values of the configuration parameters in a service graph are passed to the device script within the device package. The device script converts the parameter data to the configuration that is downloaded onto the device.

Creating a Service Graph Template

Before you begin

Create at least one function profile for the function and device.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Click **Create L4 L7 Service Graph Template**.

Step 8 On the **Create L4 L7 Service Graph Template** screen, complete the following fields:

a) Enter a unique name and description for the service graph template.

b) From the **Type** drop-down list, choose the type of template you want to create.

The template type determines which configuration parameters you can include in the service graph template. The template type can be one of the following:

- **Single Node - Firewall in Transparent Mode**—A single node graph that inserts a firewall into the traffic path. The graph configures the firewall in transparent mode without routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Single Node - Firewall in Routed Mode**—A single node graph that inserts a firewall into the traffic path. The graph configures the firewall in routed mode, which performs the routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Single Node - ADC in One-Arm Mode**—A single node graph that inserts an ADC into the traffic path. The graph configures the ADC in 1-ARM mode. The bridge domain is used for traffic that is explicitly provided.
- **Single Node - ADC in Two-Arm Mode**—A single node graph that inserts an ADC into the traffic path. The graph configures the ADC in 2-ARM mode without routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Two Nodes - Firewall in Transparent and ADC in One-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in transparent mode without routing and the

ADC in 1-ARM mode. The bridge domain that is used for the traffic from the firewall to the ADC and the ADC to the provider EPG is explicitly provided.

- **Two Nodes - Firewall in Routed and ADC in One-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in routed mode and the ADC in 1-ARM mode. The bridge domain that is used for the traffic in to and out of the ADC is explicitly provided.
- **Two Nodes - Firewall in Routed and ADC in Two-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in routed mode and the ADC in 2-ARM mode. The bridge domain that is used for the traffic from the firewall to the ADC and the firewall to the consumer EPG is explicitly provided.
- **Two Nodes - Firewall in Transparent and ADC in Two-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in transparent mode and the ADC in 2-ARM mode. The bridge domain that is used for the traffic for Firewall to ADC is explicitly provided.

c) Complete the following fields to add the configurations to the service graph template. If you have chosen Two Nodes template type, you have to specify the following details for two nodes.

If you chose a template type with a firewall, the firewall is always Node One, whether you choose a Single Node or Two Nodes template type. If you chose a template type with an ADC, the ADC is Node One for a Single Node template type and Node Two for a Two Nodes template type.

- **Managed**—Specifies whether the device is managed or unmanaged. For unmanaged device, you can enable policy-based route redirect by choosing **true** from **Route Redirect** drop-down list. For a managed device, complete the following fields.
  - **Function Name**—Specifies the virtual function for a managed device. Click **Select** and choose a function name that you want to use. This is a single virtual function on a service device such as a firewall, a load balancer, or an SSL offloading device.
  - **Function Profile**—Specifies the function profile for a managed device. Click **Select** and choose a function profile that you want to use. The profile includes the abstract device configuration, the abstract group configuration, and the abstract function configuration.
- **Route Redirect**—This field is applicable for ADC and Firewall Routed mode. Choose **true** from the drop-down list to enable policy-based route redirect on the ADC or Firewall Routed mode.

Step 9 Click **Submit**.

Applying a Service Graph Template

Before you begin

Depending upon the configuration parameters you plan to use, create the following:

- Consumer EPG or external network
- Provider EPG or external network
- Contract
- Device clusters

- Cluster interfaces
- Bridge domains, if you plan to use a general connector type
- Router configuration, if you plan to use route peering
- Redirect Policy

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Choose the service graph template with managed or unmanaged node that you want to apply.

Check the **Managed** column of the **Nodes** tab of service graph template to determine if the node is managed or unmanaged.

Step 8 Click **Apply L4 L7 Service Graph Template**.

Step 9 On the **Apply L4 L7 Service Graph Template** screen, complete the following fields:

a) From the **Consumer EPG/External Network** drop-down list, choose either **EPG** or **External Network** and then do one of the following:

- Click **Select** and check the consumer EPG you want to use.
- Click **Select** and check the consumer external network you want to use.

b) From the **Provider EPG/External Network** drop-down list, choose either **EPG** or **External Network** and then do one of the following:

- Click **Select** and check the provider EPG you want to use.
- Click **Select** and check the provider external network you want to use.

c) From the **Create a New Contract/Choose an Existing Contract Subject** drop-down list, choose one of the following:

- **Create a New Contract** and then complete the contract name and filters fields for that contract.
- **Choose an Existing Contract Subject** and then click **Select** and check the contract subject that you want to use.

d) In the **Node One Consumer Connector** area, the status of the policy-based routing is displayed. When the policy-based routing status is true, the **Redirect Policy** drop-down list appears from which you can chose a redirect policy for the contract subject. You have to choose the device cluster, function profile, the consumer connector type and the consumer layer 3 destination virtual IP (VIP) address, and then complete the appropriate fields as per the chosen consumer connector type.

Note The function profile is enabled only when the function profile is not provided as input while creating the service graph template.

- **General**—Choose the **Consumer Bridge Domain** and **Consumer Cluster Interface**.
- **Route Peering**—Choose the **Router Configuration**, **Consumer Cluster Interface**, and **Consumer External Network**.

e) In the **Node One Provider Connector** area, the status of the policy-based routing is displayed. You can choose the provider connector type and the provider layer 3 destination VIP address, and then complete the appropriate fields as per the chosen provider connector type.

- **General**—Choose the **Provider Bridge Domain** and **Consumer Cluster Interface**.
- **Route Peering**—Choose the **Router Configuration**, **Provider Cluster Interface**, and **Provider External Network**.

f) If your service graph or service graph template is a Two Node type, complete the **Node Two Connector** fields for that node.

Step 10 Click **Submit**.

Service Graphs

Service graphs identify the set of network or service functions that are needed by an application. You can instantiate service graphs on the ACI fabric through Cisco UCS Director.

By using a service graph, you can install a service, such as an ASA firewall, once and deploy it multiple times in different logical topologies. Each time the graph is deployed, ACI takes care of changing the configuration on the firewall to enable the forwarding in the new logical topology.

A service graph represents the network using the following elements:

- Function node—A function node represents a function that is applied to network traffic, such as a transform (SSL termination, VPN gateway), filter (firewalls), or terminal (intrusion detection systems). A function within the service graph might require one or more parameters and have one or more connectors.
- Terminal node—A terminal node enables input and output from the service graph.
- Connector—A connector enables input and output from a node.
- Connection—A connection determines how traffic is forwarded through the network.

After you configure a service graph, the network services are automatically configured according to the service function requirements in the service graph. This does not require any change in the service device.

A service graph is represented as two or more tiers of an application with the appropriate service function inserted between them.

A service appliance (or device) performs a service function within the graph. One or more service appliances might be required to render the services required by a graph. One or more service functions can be performed by a single-service device.

Service graphs and service functions have the following characteristics:

- Traffic sent or received by an endpoint group can be filtered based on a policy, and a subset of the traffic can be redirected to different edges in the graph.

- Service graph edges are directional.
- Taps (hardware-based packet copy service) can be attached to different points in the service graph.
- Logical functions can be rendered on the appropriate (physical or virtual) device, based on the policy.
- The service graph supports splits and joins of edges, and it does not restrict the administrator to linear service chains.
- Traffic can be reclassified again in the network after a service appliance emits it.
- Logical service functions can be scaled up or down or can be deployed in a cluster mode or 1:1 active-standby high-availability mode, depending on the requirements.

For more information about the requirements of service graphs and their deployment, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Adding a Service Graph

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Click **Add**.

Step 8 On the **Add Service Graph** screen, complete the fields, including the following:

a) Enter a unique name and description for the service graph.

b) Click **Select** and check the node that you want to use.

If the node you want to use is not in the list, click **Add** to create the node.

Step 9 Click **Submit**.

Adding a Filter to a Service Graph Node

A filter policy is a group of resolvable filter entries. Each filter entry is a combination of network traffic classification properties.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Click the service graph you want to update and click **View Details**.

Step 8 Click the node where you want to add a filter and click **View Details**.

Step 9 Click **Connectors**.

Step 10 Click **Add**.

Step 11 On the **Add Filter to Service Graph Node** screen, complete the following fields:

a) From the **Connector Mode** drop-down list, choose **internal** or **external**.

b) Click **Select** and check the filter that you want to use.

Step 12 Click **Submit**.

Custom Quality of Service

Achieving the required Quality of Service (QoS) by effectively managing the priority of applications on the fabric is important when deploying an end-to-end solution. Thus, QoS is the set of techniques to manage data center fabric resources.

When QoS is used in ACI to classify packets, packets are classified using layer 2 Dot1P policy, layer 3 differentiated services code point (DSCP) policy, or contracts. DSCP/Dot1p Policy is configured and applied at the EPG level through custom QoS policy.

Adding a Custom QOS Policy

Create a custom QoS policy and then associate the policy with a cluster interface context.

Before you begin

Create the tenant, application, and EPGs that will consume the custom QoS policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click **Add**.

Step 8 On the **Create Custom QOS Policy** screen, complete the following fields:

a) Enter a unique name for the custom QOS policy.

b) Enter a short description for the custom QOS policy.

Step 9 Click **Submit**.

Adding a DSCP to a Priority Map

DSCP policy within the custom QoS policy is a set of rules; each rule gives mapping of a range of DSCP values to a DSCP target.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click the row with the custom QoS policy to which you want to add DSCP policy and click **View Details**.

Step 8 Click **DSCP to Priority Map**.

Step 9 Click **Add**.

Step 10 On the **Add DSCP to Priority Map** screen, complete the following:

a) (Optional) Choose the priority level of the DSCP policy in QoS as **Unspecified**, **Level3**, **Level2**, or **Level1**. By default, the unspecified is set as priority.

b) From the **DSCP Range From** and **DSCP Range To** drop-down lists, choose the starting and ending value for the DSCP range. To set the DSCP range from 0 to 63, choose **Enter customized value** from the drop-down lists and enter the actual value in the **Enter DSCP Range From** and **Enter DSCP Range To** fields.

c) (Optional) Choose a DSCP target to which the DSCP range has to be mapped. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 63 as the DSCP target in the **Enter DSCP Target** field.

d) (Optional) Choose a target class of service (CoS) from the drop-down list. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 8 as the target CoS in the **Enter Target Cos** field.

Step 11 Click **Submit**.

Adding a Dot1P Classifier

Dot1P policy within the custom QoS policy is a set of rules; each rule gives mapping of a range of Dot1P values to a DSCP target.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click the row with the custom QoS policy to which you want to add Dot1P policy and click **View Details**.

Step 8 Click **Dot1P Classifier**.

Step 9 Click **Add**.

Step 10 On the **Add Dot1P Classifier** screen, complete the following:

a) Choose the priority level of the Dot1P policy in QoS as **Unspecified**, **Level3**, **Level2**, or **Level1**. By default, the unspecified is set as priority.

b) From the **Dot1P Range From** and **Dot1P Range To** drop-down lists, choose the starting and ending value for the Dot1P range.

c) Choose a DSCP target to which the Dot1P range has to be mapped. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 64 as the DSCP target in the **Enter DSCP Target** field.

d) Choose a target cost of service (CoS) from the drop-down list.

Step 11 Click **Submit**.

Adding a Logical Device Context

The service graph uses a specific device based on a device selection policy, known as a logical device context.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Logical Device Context**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Logical Device Context** screen, complete the following fields:

a) Click **Select** and check the device cluster that you want to use.

b) Click **Select** and check the contract name that you want to use.

c) Click **Select** and check the graph name that you want to use.

d) Click **Select** and check the node name that you want to use.

e) Enter a unique name for the device context. The name should not exceed 64 characters.

Step 9 Click **Submit**.

Adding a Subnet to a Logical Device Context

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Logical Device Context**.

Step 7 Click the row with the logical device context to which you want to add a subnet and click **View Details**.

Step 8 Click **Cluster Interface Context**.

Step 9 Click the row with the cluster interface context to which you want to add a subnet and click **View Details**.

Step 10 Click **Subnets**.

Step 11 Click **Add**.

Step 12 On the **Add Subnet to Cluster Interface Context** screen, complete the following fields:

a) Enter a gateway IP address in the format: <valid IP address>/<valid prefix length>. For example, 10.10.10.1/24.

If this gateway is for Anycast, the netmask must be **/32** and check the **Subnet Control (No Default SVI Gateway)** check box to not to set the subnet as the default SVI gateway.

b) From the **Scope** drop-down list, choose **Private to VRF** or **Advertised Externally**. By default, the **Private to VRF** is set as the scope. The **Private to VRF** implies that the subnet can only be used in the tenant. The Advertised Externally option is used to advertise tenant subnets externally on the L3Out.
c) Check the **Shared Between VRFs** check box to define subnets under an endpoint group, with the shared option configured, to route leak to other tenants within the fabric.
d) Enter short description for the subnet.
e) Check the **Subnet Control (ND RA Prefix)** check box to apply control specific to ND RA prefix protocols to the subnet. By default, the check box is checked.
f) Check the **Subnet Control (No Default SVI Gateway)** check box to not to configure Pervasive SVI for the subnet. This setting is used to leak more specific prefix routes to other VRFs. If the **Subnet Control (No Default SVI Gateway)** check box is checked, you can use /32 netmask for the subnet, especially for Anycast services. By default, the check box is left unchecked.
g) Check the **Subnet Control (Querier IP)** check box to enable IGMP snooping on the subnet. By default, the check box is left unchecked.
h) Check the **Preferred** check box to set the subnet as the preferred subnet for the device context. By default, the check box is left unchecked.
i) Check the **Type Behind Subnet** check box to enable AnyCast MAC address. By default, the check box is left unchecked. The **MAC address** field appears only when the **Type Behind Subnet** check box is checked. Enter a MAC address in the format: xx:xx:xx:xx:xx:xx. For example, aa:11:bb:11:cc:11.

Step 13 Click **Submit**.

Adding a Cluster Interface Context

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Logical Device Context**.

Step 7 Click the row with the logical device context that you want to update and click **View Details**.

Step 8 Click **Cluster Interface Context**.

Step 9 Click **Add**.

Step 10 On the **Create Cluster Interface Context** screen, complete the following fields:

a) Click **Select** and check the logical device context to which you want to add an interface.
b) Enter the connector name. By default, **any** is set as the connector name.
c) Click **Select** and check the logical interface name that you want to add to the logical device context.
d) Click **Select** and check the bridge domain name that you want to add to the logical device context.
e) Click **Select** and check the Layer 3 network that you want to add to the logical device context.
f) From the **L3 Destination (VIP)** drop-down list, choose an appropriate option.

- **Unspecified**—This is the default option. Choose this option to not to specify rule for Layer 3 destination.

- **True**—If the PBR policy is not configured on a specific service node, the node connector is treated as an L3 Destination and will continue to be in the new Cisco APIC version.
- **False**—Set false to enable user to choose the PBR policy for logical interface.

g) The **L4-L7 Policy Based Redirect** field appears only when **False** is selected as L3 Destination (VIP). Click **Select** and check the L4-L7 PBR that need to be associated to the interface context.
h) Click **Select** and check the custom QoS policy that need to be associated to the interface context.
i) Choose **True** from the **Permit Logging** drop-down list to enable permit logging for cluster interface context.

Step 11 Click **Submit**.

Adding a Virtual IP Address to a Cluster Interface Context

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Logical Device Context**.
Step 7 Click the row with the logical device context that you want to update and click **View Details**.
Step 8 Click **Cluster Interface Context**.
Step 9 Click the row with the cluster interface context that you want to update and click **View Details**.
Step 10 Click **Virtual IP Address**.
Step 11 Click **Add**.
Step 12 On the **Add Virtual IP Address to Logical Interface** screen, enter the IPv4 address for the logical interface.
Step 13 Click **Submit**.