Cisco APIC and Anycast Services

New and Changed Information
New and Changed Information

Table 1: New Features and Changed Behavior in Cisco APIC

<table>
<thead>
<tr>
<th>Cisco APIC Release Version</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(1x)</td>
<td>Anycast Service Support</td>
<td>Anycast services are supported in the Cisco ACI fabric. A typical use case is to support ASA firewalls in the pods of a multipod fabric, but Anycast could be used to enable other services, such as DNS servers or printing services.</td>
</tr>
</tbody>
</table>

About Anycast Services

Anycast services are supported in the Cisco ACI fabric. A typical use case is to support Cisco Adaptive Security Appliance (ASA) firewalls in the pods of a multipod fabric, but Anycast could be used to enable other services, such as DNS servers or printing services. In the ASA use case, a firewall is installed in every pod and Anycast is enabled, so the firewall can be offered as an Anycast service. One instance of a firewall going down does not affect clients, as the requests are routed to the next, nearest instance available. You install ASA firewalls in each pod, then enable Anycast and configure the IP address and MAC addresses to be used.

APIC deploys the configuration of the Anycast MAC and IP addresses to the leaf switches where the VRF is deployed or where there is a contract to allow an Anycast EPG.

Initially, each leaf switch installs the Anycast MAC and IP addresses as a proxy route to the spine switch. When the first packet from the Anycast Service is received, the destination information for the service is installed on the leaf switch behind which the service is installed. All other leaf switches continue to point to the spine proxy. When the Anycast service has been learned, located behind a leaf in a pod, COOP installs the entry on the spine switch to point to the service that is local to the pod.

When the Anycast service is running in one pod, the spine receives the route information for the Anycast service present in the pod through BGP-EVPN. If the Anycast service is already locally present, then COOP caches the Anycast service information of the remote pod. This route through the remote pod is only installed when the local instance of the service goes down.

Guidelines and Limitations for Anycast Services

Follow these guidelines and limitations when configuring and using Anycast services:

- Anycast is supported on Cisco Nexus 9000 Series switches with model numbers that end in EX, and later (for example, N9K-C93180LC-EX).
- Up to 2000 Anycast services are supported per fabric.
- A service node is used for Anycast services in the pod where the policy is applied.
- IP Aging Policy must be disabled.
- Anycast can be configured on application EPGs or through Layer 4 to Layer 7 Services (with or without Policy-Based Redirect (PBR)). For the "without PBR" use case, the traffic must be routed on ACI fabric.
Routed traffic in this case means the leaf switch routes traffic to an Anycast IP/MAC. Bridged traffic means that the switch leaf performs L2 forwarding, based on the destination MAC. For example, if the consumer endpoint and firewall with Anycast service are in the same bridge domain, and the firewall is a gateway of the consumer endpoint, it is L2 forwarding on ACI.

**Note**
You can use PBR with Anycast services starting with the Cisco APIC release 3.2(4).
- A PBR service node that is used for Anycast services must not be the consumer or provider bridge domain. The consumer and provider bridge domain can be the same.
- An inter-VRF contract can be used for a regular EPG-to-regular EPG contract, but not for an L3Out EPG contract.

Anycast services are not supported with the following features and options:
- Multi-Site management
- Remote leaf switches

To use Anycast service, you must meet the following considerations about service nodes:
- The service nodes must be connected to bridge domains, not L3Outs.
- The service nodes must act as one logical device providing the same IP/MAC and connection handling.
- The service node must not have duplicate IP detection capability.
- If the service node is a two-arm design, the service device must be able to bring down the interface if the other side is down.
- In each pod, all local service nodes (member of one service) must be connected to the same single leaf pair (vPC).
- The Anycast IP and MAC must not be an existing static endpoint.

**Note**
If you configure an Anycast MAC and IP address using the addresses for an existing static endpoint, the configuration is pushed from the APIC to the switch and no fault is generated, but the switch does not install the Anycast addresses in the hardware. Deleting the static endpoint does not resolve the problem. You must delete both the static endpoint and the Anycast configurations and reconfigure the Anycast addresses.

The following functions for traffic load-balancing to individual service nodes are not required for Anycast services:
- ECMP
- Symmetric policy-based redirect
- Pod ID Aware Redirection
- IP SLA Monitoring Policies
- Redirect Health Groups

**Configuring Anycast Services Using the GUI**

There are three ways to configure Anycast services using the Cisco APIC GUI:
• Anycast Service Behind an EPG Subnet
• Anycast Service as part of a Layer 4 to Layer 7 Service Graph with Policy-Based Redirect (PBR)
• Anycast Service as part of a Layer 4 to Layer 7 Service Graph without PBR

Before you begin

• The tenant, application profile, and application EPG have been created.
• The node group and L3Out policies have already been created.
• The Interpod Network (IPN) is already configured.
• Multipod is configured.
• In each pod, the spine switch used to connect to the IPN is also connected to at least one leaf switch.
• ASA firewalls are installed in each pod.

Procedure

Step 1
For an Anycast Service behind an application EPG subnet, perform the following steps:

a) On the menu bar, click Tenants > tenant-name.

b) Expand Application Profiles, click on the application profile for the EPG where you want to connect the Anycast service, expand Application EPGs, and expand the EPG where you want to add the Anycast service.

c) Right-click Subnets and choose Create EPG Subnet.

d) In the Default Gateway IP field, enter the Anycast IP address with a /32 or /128 netmask.

e) Under Subnet Control, enable No Default SVI Gateway.

f) In the Type Behind Subnet field, choose Anycast MAC and enter the Anycast MAC address in the MAC Address field.

g) Click Submit.

Step 2
For an Anycast Service in an L4-L7 service graph with PBR, perform the following steps:

a) Before you start, create the Service Graph Template, Layer 4 to Layer 7 device, node, and bridge domain (use the same BD as for the node). For more information about deploying Layer 4 to Layer 7 services, see Cisco APIC Layer 4 to Layer 7 Services Deployment.

b) On the menu bar, click Tenants > tenant-name.


d) Right-click L4-L7 Policy Based Redirect, choose Create L4-L7 Policy Based Redirect, and then enter the following properties.

• Enter a name for the PBR policy.

• Click the Enable Anycast check box.

  Note: Enable Pod ID Aware Redirection and IP SLA Monitoring Policy are not supported with Anycast services.

• Click the + icon on Destinations to add the Anycast IP and MAC address.

• In the IP field, enter the Anycast IP address with a /32 or /128 netmask.
• In the MAC field, enter the Anycast MAC address.

Note Redirect Health Group is not supported with Anycast services.

Step 3  For an Anycast Service in an L4-L7 service graph without PBR, perform the following steps:
   a) Before you start, create the Service Graph Template, Layer 4 to Layer 7 device, node, bridge domain, and a logical interface context with a cluster interface context. For more information about deploying Layer 4 to Layer 7 services, see Cisco APIC Layer 4 to Layer 7 Services Deployment.
   b) On the menu bar, click Tenants > tenant-name.
   c) Expand Services, L4-L7, Device Selection Policies, and the logical device context.
   d) Click the logical interface context where you want to add the Anycast service.
   e) Click the + icon to open Subnets.
   f) Enter the Anycast IP address with /32 netmask in the IP address field.
   g) Under Subnet Control, click No Default Gateway.
   h) In the Apply Policy field, click Anycast MAC and enter the Anycast MAC address.
   i) Click Submit.

Configuring Anycast Services Using the NX-OS Style CLI

These examples show how to configure Anycast services in three methods, using the NX-OS style CLI:

• Behind an EPG.
• As part of a Layer 4 to Layer 7 Service Graph with Policy Based Redirect (PBR)
• As part of a Layer 4 to Layer 7 Service Graph without PBR

Before you begin

• The tenant, application profile, and application EPG have been created.
• The node group and L3Out policies have already been created.
• The Interpod Network (IPN) is already configured.
• Multipod is configured.
• In each pod, the spine switch used to connect to the IPN is also connected to at least one leaf switch.
• ASA firewalls are installed in each pod.

Procedure

Step 1  Configure Anycast services behind an EPG subnet, using the following commands:
   a) configure
      Enters configuration mode.
      Example:
b) **tenant tenant-name**
   Creates a tenant if it does not exist or enters tenant configuration mode.
   
   **Example:**
   ```
   apic1(config)# tenant anycast1-it
   ```

c) **application app-name**
   Creates an application profile if it doesn't exist and enters application profile configuration mode.
   
   **Example:**
   ```
   apic1(config-tenant)# application AP0
   ```

d) **epg epg-name**
   Creates an EPG if it doesn't exist and enters EPG configuration mode.
   
   **Example:**
   ```
   apic1(config-tenant-app)# epg epg1
   ```

e) **endpointip ip-address anycast mac-address**
   Configures the Anycast IP address with netmask and MAC address for the Anycast service behind the EPG. The Anycast subnet must have a /32 or /128 netmask.
   
   **Example:**
   ```
   apic1(config-tenant-app-epg)# endpoint ip 1.2.3.4/32 anycast 00:11:22:33:44:55
   ```

**Step 2** Configure Anycast for Layer 4 to Layer 7 services with PBR, using the following commands:

a) **configure**
   Enters configuration mode.
   
   **Example:**
   ```
   apic1# configure
   ```

b) **tenant name**
   Creates a tenant if it does not exist or enters tenant configuration mode.
   
   **Example:**
   ```
   apic1(config)# tenant t1
   ```

c) **svcredir-pol name**
   Enters service-redirect policy mode and creates a service redirection policy.
   
   **Example:**
   ```
   apic1(config-tenant)# svcredir-pol N1Ext
   ```

d) **anycast enable**
   Enables Anycast for the service redirection policy. Use the no form of the command to disable Anycast for the policy.
   
   **Example:**
   ```
   apic1(svcredir-pol)# anycast enable
   ```

e) **redir-dest ip-addr mac-addr**
   Defines the Anycast IP and MAC addresses for the Layer 4 to Layer 7 service redirection policy.
Step 3  Configure Anycast for Layer 4 to Layer 7 services without PBR, with the following commands:

a)  configure
   Enters configuration mode.
   **Example:**
   ```
   apic1# configure
   ```

b)  tenant name
   Creates a tenant if it does not exist or enters tenant configuration mode.
   **Example:**
   ```
   apic1(config)# tenant t1
   ```

c)  l4l7 graph connector-name contract name
   Creates a Layer 4 to Layer 7 service graph associated with a contract.
   **Example:**
   ```
   apic1(config-tenant)# l4l7 graph WebGraph contract default
   ```

d)  service device-cluster-name
   Defines the service with a device cluster.
   **Example:**
   ```
   apic1(config-graph)# service N1
   ```

e)  connector name [cluster INTERFACE cluster INTERFACE name]
   Enters connector configuration mode and defines the device cluster interface.
   **Example:**
   ```
   apic1(config-service)# connector provider
   ```

f)  subnet-ip IP-addr with netmask subnet-ctrl no-default-gateway
   Defines the Anycast IP address (with /32 netmask and the subnet control, no-default-gateway). To remove it, use the no form of the command.
   **Example:**
   ```
   apic1(config-connector)# subnet-ip 50.50.50.50/32 subnet-ctrl no-default-gateway
   ```

g)  mac-address mac-address
   Defines the Anycast MAC address. To remove it, use the no form of the command.
   **Example:**
   ```
   apic1(config-subnet-ip)# mac-address 00.00.00.00.50
   ```

Example
The following example configures Anycast services behind EPG1:
The following example configures Anycast services in a Layer 4 to Layer 7 service redirection policy:

```bash
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# svcredir-pol N1Ext
apic1(svcredir-pol)# anycast enable
apic1(svcredir-pol)# redir-dest 2000::25 00:00:00:00:00:07
```

The following example configures Anycast services in a Layer 4 to Layer 7 service without PBR:

```bash
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# 1417 graph WebGraph contract default
apic1(config-graph)# service N1
apic1(config-service)# connector provider
apic1(config-connector)# subnet-ip 50.50.50.50/32 subnet-ctrl no-default-gateway
apic1(config-subnet-ip)# mac-address 00.00.00.00.00.50
```

## Configuring Anycast Services Using the REST API

These examples show how to configure Anycast services in three methods:

- Behind an EPG.
- As part of a Layer 4 to Layer 7 Service Graph with Policy Based Redirect (PBR)
- As part of a Layer 4 to Layer 7 Service Graph without PBR

### Before you begin

- The tenant, application profile, and application EPG have been created.
- The node group and L3Out policies have already been created.
- The Interpod Network (IPN) is already configured.
- Multipod is configured.
- In each pod, the spine switch used to connect to the IPN is also connected to at least one leaf switch.
- ASA firewalls are installed in each pod.

### Procedure

#### Step 1

To configure Anycast services behind an EPG, send a post with XML such as the following example:

**Example:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="tn1" status="created,modified">
    <fvAp name="a0">
      <fvAEPg name="web">
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```
Step 2

To configure Anycast services as part of a Layer 4 to Layer 7 service graph with PBR, send a post with XML such as the following example:

Example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="tn1" >
    <vnsSvcCont>
      <vnsSvcRedirectPol name="N1Ext" AnycastEnabled="yes">
        <vnsRedirectDest ip="2000::25/128" mac="00:00:00:00:00:07"/>
      </vnsSvcRedirectPol>
      <vnsSvcRedirectPol name="N1Int" AnycastEnabled="yes">
        <vnsRedirectDest ip="30.30.30.100/32" mac="00:00:00:00:00:08"/>
      </vnsSvcRedirectPol>
    </vnsSvcCont>
  </fvTenant>
</polUni>
```

Step 3

To configure Anycast services as part of a Layer 4 to Layer 7 service graph without PBR, send a post with XML such as the following example:

Example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="tn1" >
    <vnsLDevCtx ctctNameOrLbl="webCtrct" graphNameOrLbl="WebGraph" nodeOrLbl="N1">
      <vnsRsLDevCtxToLDev tDn="uni/tn-tn1/lDevVip-N1"/>
      <vnsLIfCtx connNameOrLbl="provider">
        <fvSubnet ip="50.50.50.50/32" ctrl="no-default-gateway">
          <fvEpAnycast mac="00:00:00:00:00:50"/>
        </fvSubnet>
      </vnsLIfCtx>
      <vnsLIfCtx connNameOrLbl="consumer">
        <fvSubnet ip="2000::25/128" ctrl="no-default-gateway">
          <fvEpAnycast mac="00:00:00:00:00:51"/>
        </fvSubnet>
      </vnsLIfCtx>
    </vnsLDevCtx>
  </fvTenant>
</polUni>
```
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.