Route and Subnet Scope

This chapter contains the following sections:

L3Out EPG Scope and Control Parameters

Scope and Aggregate Controls for Subnets

The following section describes some scope and aggregate options available when creating a subnet:

Export Route Control Subnet—The control advertises specific transit routes out of the fabric. This is for transit routes only, and it does not control the internal routes or default gateways that are configured on a bridge domain (BD).

Import Route Control Subnet—This control allows routes to be advertised into the fabric with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) when Import Route Control Enforcement is configured.

External Subnets for the External EPG (also called Security Import Subnet)—This option does not control the movement of routing information into or out of the fabric. If you want traffic to flow from one external EPG to another external EPG or to an internal EPG, the subnet must be marked with this control. If you do not mark the subnet with this control, then routes learned from one EPG are advertised to the other external EPG, but packets are dropped in the fabric. The drops occur because the APIC operates in a allowed list model where the default behavior is to drop all data plane traffic between EPGs, unless it is explicitly permitted by a contract. The allowed list model applies to external EPGs and application EPGs. When using security policies that have this option configured, you must configure a contract and a security prefix.

Shared Route Control Subnet—Subnets that are learned from shared L3Outs in inter-VRF leaking must be marked with this control before being advertised to other VRFs. Starting with APIC release 2.2(2e), shared L3Outs in different VRFs can communicate with each other using a contract. For more about communication between shared L3Outs in different VRFs, see the *Cisco APIC Layer 3 Networking Configuration Guide*.

Shared Security Import Subnet—This control is the same as External Subnets for the External EPG for Shared L3Out learned routes. If you want traffic to flow from one external EPG to another external EPG or to another internal EPG, the subnet must be marked with this control. If you do not mark the subnet with this control, then routes learned from one EPG are advertised to the other external EPG, but packets are dropped in the fabric.When using security policies that have this option configured, you must configure a contract and a security prefix.

Aggregate Export, Aggregate Import, and Aggregate Shared Routes—This option adds 32 in front of the 0.0.0.0/0 prefix. Currently, you can only aggregate the 0.0.0.0/0 prefix for the import/export route control subnet. If the 0.0.0.0/0 prefix is aggregated, no route control profile can be applied to the 0.0.0.0/0 network.

Aggregate Shared Route—This option is available for any prefix that is marked as Shared Route Control Subnet.

Route Control Profile—The ACI fabric also supports the route-map set clauses for the routes that are advertised into and out of the fabric. The route-map set rules are configured with the Route Control Profile policies and the Action Rule Profiles.

Security Import Policies

Static L3Out EPG

The policies discussed in the documentation have dealt with the exchange of the routing information into and out of the ACI fabric and the methods that are used to control and tag the routes. The fabric operates in a allowed list model in which the default behavior is to drop all dataplane traffic between the endpoint groups unless it is explicitly permitted by a contract. This allowed list model applies to the external EPGs and the tenant EPGs.

There are some differences in how the security policies are configured and how they are implemented for the transit traffic compared to the tenant traffic.

Transit Security Policies

- Uses prefix filtering.
- Starting with Release 2.0(1m), support for Ethertype, protocol, L4 port, and TCP flag filters is available.
- Implemented with the security import subnets (prefixes) and the contracts that are configured under the external EPG.

Tenant EPG Security Policies

- Do not use prefix filtering.
- Support Ethertype, protocol, L4 port, and TCP flag filters.
- Supported for tenant EPGs ⟷ EPGs and tenant EPGs ⟷ External EPGs.

If there are no contracts between the external prefix-based EPGs, the traffic is dropped. To allow traffic between two external EPGs, you must configure a contract and a security prefix. As only prefix filtering is supported, the default filter can be used in the contract.

External L3Out Connection Contracts

The union of prefixes for L3Out connections is programmed on all the leaf nodes where the L3Out connections are deployed. When more than two L3Out connections are deployed, the use of the aggregate rule 0.0.0.0/0 can allow traffic to flow between L3Out connections that do not have a contract.

You configure the provider and consumer contract associations and the security import subnets in the L3Out Instance Profile (instP).

When security import subnets are configured and the aggragate rule, 0.0.0.0/0, is supported, the security import subnets follow the ACL type rules. The security import subnet rule 10.0.0.0/8 matches all the addresses from 10.0.0.0 to 10.255.255.255. It is not required to configure an exact prefix match for the prefixes to be permitted by the route control subnets.

Be careful when configuring the security import subnets if more than two L3Out connections are configured in the same VRF, due to the union of the rules.

Transit traffic flowing into and out of the same L3Out is dropped by policies when configured with the 0.0.0.0/0 security import subnet. This behavior is true for dynamic or static routing. To prevent this behavior, define more specific subnets.

Dynamic L3Out EPG Classification

Prior to Cisco APIC 5.2(4) release, pcTag for external subnets was derived from external EPG's pcTag as the external subnets were configured under external EPG. When routing changed, external subnets were learned from another L3Out or external EPG. pcTag would not change with changes in routing.

Beginning in the Cisco APIC 5.2(4) release, the Dynamic L3Out EPG Classification (DEC) feature is introduced to enable dynamic changes in pcTag with routing changes.

This feature would also allow administrators to configure external EPG with route-maps by matching subnets or BGP communities. Route-map with a set external EPG configuration can be applied either on L3Out using default-import or on BGP peer by using route control profile. External EPG and contract configuration on L3Out remains same as before. Based on the route-map, a particular external EPG and associated contract is determined for prefixes.

Note External EPG selection made through route-map has precedence over the external EPG subnets configured on L3Out. For example, if route-map configuration associates 10.1.1.0/24 to *external EPG1*, and subnet *10.1.1.0/24* is configured on *external EPG2*, then *external EPG1* will be programmed in hardware for *10.1.1.0/24* because external EPG determination through route-map is preferred.

Guidelines and Limitations for DEC

- This feature supports only BGP and OSPF.
- DEC is only supported with L3Out default-import route-maps or BGP peer import route-maps.
- To enable shared security, configure external EPGs with the shared security flags and subnets that you want to share.
- DEC does not support the following features:
  - Intersite
  - Integration with a floating L3Out
  - Static routing
  - EIGRP
  - Segment routing
  - AM

- BGP next-hop propagation with floating L3Out
- Cisco ACI GOLF, SR-MPLS, and coexistence with a fallback route

Configuring Dynamic L3Out EPG Classification Using GUI

This procedure configures the dynamic L3Out EPG classification (DEC), and assumes that you have configured the Layer 3 outside network connections using BGP. You can also perform these tasks for an L3Out configured using OSPF.

This task lists steps to create import and export policies. By default, import controls are not enforced, so you must manually assign the import control.

Before you begin

- The tenant, private network, and bridge domain are created.
- The Layer 3 outside for tenant networks is created.

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, choose ***tenant_name*** > **Networking** > **L3Outs** > ***l3out_name***.

Step 4 Right click *l3out_name* and click **Create Route map for import and export route control**.

Step 5 In the **Create Route map for import and export route control** dialog box, perform the following actions:

a) From the **Name** field drop-down list, choose **default-import**.
Depending on your selection, whatever is advertised on the specific L3Out is automatically used.
b) In the **Type** field, choose **Match Prefix AND Routing Policy**.
c) In the **Contexts** area, click **+** to open the **Create Route Control Context** dialog.

Step 6 In the **Create Route Control Context** dialog box, perform the following actions:

a) In the **Order** field, enter the desired order number.
b) In the **Name** field, enter a name for the route control private network.
c) In the **Associated Matched Rules** table, click **+**.
d) From the **Rule Name** drop-down list, choose **Create Match Rule for a Route Map**.
e) In the **Create Match Rule for a Route Map** dialog box, in the **Name** field, enter a route match rule name.
f) Specify the match community regular expression term and match community terms as desired.

Match community factors will require you to specify the name, community, and scope.

g) Click **Submit**.
h) From the **Set Rule** drop-down list, choose **Create Set Rules for a Route Map**.
i) In the **Create Set Rules for a Route Map** dialog box, in the **Name** field, enter a name for the rule.
j) Put a check in the **Set External EPG** check box, choose an EPG in the **External EPG** drop-down list, and click **Finish**.
The policy is created and associated with the action rule.
k) In the **Create Route Control Context** window, click **OK**.

l) In the **Create Route map for import and export route control** dialog box, click **Submit**.

Step 7 In the **Work** pane, choose the **Policy** > **Main** tabs.
In the **Work** pane, the **Properties** are displayed.

Step 8 (Optional) Next to **Route Control Enforcement**, put a check in the **Import** check box to enable the import policy, then click **Submit**.

The import control policy is disabled by default. The import control policy is supported for BGP and OSPF, but not for EIGRP. If the you enable the import control policy for an unsupported protocol, the protocol will be automatically ignored. The export control policy is supported for BGP, EIGRP, and OSPF. Also, you need not put a check in the **Import** check box for the import policy when you configure BGP per neighbor import route-map.

Note If BGP is established over OSPF, then the import control policy is applied only for BGP and ignored for OSPF.

Step 9 To create a customized export policy, in the **Navigation** pane, right-click **Route map for import and export route control**, choose **Create Route map for import and export route control**, and perform the following actions:

a) In the **Create Route map for import and export route control** dialog box, from the **Name** drop-down list, choose or enter a name for the export policy.
b) In the **Contexts** table, click **+** to open the **Create Route Control Context** dialog.
c) In the **Create Route Control Context** dialog box, in the **Order** field, enter a value.
d) In the **Name** field, enter a name for the route control private network.
e) (Optional) From the **Associated Match Rules** table, click **+**, choose **Create Match Rule For a Route Map** from the **Rule Name** drop-down list, fill out the fields as desired, and click **Submit**.
f) From the **Set Rule** drop-down list, choose **Create Set Rules For a Route Map**.

Alternatively, you can choose an existing set rule.

g) If you chose **Create Set Rules For a Route Map**, in the **Create Set Rules For A Route Map** dialog box, enter a name for the set rules in the **Name** field, put a check in the box for the rules you want to set, enter the appropriate values for the rules, then click **Finish**.
In the **Create Route Control Context** dialog box, the policy is created and associated with the action rule.
h) Click **OK**.
i) In the **Create Route map for import and export route control** dialog box, click **Submit**.

In the **Work** pane, the export policy is displayed.

Note To enable the export policy, it must first be applied. For the purpose of this example, the policy is applied to all the subnets under the network.

Step 10 In the **Navigation** pane, expand ***tenant_name*** > **Networking** > **L3Outs** > ***L3Out_name*** > **External EPGs** > ***external_EPG_name*** , and perform the following actions:

a) In the **Route Control Profile** table, click **+**.
b) In the **Name** drop-down list, choose the policy that you created earlier.
c) In the **Direction** drop-down list, choose **Route Export Policy**.
d) Click **Update**.
e) Click **Submit**.