Nexus Dashboard Orchestrator DHCP Relay for ACI Fabrics, Release 4.3.x

Table of Contents

DHCP Relay Policy

Typically, when your DHCP server is located under an EPG, all the endpoints in that EPG have access to it and can obtain the IP addresses via DHCP. However, in many deployment scenarios, the DHCP server may not exist in the same EPG, BD, or VRF as all the clients that require it. In these cases a DHCP relay can be configured to allow endpoints in one EPG to obtain IP addresses via DHCP from a server that is located in another EPG/BD deployed in a different site or even connected externally to the fabric and reachable via an L3Out connection.

You can create the DHCP Relay policy in the Orchestrator GUI to configure the relay. Additionally, you can choose to create a DHCP Option policy to configure additional options you can use with the relay policy to provide specific configuration details. For all available DHCP options, refer to RFC 2132.

When creating a DHCP relay policy, you specify an EPG (for example, epg1) or external EPG (for example, ext-epg1) where the DHCP server resides. After you create the DHCP policy, you associate it with a bridge domain, which in turn is associated with another EPG (for example, epg2) allowing the endpoints in that EPG to reach the DHCP server. Finally, you create a contract between the relay EPG (epg1 or ext-epg1) and application EPG (epg2) to allow communication. The DHCP policies you create are pushed to the APIC when the bridge domain to which the policy is associated is deployed to a site.

Guidelines and Limitations

The DHCP relay policies are supported with the following caveats:

- DHCP relay policies are supported for fabrics running Cisco APIC Release 4.2(1) or later.
- The DHCP servers must support DHCP Relay Agent Information Option (Option 82).

  When an ACI fabric acts as a DHCP relay, it inserts the DHCP Relay Agent Information Option in DHCP requests that it proxies on behalf of clients. If a response (DHCP offer) comes back from a DHCP server without Option 82, it is silently dropped by the fabric.

- DHCP relay policies are supported in user tenants or the common tenant only. DHCP policies are not supported for the infra or mgmt tenants.

  When configuring shared resources and services in the ACI fabric, we recommend creating those resources in the common tenant, that way they can be used by any user tenant.

- DHCP relay server must be in the same user tenant as the DHCP clients or in the common tenant.

  The server and the clients cannot be in different user tenants.

- DHCP relay policies can be configured for the primary SVI interface only.
  If the bridge domain to which you assign a relay policy contains multiple subnets, the first subnet you add becomes the primary IP address on the SVI interface, while additional subnets are configured as secondary IP addresses. In certain scenarios, such as importing a configuration with a bridge domain with multiple subnets, the primary address on the SVI may change to one of the secondary addresses, which would break the DHCP relay for that bridge domain.
  You can use the show ip interface vrf all command to verify IP address assignments for the SVI interfaces.
- If you make changes to the DHCP policy after you have assigned it to a bridge domain and deployed the bridge domain to one or more sites, you will need to re-deploy the bridge domain for the DHCP policy changes to be updated on each site's APIC.
- For inter-VRF DHCP relay with the DHCP server reachable via an L3Out, DHCP relay packets must use site-local L3Out to reach the DHCP server. Packets using an L3Out in a different site (Intersite L3Out) to reach the DHCP server is not supported.
- The following DHCP relay configurations are not supported:
  - DHCP relay label on L3Out interfaces
  - Importing existing DHCP policies from APIC.
  - DHCP relay policy configuration in Global Fabric Access Policies is not supported
  - Multiple DHCP servers within the same DHCP relay policy and EPG.

    If you configure multiple providers under the same DHCP relay policy, they must be in different EPGs or external EPGs.

- For a bridge domain with tenant-scoped labels, when associating the DHCP relay policy with the bridge domain, you must follow these steps in this order for the DHCP labels to be imported correctly:

  1. Import the DHCP relay and DHCP option policies into the tenant policy template.

2. Import the EPG in the application template.

If the EPG is using the same bridge domain, importing the EPG using this process also imports the bridge domain, as well as the relation to the DHCP label.

Creating DHCP Relay Policies

Before you begin:

You must have the following:

- A DHCP server set up and configured in your environment.
- If the DHCP server is part of an application EPG, that EPG must be already created in the Cisco Nexus Dashboard Orchestrator.
- If the DHCP server is external to the fabric, the external EPG associated to the L3Out that is used to access the DHCP server must be already created.

This section describes how to create a DHCP relay policy.

If you make changes to the DHCP policy after you have assigned it to a bridge domain and deployed the bridge domain to one or more sites, you must redeploy the bridge domain for the DHCP policy changes to update on each site's APIC.

1. Log in to your Cisco Nexus Dashboard and open the Cisco Nexus Dashboard Orchestrator service.
2. Create a new Tenant Policy.
   a. From the left navigation pane, choose **Config > Tenant Policies**.
   b. On the **Tenant Templates > Tenant Policies** page, click **Add Tenant Policy Template**.
   c. In the Tenant Policies page's right properties sidebar, provide the **Name** for the tenant.
   d. From the **Select a Tenant** drop-down, choose the tenant with which you want to associate this template.

      All the policies that you create int his template as described in the following steps will be associated with the selected tenant and deployed to it when you push the template to a specific site.
3. Create a DHCP Relay Policy.
   a. From the **+Create Object** drop-down, select **DHCP Relay Policy**.
   b. In the right properties sidebar, provide the **Name** for the policy.
   c. (Optional) Click **Add Description** and provide a description for the policy.
   d. Click **Add Provider** to configure the DHCP server to which you want to relay the DHCP requests originated by the endpoints.
   e. Select the provider type. When adding a relay policy, you can choose one of the following two types:
      - Application EPG – Specifies the application EPG that includes the DHCP server to which you want to relay the DHCP requests.
      - L3 External Network – Specifies the External EPG associated to the L3Out that is used to access the network external to the fabric where the DHCP server is connected.

You can select any EPG or external EPG that has been created in the Orchestrator and assigned to the tenant you specified, even if you have

not yet deployed it to sites. If you select an EPG that hasn't been deployed, you can still complete the DHCP relay configuration, but you need to deploy the EPG before the relay is available for use.

f. Click **Select an Application EPG** or **Select an External EPG** (based on the provider type you selected) and choose the provider EPG.

g. In the **DHCP Server Address** field, provide the IP address of the DHCP server.

h. Enable the **DHCP Server VRF Preference** option if necessary.
This feature was introduced in Cisco APIC release 5.2(4). For more information on the use cases where it is required see Cisco APIC Basic Configuration Guide.

i. Click **OK** to save the provider information.

j. Repeat the previous substeps for any additional providers in the same DHCP Relay policy.

k. Repeat this step to create any additional DHCP Relay policies.

Creating DHCP Option Policies

Before you begin:

You must have the following already configured:

- A DHCP server set up and configured in your environment.
- An EPG that contains the DHCP server that is already created in the Cisco Nexus Dashboard Orchestrator.
- A DHCP Relay policy created, as described in Creating DHCP Relay Policies.

This section describes how to create a DHCP option policy. DHCP options are appended to the end of the messages that DHCP servers and clients Exchange and can be used to provide extra configuration information to your DHCP server. Each DHCP option has a specific code that you must provide when adding the option policy. For a complete list of DHCP options and codes, see RFC 2132.

1. Log in to your Cisco Nexus Dashboard and open the Cisco Nexus Dashboard Orchestrator service.
2. Create a new or update an existing Tenant Policy.
   a. From the left navigation pane, choose **Configure > Tenant Templates > Tenant Policies**.
   b. On the **Tenant Policy Templates** page, select an existing policy or click **Add Tenant Policy Template**.
   c. If creating a new policy, in the Tenant Policies page's right properties sidebar, provide the **Name** for the tenant.
   d. If creating a new policy, from the **Select a Tenant** drop-down, choose the tenant with which you want to associate this template.

      All the policies that you create int his template as described in the following steps will be associated with the selected tenant and deployed to it when you push the template to a specific site.
3. Create a DHCP Option Policy.
   a. From the **+Create Object** drop-down, select **DHCP Option Policy**.
   b. In the right properties sidebar, provide the **Name** for the policy.
   c. (Optional) Click **Add Description** and provide a description for the policy.
   d. Click **Add Option**.
   e. Provide option details.
      For each DHCP option, provide the following:
      - **Name** - While not technically required, we recommend using the same name for the option as listed in RFC 2132.
        For example, Name Server.
      - **Id** - Provide the value if the option requires one.
        For example, a list of name servers available to the client for the Name Server option.
      - **Data** - Provide the value if the option requires one.
        For example, a list of name servers available to the client for the Name Server option.

f. Click **OK** to save.

g. Repeat the previous substeps for any additional options in the same DHCP Option policy.

h. Repeat this step to create any additional DHCP Option policies.

Assigning DHCP Policies

Before you begin:

You must have the following already configured:

- A DHCP relay policy, as described in Creating DHCP Relay Policies.
- (Optional) A DHCP option policy, as described in Creating DHCP Option Policies.
- The bridge domain to which you assign the DHCP policy, as described in the Creating Schemas and Templates chapter.

This section describes how to assign a DHCP policy to a bridge domain.

If you make changes to the DHCP policy after you have assigned it to a bridge domain and deployed the bridge domain to one or more sites, you must redeploy the bridge domain it for the DHCP policy changes to be updated on each site's APIC.

1. Log in to your Cisco Nexus Dashboard Orchestrator GUI.
2. From the left navigation menu, select **Configure > Schemas**.
3. Select the schema where the bridge domain is defined.
4. Scroll down to the **Bridge Domain** area and select the bridge domain.
5. In the right sidebar, scroll down and check the **DHCP Policy** option check box.
6. From the **DHCP Relay Policy** drop-down, select the DHCP policy that you want to assign to this BD.
7. (Optional) From the **DHCP Option Policy** drop-down, select the option policy.

   A DHCP option policy provides extra options to be passed to the DHCP relay. For extra details, see Creating DHCP Option Policies.
8. Assign the bridge domain to any EPG that needs access to the DHCP server through the relay.

Creating DHCP Relay Contract

Before you begin:

You must have the following already configured:

- A DHCP relay policy, as described in Creating DHCP Relay Policies.
- (Optional) A DHCP option policy, as described in Creating DHCP Option Policies.
- The bridge domain to which you have assigned the DHCP policy, as described in Assigning DHCP Policies.

DHCP packets are not filtered by contracts but contracts are required often to propagate routing information within the VRF and across VRFs. Although the DHCP packets are not filtered, it is recommended to configure contracts between the client EPG and the EPG configured as the provider in the DHCP relay policy.

This section describes how to create a contract between the EPG that contains the DHCP server and the EPG that contains endpoints that must use the relay. Although you have already created and assigned the DHCP policy to the bridge domain and the bridge domain to the clients' EPG, you must create and assign the contract to enable programming of routes to allow client to server communication.

1. Log in to your Cisco Nexus Dashboard Orchestrator GUI.
2. From the left navigation menu, select **Configure > Schemas**.
3. Select the schema where you want to create the contract.
4. Create a contract.

   DHCP packets are not filtered by the contract so no specific filter is required, but a valid contract should be created and assigned to ensure proper BD and routes deployment.

   a. Scroll down to the **Contracts** area and click **+** to create a contract.
   b. In the right sidebar, provide the **Display Name** for the contract.
   c. From the **Scope** drop-down, select the appropriate scope.

      Because the DHCP server EPG and application EPG must be in the same tenant, you can select one of the following:

      - vrf, if both EPGs are in the same VRF.
      - tenant, if the EPGs are in different VRFs.

   d. You can leave the **Apply Both Directions** knob on.
5. Assign the contract to the DHCP relay EPG.
   a. Browse to the template where the EPG is located.
   b. Select the EPG or external EPG where the DHCP server resides.

      This is the same EPG that you selected when creating the DHCP relay policy.

   c. In the right sidebar, click **+Contract**.

d. Select the contract that you created and provider for its type.

6. Assign the contract to the application EPG whose endpoints require DHCP relay access.
   a. Browse to the template where the application EPG is located.
   b. Select the application EPG.
   c. In the right sidebar, click **+Contract**.
   d. Select the contract that you created and consumer for its type.

Verifying DHCP Relay Policies in APIC

This section describes how to verify that the DHCP relay policies you have created and deployed using the Nexus Dashboard Orchestrator are correctly pushed to each site's APIC. The DHCP policies you create are pushed to the APIC when the bridge domain to which the policy is associated is deployed to a site.

1. Log in to the site's APIC GUI.
2. From the top navigation bar, select **Tenants > <tenant-name>**.

   Select the tenant where you deployed the DHCP policy.

3. Verify that the DHCP relay policy is configured in APIC.

   In the left tree view, navigate to **<tenant-name> > Policies > Protocol > DHCP > Relay Policies**. Then confirm that the DHCP relay policy you configured has been created.

4. Verify that the DHCP option policy is configured in APIC.

   If you have not configured any DHCP option policies, you can skip this step.

   In the left tree view, navigate to **<tenant-name> > Policies > Protocol > DHCP > Option Policies**. Then confirm that the DHCP option policy you configured has been created.

5. Verify that the DHCP policy is correctly associated with the bridge domain.

   In the left tree view, navigate to **<tenant-name> > Networking > Bridge Domains > <bridge-domain-name> > DHCP Relay Labels**. Verify that the DHCP policy is also associated with the deployed bridge domain.

Editing or Deleting Existing DHCP Policies

This section describes how to edit or delete a DHCP relay or option policy.

NOTE:

- If you make changes to the DHCP policy after you have assigned it to a bridge domain and deployed the bridge domain to one or more sites, you will need to re-deploy it for the DHCP policy changes to update on each site's APIC.
- You cannot deleted policies that are associated with one or more bridge domains, you must first unassign the policy from every bridge domain.

1. Log in to your Nexus Dashboard Orchestrator GUI.
2. From the left navigation menu, select **Config > Tenant Templates > Tenant Policies**.
3. Click the actions menu next to the DHCP policy and select **Edit** or **Delete**.

First Published: 2024-03-01
Last Modified: 2024-03-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883