Creating and Managing Admin Domains

This chapter has the following sections:

Admin Domain Overview

The Admin Domain feature enables you to partition the data center and define data center pods to group hardware and software VTEPs, Layer 3 gateways, and DCI gateways into administrative domains with similar properties. Admin Domains are independent of each other. You can create an admin domain, and specify certain functional roles within the admin domain. Admin domains are logical groups you create, based on the functional roles, which makes centralized L3 or Distributed L2/L3 deployments flexible and extendable.

Cisco VTS provides the functional roles, which you can use as desired to create the admin domains. You can set the system mode, control protocols, other parameters like replication mode (multicast/ingress), for each admin domain , and also assign devices to each of the functional roles. For example, you can pick certain leafs and put it in one group, and associate certain functional parameters to that group. The following functional roles are available:

- L2 Gateway
- L3 Gateway
- DC Gateway
- DCI
- Route Reflector Functional Group

For the L2 Gateway group you can pick the desired leafs and associate certain functional parameters to that group. Similarly, you can define another L3 gateway group, and you can link between these two groups. All L2 configuration can be pushed into the L2 gateway group; and all L3 configuration can be pushed into L3 gateway group.

You can create an L3 gateway group and can link from the L3 group to the DC gateway. You can have the DCI at the top, and this can be linked to the DC gateway.

The DC gateway can be outside the Admin Domain, and more than one Admin Domains may connect to this. You can have the DC gateway inside an Admin Domain, and connect it to an external DCI.

See for detailed information about creating Admin Domains.

The design validated in this release has:

- L2/L3 gateway groups in all Admin Domain-Each Admin Domain can have its own L2 / L3 gateway.
- DC Gateway outside the Admin Domain
- DCI outside the Admin Domain.

Viewing Admin Domain

The **Admin Domains** home page lists all the Admin Domains that you have created. It provides the option to create a new Admin Domain.

It also displays the status of the Admin Domains. You can also edit an Admin Domain.

To view admin domains:

Step 1 Go to **Admin Domains** > **Domains**.

The Admin Domains / Domains window appears.

You can see two types of views on the Admin Domain page. The two types of views are as follows:

- List view
- Tree view

Step 2 To view the details of an Admin Domain, click the desired admin domain.

You can create an Admin Domain from the table. To do this, click the **Add (+)** icon in the table, and provide the required details. You can also edit or delete an Admin Domain.

Creating an Admin Domain

To create an admin domain:

Before you begin

Ensure that you have:

- Created authorization groups populated with the correct credentials.
- Discovered the topology and imported the CSV file (after assigning / reviewing device roles). See Performing Auto Discovery and Managing Inventory sections for details.
- Reviewed the Supported Platforms section in the *Cisco Virtual Topology System Installation Guide,* which provide information about the platforms that Cisco VTS support, and their roles.

Step 1 Go to **Admin Domains** > **Domains**.

The Admin Domains / Admins window appears.

Step 2 Click **Create (+)**.

The Create New Admin Domain popup window appears.

Step 3 Enter the name and description in the **Create New Admin Domain** popup window.

Step 4 Click **Create**.

The Admin Domain canvas appears.

You can see the following functional groups on the left-hand side of the canvas:

	Functional Group	Description
1	DCI	DCI is an external gateway.
2	DC GW	DC GW is a border leaf. **Note** If it is a DCI mode, then you need to add DCI device to both the DC GW and DCI. In an integrated mode, we need to add DCI to both DC GW functional group and DCI functional group.
3	L3 GW	A group of all L3 devices that can be within an admin domain and that particular device share a particular property or same functionalities. **Note** An admin can create a logical L3 groups and map devices that will exhibit a similar policy behavior under this group.
4	L2 GW	A group of all L2 devices that can be within an admin domain and that particular device share a particular property or same functionalities. **Note** An admin can create a logical L2 groups and map devices that will exhibit a similar policy behavior under this group.

Step 5 Click the functional group. The functional group icon appears on the canvas. You need to drag and drop the functional group and assign properties to them.

Functional Group	Property

DCI	Specify:
	• Whether it is a New or Shared DCI.
	• The Redundancy / Availability settings:
	  • Enable/Disable Redundancy using the toggle switch.
	  • ICCP—VXLAN/fabric ICCP group number. Valid range is 1 to 4294967295. MPLS/core ICCP group number. Valid range is 1 to 4294967295
	  • ESI—Ethernet Segment ID for NVE overlay. Valid entry is a nine octet string. Each octet can contain one or two numbers in the range 0 to F.
	
	Click Stitching Profile and choose the required profile.

DC GW	Specify: • Whether it is a New or Shared DC GW. • The Control Protocol—BGP EVPN.

Functional Group	Property
L3 GW	Specify: • Whether it is a New and Shared L3 GW. • The Control Protocol—BGP EVPN. • The Replication Mode—Multicast or Ingress. This is the data plane replication mode that will be used for VXLAN data plane traffic. The admin domain can contain devices that support common replication mode. **Note** • Cisco Nexus 5600 and Cisco Nexus 7000 supports Multicast replication mode only. • VTF supports Ingress mode only. • Cisco Nexus 9000 supports both modes. • Distribution Mode—Decentralized. **Note** L3 GW group is created as Decentralized when the L2/L3 VXLAN are terminated on the same leaf. Therefore, if you have multiple L2 VXLAN and you want to connect them together using an L3 VXLAN, you need to create a decentralized L3 GW group and add all the L2GW group devices to this L3GW group, and connect the L2 GW and L3 GW group together. An L3 GW group can be created as a Decentralized Gateway group when the L3 GW groups are distributed between multiple L2 GW group within an Admin Domain.
L2 GW	Specify: • Whether it is a New and Shared L2 GW. • The Control Protocol—BGP EVPN. • The Replication Mode—Multicast or Ingress. • The Distribution Mode—Decentralized.

Step 6 Assign Devices for each functional group.

Note If you had created a device group (under **Resource Pools > VLAN Pool**), the device group information does not get displayed in the device list for DCI and DC GW functional groups, while you create an admin domain. However, the device group gets displayed in the device list for L3 GW and L2 GW functional group.

For devices that have no Loopback Interface Numbers/Loopback IP/BGP-ASN Number, you can find a warning icon adjacent to device name. You must update these values in Network Inventory, if these devices need to be a part of the admin domain.

Click the drop-down icon on the right-hand side to see how many devices are placed in this group or how many devices are available to be placed in this group. The **All** option shows both placed devices and available devices.

For more information about supported devices, see the Supported Platforms section in the *Cisco Virtual Topology System Installation Guide*.

Step 7 Link the functional groups based on your requirement. You can click a functional group and drag the mouse pointer to the functional group you want to connect to, to form a link.

Note For L2VNI, you can extend the connection from L2 gateway to DC gateway by connecting them. To remove the link, click on the link that needs to be removed and click on Remove Link in the popup box. Click **Yes** in the confirmation box to remove the link. See Extending Layer 2 Network Across Data Centers for details.

While creating admin domain with large number of devices per L2GWgroup or L3GWGroup, user must add devices in smaller batches. Note that locally we have tried batch of 40 devices and the admin domain creation gets completed within 11 minutes.

Step 8 Click **Save** to save the new Admin Domain with all the nodes, properties, and links.

Click **Cancel** icon if you want to go back to the main menu.

Note When we add DCI and DCGW without connectivity to L3GW & L2GW and save Admin Domain, upon deletion of DCI/DCGW from UI does not delete from NCS_CLI.

Creating DCI Interconnect Profiles

The DCI Interconnect Profiles page lets you create DCI interconnect profiles. These profiles enables services like route leaking to internet, and L2 VNI extension.

To create a DCI Interconnect Profile:

Step 1 Go to **Admin Domains** > **DCI Interconnect Profiles**. The DCI Interconnect Profiles page appears.

Step 2 Click the **Add (+)** button. In the Create Profile page, enter the DCI Interconnect Profile properties:

- Name—The profile name. This is mandatory.
- Description
- Control Plane Protocol—Specify the control plane protocol. It is BGP by default.

Step 3 Choose the interconnect type. You may choose one or both of the following interconnect types:

- Internet—IPv4 unicast and IPv6 unicast address families are added.
- MPLS L2 VPN—L2VPN EVPN address family are added.

Enter the following for the interconnect type you choose. This is optional:

- Fabric Facing Route Policy Route Map—Route filter to apply for fabric facing routes. Maximum length is 64 characters.
- Core Facing Route Policy Route Map—Route filter to apply for core facing routes. Maximum length is 64 characters.

Step 4 Click **Remote Neighbors Settings**, and enter the following:

- AS Number—Enter a natural number between 1 and 65000.
- Loopback Interface Number—Loopback interface which connect to the remote neighbor. Enter an integer. Range is 0 to 2147483647.

Step 5 Click the **Add (+)** button to add remote neighbors.

You may add one or more remote neighbors. Use the **Add (+)** button to add more remote neighbors. The IP address can be IPv4 or IPv6.

Step 6 Click **Save Profile**.