CONTENTS

CHAPTER 1

Introduction 1
  Understanding Cisco VTS 1
  Cisco VTS Architecture Overview 2
  Cisco Virtual Topology Forwarder 3
  Virtual Topology System High Availability 3

CHAPTER 2

Getting Started with Cisco Virtual Topology System 5
  Logging in 5
  Using the Setup Wizard 6
    System Settings 6
    Virtual Machine Manager 7
  Authorization Group 8
  Discovery 8
  Inventory 9
  Using the Expert Mode—Quick Guide 10
  Initial Configuration Tasks 11
  Important Notes Regarding VMware vSphere Distributed Switch (VDS) 15
    For Non-VPC Specific Configuration 15
    For VPC Specific Configuration 16

CHAPTER 3

Managing Users and Groups 17
  Creating Users 17

CHAPTER 4

Managing Inventory 19
  Creating Authorization Groups 19
  Performing Auto Discovery 20
  Importing Inventory using CSV File 21
  Viewing the Network Topology 23
Contents

Viewing Network Inventory 23
Adding Fabric Connection 24
Synchronizing Configuration 25
Viewing Host Inventory 25
Installing OpenStack Host Agent and VTF using GUI 26
Viewing the IOS XRv to VTF Mapping 27
Migrating from vPC to ESI 28
Redeploying Device Inventory 30

CHAPTER 5
Managing Resource Pools 31
Specifying Global VNI Pool Range 31
Specifying VLAN Pool Range 32
Specifying Device VLAN Pool Range 32
Specifying Group VLAN Pool Range 33
Specifying Multicast IP Pool 33

CHAPTER 6
Creating and Managing Admin Domains 35
Admin Domain Overview 35
Viewing Admin Domain 36
Creating an Admin Domain 36

CHAPTER 7
Managing Templates 41
Creating Route Templates 42
Adding Static Routes 42
Adding Route Targets 43
Disabling Auto Route Target Configuration 44
Creating L3 Extension Templates 45
Editing Templates 46
Copying a Template 46
Deleting Templates 46
Attaching Templates to Tenants 47
Attaching Template while Adding Tenants 47
Attaching Template while Editing a Tenant 47
Detaching Template from Tenants 48
Attaching Templates to Routers 48
Introduction

This chapter provides an overview of Cisco Virtual Topology System (VTS). It has the following sections:

- Understanding Cisco VTS, page 1
- Cisco VTS Architecture Overview, page 2
- Cisco Virtual Topology Forwarder, page 3
- Virtual Topology System High Availability, page 3

Understanding Cisco VTS

The Cisco Virtual Topology System (VTS) is a standards-based, open, overlay management and provisioning system for data center networks. It automates DC overlay fabric provisioning for both physical and virtual workloads.

Cisco VTS provides a network virtualization architecture and software-defined networking (SDN) framework that meets the requirements of multitenant data centers for cloud services. It enables a policy-based approach for overlay provisioning.

Cisco VTS automates complex network overlay provisioning and management tasks through integration with cloud orchestration systems such as OpenStack and VMware vCenter and abstracts out the complexity involved in managing heterogeneous network environments. The solution can be managed from the embedded Cisco VTS GUI or entirely by a set of northbound Representational State Transfer (REST) APIs that can be consumed by orchestration and cloud management systems.

Cisco VTS provides:

- Fabric automation
- Programmability
- Open, scalable, standards based solution
- Cisco Nexus 5000, 7000, and 9000 Series Switches. For more information, see Supported Platforms in Cisco VTS 2.2 Installation Guide.
- Software forwarder (Virtual Topology Forwarder [VTF])
Cisco VTS Architecture Overview

Cisco VTS architecture has two main components: the Policy Plane and the Control Plane. These perform core functions such as SDN control, resource allocation, and core management function.

Figure 1: Cisco VTS Architecture

- **Policy Plane:** The policy plane enables Cisco VTS to implement a declarative policy model designed to capture user intent and render it into specific device-level constructs. The solution exposes a set of modular policy constructs that can be flexibly organized into user-defined services for use cases across service provider and cloud environments. These policy constructs are exposed through a set of REST APIs that can be consumed by orchestrators and applications to express user intent, or instantiated through the Cisco VTS GUI. Policy models are exposed as system policies or service policies.

  System policies allow administrators to logically group devices into pods within or across data centers to define Admin Domains with common system parameters (for example, BGP-EVPN control plane with distributed Layer 2 and 3 gateways).

  The inventory module maintains a database of the available physical entities (for example, data center interconnect [DCI] routers and top-of-rack leaf, spine, and border-leaf switches) and virtual entities (for example, VIFs) in the Virtual Topology System domain. The database also includes interconnections between these entities and details about all services instantiated within a Virtual Topology System domain.
The resource management module manages all available resource pools in the Virtual Topology System domain, including VLANs, VXLAN Network Identifiers (VNIs), IP addresses, and multicast groups.

- **Control Plane**: The control plane module serves as the SDN control subsystem that programs the various data planes including the VTFs residing on the x86 servers, hardware leafs, DCI gateways. The control plane hosts the Cisco IOS XRv Software instance that provides route peering capabilities between the DCI gateways or to a BGP route reflector. Cisco IOS XRv is the virtualized version of Cisco IOS XR Software. The control plane enables an MP-BGP EVPN-based control plane for VXLAN overlays originating from leafs or software VXLAN tunnel endpoints (VTEPs).

The device management module enables device configuration and management capabilities within Virtual Topology System, with multiprotocol support to support a multivendor environment.

**Cisco Virtual Topology Forwarder**

Cisco VTS solution provides a l2/l3 software switch that can act as a software VTEP and is called Virtual Topology forwarder (VTF). Cisco VTS can be deployed with a Virtual Topology Forwarder (VTF). VTF is a lightweight, multitenant software data plane designed for high performance packet processing on x86 servers. VTF uses Vector Packet Processing (VPP). VPP is a full-featured networking stack with a software forwarding engine. VTF leverages VPP technology and Intel Data Path Development Kit (DPDK) for high performance Layer 2 (L2), Layer 3 (L3), and VXLAN packet forwarding.

VTF allows Cisco VTS to terminate VXLAN tunnels on host servers by using the VTF as a Software VXLAN Tunnel Endpoint (VTEP). Cisco VTS also supports hybrid overlays by stitching together physical and virtual endpoints into a single VXLAN segment.

VTF is deployed as a virtual machine to deliver a high-performance software data plane on a host server.

**Virtual Topology System High Availability**

The Virtual Topology System solution is designed to support redundancy, with two solution instances running on separate hosts in an active-standby configuration.

During initial setup, each instance is configured with both an underlay IP address and a virtual IP address. Virtual Router Redundancy Protocol (VRRP) is used between the instances to determine which instance is active.

The active-instance data is synchronized with the standby instance after each transaction to help ensure consistency of the control-plane information to accelerate failover after a failure. BGP peering is established from both Virtual Topology System instances for the distribution of tenant-specific routes. During the switchover, nonstop forwarding (NSF) and graceful restart help ensure that services are not disrupted.

See the Configuring High Availability section of the Cisco VTS 2.2 Installation Guide for the detailed procedure about setting up high availability.
CHAPTER 2

Getting Started with Cisco Virtual Topology System

This chapter provides an overview of Cisco Virtual Topology System (VTS). It also provides a high level workflow of the tasks that you need to perform after you install Cisco VTS.

- Logging in, page 5
- Using the Setup Wizard, page 6
- Using the Expert Mode—Quick Guide, page 10
- Initial Configuration Tasks, page 11
- Important Notes Regarding VMware vSphere Distributed Switch (VDS), page 15

Logging in

To log in to the Cisco VTS GUI:

Step 1 Open a supported browser, and enter the URL of the server. For example: http://<IP Address>. Cisco VTS supports Google Chrome and Mozilla Firefox browsers. Cisco VTS has been tested on Google Chrome version 49.0.2623.112 m and Mozilla Firefox version 45.0.1.

Step 2 Enter the username and passphrase, and click Login. The default username and passphrase is admin/admin. You will be required to change the passphrase for the admin account the first time you are logging in. Click the Passphrase guidelines link for details about the passphrase guidelines.

Step 3 Enter the New Passphrase, and reenter the new passphrase in the Confirm New Passphrase field.

Step 4 Click Change Passphrase.

Note To change your passphrase subsequently, click Change Passphrase on the top right settings button.

The Cisco VTS welcome screen is displayed. The screen provides two options for you to continue with the set up tasks:
• Guide me to set up—This option takes you to the Cisco VTS Setup Wizard. This wizard guides you through the initial configuration tasks to get your system ready for further operations.

• I will set up myself—This option takes you to the Quick Guide, which displays the tasks you need to complete in order to get started with the system.

If you are familiar with the Cisco VTS setup tasks, you may opt to close the Quick Guide and proceed with the tasks. You can access the Quick Guide anytime from the Settings menu on the top right corner of the Cisco VTS GUI.

---

**Using the Setup Wizard**

The Cisco VTS Setup wizard guides you through a series of steps that helps you set up the system and get started. We recommend that you use the Setup wizard if you are not familiar with the VTS UI and the sequence of the initial configuration tasks.

**Note**

Not all steps in the wizard are mandatory. Green check mark indicates that the task is not mandatory. These tasks can be done outside of the wizard flow or have default values.

The following sections provide information about the series of screens that are part of the wizard.

**System Settings**

This is the initial screen in the Setup wizard. This helps you to set up the following system parameters:

- Domain ID
- DHCP Server IP
- AnyCast Gateway Mac

Enter the values, and click Next.
The Virtual Machine Manager screen is displayed.
Virtual Machine Manager

The Virtual Machine Manager screen in the Setup wizard helps you to register the VMM.

**Step 1**
Click the Add (+) button.
The Add Virtual Machine Manager popup is displayed.

**Step 2**
Enter the following details:

- **VMM Type**—Specify the VMM type. Choose vcenter or openstack from the drop-down list.
- **Version Name**—Specify the version details. See Note below for details.
- **Description**—Enter a description for the VMM.
- **IP Address-Port**—If you choose vcenter, enter the IP address and the port. The default port is 443. If you choose openstack, enter the IP address.
- **User Name**—Enter the VMM username.
- **Passphrase**—Enter the VMM passphrase.

**Note**

1. If VMM Type is **openstack** and Version Name is **openstack-liberty-centos**, a new field VTF Deployment Mode appears in the Add VMM popup.
2. VTF Deployment Mode field had two modes: **vtf-vhost** and **vtf-as-vm**.
3. openstack-liberty-rhel, openstack-icehouse, openstack-juno, and openstack-kilo support only VM mode.
4. Openstack-liberty-centos supports both vhost and VM modes.
5. In vHost mode VTF installation has to be done manually.
6. VTF deployment mode can be selected at the time of VMM registration and this cannot be changed later.
7. All the computes in a data center should be either in vhost mode (VTF running as a process) or in vNode mode (VTF running as a VM). Currently VTS does not support mixed mode.

**Step 3**
Click Add
The VMM you added is listed in the Virtual Machine Manager screen.

You can check the status of VMM registration in the Status column.

**Step 4**
Click Next if the VMM registration is successful.
The Authorization Group screen is displayed.
Authorization Group

The Authorization Group screen in the Setup wizard helps you to create authorization groups. The authorization group will have credentials for logging into your devices. You can create as many authorization groups as necessary.

Click Add (+) icon. The Add Group popup window appears.
Enter the following details, and click Add:

- **Group Name**—The authorization group name.
- **Controller User Name**—This is the VTC administrative user name.
- **Device User Name**—This is the login user name for the device.
- **Passphrase**—This is the login passphrase for the device.

The authorization group gets added to the authorization group table.
To edit an authorization group, select the Auth Group Name check box and click the **Edit** icon.
To delete an authorization group, select the Auth Group Name check box and click the **delete (X)** icon.

Discovery

The Discovery screen helps you to discover the devices in your network, and add them to the inventory. You can perform auto discovery, or import devices manually using a .CSV file. Before you perform this step, ensure that:

- Link Layer Discovery Protocol (LLDP) has to be enabled on leafs, spine, DCI, and computes. See documentation for the respective devices for details about how to enable LLDP on these devices.
- A seed device has to be identified, and the IP should be provided. The seed IP is that of one of the leaf or spine devices.
- All devices must have the same set of credentials. These credentials will be used during the discovery process. See Managing Inventory, on page 19 for more information. The credentials must be of the appropriate privilege level on the devices.

To perform discovery:

**Step 1**  Click Discovery.
**Step 2**  Enter the Seed Device IP.
**Step 3**  Enter the Seed Device User Name.
**Step 4**  Enter the Seed Device Passphrase.
**Step 5**  Click Start Discovery.
After the discovery is complete, you may edit the editable fields in the table to modify the device details, before you add the details into the Cisco VTS inventory.

To import device details into inventory via CSV file, manually, click the **Import CSV**, then select the CSV file and import it.

If you want to edit details for more than one devices, you may select the devices, and then click **Bulk Edit** option. Click Apply after you make the changes.

**Step 6**

To add the devices to Cisco VTS inventory, select the devices and click **Add to Inventory** button.

**Note** When you add the devices to inventory using the Add to Inventory button, all the devices in the table are added to the inventory.

**Step 7**

Click **Next**.
The Inventory screen is displayed.

---

**Inventory**

The Inventory screen of the Setup wizard displays view inventory details: It has three tabs:

- Network Inventory—Details about the switches in the inventory. It shows the following details.
  - Device Name
  - Admin State
  - IP Address
  - Auth Group
  - Device Platform
  - Device Role
  - Group Tag
  - bgp-asn
  - Loopback Interface Number
  - Loopback Interface IP

  **Note** You need to discover the devices and add them to the inventory before you bring up the IoS XRv. If you do these tasks simultaneously, you might encounter errors.

- Fabric Inventory—Details about the fabric connection between the switches. It shows the following details:
  - Device Name
  - Device Type
  - Device Interface
• Device IP Address
• Device Port Name
• Connection ID

• Host Inventory—Details about the servers connected to the switches It shows the following details:
  • Host Name
  • Host Type
  • Host Interface
  • Host IP Address
  • Device Port Name
  • Connection ID
  • Capability—The host capability - Physical or Virtual.
  • Status—Shows the installation status.

The Host Inventory has the **Install Capabilities** button. You can select the host from the list, and click **Install Capabilities**. If the host is connected to a physical VTEP (ToR), it installs the host agent in case of an OpenStack environment. If the capability is Virtual, clicking Install Capabilities installs the VTF VM on that host. See *Installing OpenStack Host Agent and VTF using GUI*, on page 26.

Click on the info icon adjacent to the **Host Name**. Host Summary table popup appears.

If Virtual Capability is 'virtual-switch', both **Additional Host Details** and **VTF Details** can be viewed in the Host Summary table.

If Virtual Capability is 'no-virtual-switch' only **Additional Host Details** can be viewed in the Host Summary table.

Click **Finish** to exit the Setup wizard.

### Using the Expert Mode—Quick Guide

On logging in for the first time, if you choose the **I will set up myself** option, the Quick Guide appears.

You may opt to close the Quick Guide and proceed to the set up tasks on your own, via the Cisco VTS GUI. To get a list of tasks that need to be performed to set up and get started with Cisco VTS, see *Initial Configuration Tasks*, on page 11 section. At any time, you can access the Quick Guide from the settings menu on the top right corner of the Cisco VTS GUI.

The Quick Guide has the following tasks listed:

<table>
<thead>
<tr>
<th>Task</th>
<th>Subtasks</th>
<th>Doc Section</th>
</tr>
</thead>
</table>

---

**Note**
## Initial Configuration Tasks

After bringing up the Virtual Topology Controller (VTC) Virtual Machine (VM), do the following:

Before you perform the tasks below, ensure that installation is complete, day zero configuration on leafs is done, and all underlay configurations are working.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create an Authorization Group</td>
<td>Inventory &gt; Authorization Group</td>
<td>This will have credentials for logging into your devices. You can create as many auth groups as necessary.</td>
</tr>
</tbody>
</table>

### Additional Notes

**Navigation in VTS GUI / User Guide Section**
- Inventory > Authorization Group
- For more information about creating authorization group, see `Managing Users and Groups, on page 17`
<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Discover the Topology of all the leafs, spine, border-leafs, and DCI</td>
<td>Discovery &gt; Topology Discovery</td>
<td>VTFs and IOS XRv are not detected in topology discovery.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about adding devices and host information,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>see Performing Auto Discovery, on page 20</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Import the devices after adding the auth group</td>
<td>Inventory &gt; Import Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about adding devices and host information,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>see Importing Inventory using CSV File, on page 21</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Add the Domain ID, DHCP Server IP, and Anycast Gateway MAC</td>
<td>Administration &gt; System Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about adding devices and host information,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>see Administering Cisco VTS, on page 67.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Perform IOS XRv and VTF Registration. Note This step is required only</td>
<td>See the Installing the Virtual Topology Forwarder section in the</td>
<td>IOS XRv takes a few minutes to boot.</td>
</tr>
<tr>
<td></td>
<td>if you have a VTF-based deployment.</td>
<td>Cisco VTS Installation Guide</td>
<td>Register the VTF only after you see the VFG group on the GUI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To verify that the VFG group is created, go to Inventory &gt; Virtual Forwarding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Groups.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Task</td>
<td>Navigation in VTS GUI / User Guide Section</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>6</td>
<td>Login into the IOS XRv and verify that the network-controller config is pushed</td>
<td></td>
<td>This step is required only if you have a VTF-based deployment.</td>
</tr>
<tr>
<td>7</td>
<td>Update the BGP ASN information for the devices</td>
<td>Inventory &gt; Network Inventory</td>
<td>For more information, see Viewing Network Inventory, on page 23.</td>
</tr>
<tr>
<td></td>
<td>Create resource pools</td>
<td></td>
<td>For more information about creating an admin domain, see Managing Resource Pools, on page 31</td>
</tr>
</tbody>
</table>

- Resource Pools > Global VNI Pool
- Resource Pools > Device Specific VLAN Pools
- Resource Pools > Multicast IP Pool
<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
<th>Navigation in VTS GUI / User Guide Section</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Create an Admin Domain</td>
<td>Admin Domains &gt; Domains</td>
<td>Properties for the L2/L3 Gateway Group are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about creating an admin domain, see Creating an Admin Domain, on page 36</td>
<td>• Control Protocol: BGP-EVPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Replication Modes: Multicast and Ingress</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Distribution Mode: Decentralized</td>
</tr>
<tr>
<td>9</td>
<td>Add the devices to the Gateway Group</td>
<td>Admin Domains &gt; Domains</td>
<td>See the Supported Platforms section in the Cisco VTS Installation Guide for details about devices support for different roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about creating an admin domain, see Creating an Admin Domain, on page 36</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Add the ToR and IOS XRv to the L2 and L3 Gateway Group</td>
<td>Admin Domains &gt; Domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about creating an admin domain, see Creating an Admin Domain, on page 36</td>
<td></td>
</tr>
</tbody>
</table>
### Important Notes Regarding VMware vSphere Distributed Switch (VDS)

The following points need to be taken care of while you create a VDS.

**Note**
- All the ToRs in the inventory should be part of the VDSs.
- One VDS can represent one or more ToRs.
- All the hosts that are connected to a particular ToR should be part of the same VDS.

### For Non-VPC Specific Configuration

If you are not using VPC on the leaves:
- Associate one or more leafs per VDS.
- Attach the hosts' data interface to the VDS uplinks.

**Note**
See VMware documentation for the detailed procedure.
For VPC Specific Configuration

If you are using VPC on the leaves:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create one VDS switch for one or more VPC pairs.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable enhanced LACP.&lt;br&gt;See VMware documentation for the detailed procedure.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a Link Aggregation Group for each VDS.&lt;br&gt;See VMware documentation for the detailed procedure.</td>
</tr>
<tr>
<td>Step 4</td>
<td>You may remove the default port group that gets created as it will not be used.</td>
</tr>
</tbody>
</table>
Managing Users and Groups

You can create users and define the roles they have to control the access to Cisco VTS GUI operations. See the Managing Inventory chapter for details about importing inventory.

This chapter has the following sections:

- Creating Users, page 17

Creating Users

You can create users to define the role that the users have when they log in to Cisco VTS. There are two default roles available:

- Administrator
- Operator
- ncsadmin—Has the same permissions as Administrator.
- ncsoper—Has the same permissions as Operator.

To create users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click Administration &gt; User Management. The Administration / User Management window appears.</td>
</tr>
<tr>
<td>2</td>
<td>Click Add (+) icon. The Add New User popup window appears.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the User Name and Passphrase, and then select the desired role from the Role drop down list.</td>
</tr>
<tr>
<td>4</td>
<td>Click Save. The user details get added to the Users table.</td>
</tr>
</tbody>
</table>

Note

To edit the user name, check the User Name check box, click Edit icon.
To delete the user name, check the User Name check box, click Delete (X) icon.
Managing Inventory

You can discover the devices using the auto discovery option, and import the details into Cisco VTS. You can also manually create a CSV file with device details, in a prescribed format, and import it into Cisco VTS.

You can create authorization groups and assign devices you import into Cisco VTS, to these groups. Authorization groups are used to group devices with the same credentials (i.e. usernames and passphrases). Once the authorization groups are created, all the devices under these groups may be accessed without specifying the credentials every time they are accessed.

If the same credential are used for accessing all devices, one authorization group can be used. If the credentials are different for different devices, multiple authorization-groups (as many as username/passphrase pairs used by devices) need to be created.

When you do a manual import of devices, the CSV file that is used to import inventory details links the authorization group with a specific device. The applicable authorization group should be used for corresponding device entry in the CSV file.

This chapter has the following sections:

- Creating Authorization Groups, page 19
- Performing Auto Discovery, page 20
- Importing Inventory using CSV File, page 21
- Viewing the Network Topology, page 23
- Viewing Network Inventory, page 23
- Viewing Host Inventory, page 25
- Viewing the IOS XRv to VTF Mapping, page 27
- Migrating from vPC to ESI, page 28
- Redeploying Device Inventory, page 30

Creating Authorization Groups

Authorization Group is used by Cisco VTS to authenticate or to log in to the device.
To create an authorization group:

**Step 1**
Go to **Inventory > Authorization Group**. The Inventory / Authorization Group window appears.

**Step 2**
Click **Add (+)** icon. The Add Auth Group popup window appears. Enter the following details, and click **Save**:

- **Auth Group Name**—The authorization group name.
- **Controller User Name**—This is the VTC administrative user name.
- **Device User Name**—This is the login user name for the device.
- **Passphrase**—This is the login passphrase for the device.

The authorization group gets added to the Groups table.

To edit an authorization group, select the Auth Group Name check box and click the **Edit** icon.

To delete an authorization group, select the Auth Group Name check box and click the **delete (X)** icon.

---

**Performing Auto Discovery**

In the auto discovery option, Cisco VTS automatically discovers the network topology in the data center. You can modify the device details after discovery is complete and add details to the inventory.

The auto discovery option has the following prerequisites:

- Link Layer Discovery Protocol (LLDP) has to be enabled on leafs, spine, DCI, and computes. See documentation for the respective devices for details about how to enable LLDP on these devices.

**Note**
As part of Topology discovery, once the compute hosts have been discovered using LLDP, you need to add the username and passphrase to each host entry. This update is required for installation of the host-agent (in case of OpenStack) and any subsequent passphrase change via VTS GUI to go through.

- A seed device has to be identified, and the IP should be provided. The seed IP is that of one of the leaf or spine devices.
- All devices must have a common set of credentials. These credentials will be used during the discovery process. See **Managing Inventory**, on page 19 for more information. The credentials must be of the appropriate privilege level on the devices.
To perform auto discovery:

**Step 1**
Go to **Inventory > Import and Discovery**. The Inventory / Discovery window appears.

**Step 2**
Click **Discovery**. The Discover Network popup window appears.

**Step 3**
Enter the **Seed Device IP**.

**Step 4**
Enter the **Seed Device User Name**.

**Step 5**
Enter the **Seed Device Passphrase**.

**Step 6**
Click **Start Discovery**.

**Step 7**
After the auto discovery is complete, the details are displayed in the table.
You can use the **Bulk Edit** option to modify the device details for more than one devices, before you add the devices to inventory, using the **Add to Inventory** button. To avoid errors, make sure you review the details in the table before you add the devices to Inventory. The Cisco VTS discovery log file is under /var/vts/log. Check for any errors/exceptions in this log file.
If, during auto discovery, Cisco VTS fails to log into any of the nodes, then the information of the nodes along with the error details can be found in /var/vts/log.

When you add devices to the inventory using the Add to Inventory button, all devices in the table are added to inventory.

**Note**
When two ToRs are configured in VPC and no dual-homed host (connected to those ToRs) is in the VTS inventory, VTS does not correctly identify the VPC. You must add the dual-homed host connected to the ToRs in VPC to the VTS inventory, before provisioning a port on a host connected to the ToRs in VPC.

**Note**
Different ESI groups/domains must have different ES-id or system MAC. In other words, duplicate ES-id and system MAC are not allowed among ESI groups. This needs to be guaranteed by providing correct Day Zero configurations for ESI on Cisco Nexus 9000 switches.

---

**Importing Inventory using CSV File**

The device inventory details need to be uploaded using a CSV file, in the prescribed format. The inventory file is used to define device mappings. If the format is incorrect, Cisco VTS displays an error and provides the details of the error. After a successful import, the topology gets displayed based on the mapping specified in the file.

When adding device to inventory, in the list of devices connected to a switch, the interface field should contain the interface name for network devices and the MAC address for servers.

**Note**
You should be an admin user to download or upload the CSV file. Also, if you are uploading a CSV file for the first time and there are issues uploading the file, then only the partial information is uploaded. You need to delete all the devices from network inventory and re-upload the file after fixing the issues. Or else, you may encounter problems due to the partial upload.

To download a sample inventory file, click **Download Template**.
In a VMware environment, each time you add a leaf, you must create a corresponding VMware vSphere Distributed Switch (VDS). See the Important Notes Regarding VMware vSphere Distributed Switch (VDS), on page 15 section for details.

Note

Step 1
Go to Inventory > Import and Discovery. The Inventory / Discovery window appears.

Step 2
Click Import CSV
The Import Devices popup window appears.

Step 3
Click Browse to choose the CSV file.
Click Download Template to download a sample CSV file.
The CSV file has the following fields:

- device-name—The device host-name (leaf, spine, DCI)
- device-ip—IP address for the device (leaf, spine, DCI)
- device-platform—Can be Cisco Nexus 9000, Cisco Nexus 7000 etc based on the device that is part of the network.
- device-role—The role that a particular device plays in the data center.
  - leaf—If the device plays the role of a Leaf in the data center.
  - border leaf—If the device plays the role of a Border Leaf in the data center.
  - spine—If the device plays the role of a Spine in the data center.
  - spine-rr—If the Spine plays the role of a Route Reflector in the data center.
  - dci—If the device plays the role of a DCI in the data center.
- group-tag—Identifier for the group.
- port-name—Physical port connectivity (local interface)
- connection-type—server (if connected to compute host); fabric (if connected to another leaf, spine, DCI devices).
- server-id—Host-name or IP address of the connected device based upon what is configured on the actual host.
- server-type—virtual-server for computes; baremetal for connections to spine, DCI.
- interface-name—Physical port connectivity (interface of the connected device)
- auth-group—Authorization group name, created as part of initialization, with correct credentials.

Step 4
Browse for the CSV file, and click Import.

Step 5
After the import operation complete, the details are displayed in the table.
You can use the Bulk Edit option to modify the device details for more than one devices, before you add the devices to inventory, using the Add to Inventory button. To avoid errors, make sure you review the details in the table before you add the devices to Inventory.
Click the device name to open the connected devices popup window, which gives details about connected devices for a device.
**Viewing the Network Topology**

Topo. window provides a view of the data center fabric controlled by Cisco VTS. It displays the leafs, spines, border leafs, DCI, hosts, as well as the software VTEPs. You can get a tenant-based topology view using this feature.

To view the network topology:

---

**Step 1**  
Go to **Inventory > Topology**. The Inventory / Topology window appears.

**Step 2**  
Select the tenant for which you need to view the topology, from the **Select Tenant** drop down list.

The topology is displayed in the Topology window. You can use the following buttons to control the display:

- Select node mode
- Move mode
- Zoom in / Zoom out / Zoom Selection
- Fit Stage
- Full Screen mode

Hover the mouse cursor over the Topology Setting icon to view Topology Setting popup, where you can change the display icon appearance, and display color.

**Note**  
In case of FEX or VPC, if no host is connected, Cisco VTS will not show the VPC or FEX in the Topology. Also, you might encounter errors.

Different types of links will be represented as shown in legends.

Hover the mouse cursor over the link to view the Info popup, which gives the information about the link.

---

**Viewing Network Inventory**

The network inventory table displays details about the devices which have been added to the inventory.

To view the network topology:

---

Go to **Inventory > Network Inventory**. The Inventory / Network Inventory window appears with the Network Inventory table displayed.

The following details are displayed:

- Device Name
- Admin State
• IP Address
• Auth Group
• Device Platform
• Device Role
• Group Tag
• BGP-ASN
• Loopback Interface Number
• Loopback Interface IP

**Note** You need to add the BGP-ASN information, loopback interface number, and loopback interface id of every device prior to starting any provisioning.

You can add network devices via the Network Inventory table. To do this, click the **Add (+)** icon, and provide the details. You can use this option to add devices to the inventory.

To edit network device, select the device you want to edit and click the **Edit** icon.

To delete network devices from the Network Inventory table, select the device you want to delete and click the **Delete (X)** icon.

If there is problem in deleting device, you need make sure that fabric link is cleaned up manually. For example, when Device 1 is connected to Device 2, Inventory has two devices and two fabric links (this can be seen in Fabric Connection tab in Network Inventory)—one from Device 1 to Device 2, and the other from Device 2 to Device 1. While deleting Device 1 from network inventory, cleanup is done for Fabric link Device 1 to Device 2 and for the device from the inventory. The link Device 2 to Device 1 has to be cleaned up manually before you delete.

It is important that you remove the resource pool before deleting a device.

You need to discover the devices and add them to the inventory before you bring up the IoS XRv. If you do these tasks simultaneously, you might encounter errors.

To recalculate the inventory topology for a particular device, click the redeploy button. See [Redeploying Device Inventory](#) for more details.

---

**Adding Fabric Connection**

To add fabric connection:

**Step 1** Go to **Inventory > Network Inventory**. The Inventory / Network Inventory window appears with the Network Inventory table displayed.

**Step 2** Click Fabric Connection tab, then click **Add (+)** icon.

The Add Fabric Connection popup window appears.

**Step 3** Enter the necessary details and click **Save**.
Synchronizing Configuration

You can check if the device state is in sync with VTS configuration database.

To check whether the configuration is in sync:

This operation can be done only on a device that has the Admin State as **Unlocked**. If Admin state is **Locked**, you must change the Admin State to **Unlocked**, and then do the check-sync operation. Also, the out-of-sync-commit behavior in System Settings must be set to **Reject** for this feature to be enabled.

---

**Step 1**
Go to **Inventory > Network Inventory**. The Inventory / Network Inventory page displays the Network Inventory table.

**Step 2**
Click the **Config Sync** link under the Sync column, for the device.

If the configuration is in sync with the VTS database, the green In Sync icon is displayed.

If the configuration is not in sync with the device, you will get an option to compare the configuration. You can compare the actual device configuration with the VTS configuration, and can view the diff in compare-config popup. You can also use the copy to clipboard option to copy and paste the configuration in a text editor. To synchronize the configuration, you can use the following options:

- **sync-from**—Synchronize the VTS configuration by pulling configuration from the device.
- **sync-to**—Synchronize the VTS configuration by pushing configuration to the device.

**Note**
If switchname (switch hostname) is changed in the switch CLI, the sync to option will not work. The switchname has to be the same as the value in the VTS inventory.

---

Viewing Host Inventory

You can view the details of the hosts connected to the switches.

The Host Inventory has the **Install Capabilities** button. You can select the host from the list, and click **Install Capabilities**. If the host is connected to a physical VTEP (ToR), it installs the host agent in case of an OpenStack environment. If the capability is Virtual, clicking the Install Capabilities button installs the VTF VM on that host. See [Installing OpenStack Host Agent and VTF using GUI](#), on page 26.

To view host inventory details:

**Step 1**
Go to **Inventory > Host Inventory**. The Inventory / Host Inventory window appears.

**Step 2**
Select the device from the Select Device drop-down list. The following details are displayed:

- Host Name
• Host Type—baremetal is a server that is not managed by a VMM. A virtual-server is one which is managed by a VMM.

• Host Interface—The interface of the bare metal/virtual server connected to the TOR [Example: eth1 or eth2 etc].

• Host IP Address

• Device Port Name—The interface of the TOR which is connected to the baremetal/virtual server [Example: ethernet 1/1 etc].

• User Name

• Capability—The host capability - Physical or Virtual.

• Installation Status—Shows the installation status.

Note  If you have converted a Virtual server to Baremetal, before you upgrade, you will not be seeing details like Installation Status and Capabilities, after the upgrade.

To add a host from the table, select the Host Name check box corresponding to the device and click the Add (+) icon. Then provide the necessary details.

To edit a host from the table, select the Host Name check box corresponding to the device and click the Edit icon.

To delete a host from the table, select the Host Name check box corresponding to the device and click the click the Delete (X) icon.

---

**Installing OpenStack Host Agent and VTF using GUI**

You can use the Install Capabilities button to install the Host Agent and VTF on a host based on whether it is a virtual or physical server.

**Step 1**  Go to Inventory > Host Inventory. The Inventory / Host Inventory window appears

**Step 2**  Click + to add a host. You may also edit a host and modify the parameters to enable installation of physical or virtual capabilities.

• If you click + (Add) the Add New Host popup is displayed. Enter the following details.

• If you choose to edit an existing host, the following windows are displayed depending upon the host type:

  * Host Details:
    • Host Name
    • Host Type
    • Host Interface
    • Host IP Address
    • Device Port Name
    • Capability—Specify whether it is a virtual-switch ir not.
Managing Inventory

Viewing the IOS XRv to VTF Mapping

- Vmm IP Address
- User
- Passphrase

Common Parameters—These are displayed only if the host capability is virtual-switch.

- VTF IP—The IP address of the VTF.
- Subnet Mask
- Gateway
- Underlay Bridge—Name of the underlay network portgroup/bridge on the binding-host to which VTF is attached.
- Internal Bridge—Name of the tenant network port group/bridge on the binding-host to which VTF is attached.
- User
- Passphrase

Ensure that you review the tooltips for important information about the entries.

Click on the info icon adjacent to the **Host Name**. Host Summary table popup appears.

If Virtual Capability is **virtual-switch**, both **Additional Host Details** and **VTF Details** can be viewed in the Host Summary table.

If Virtual Capability is **no-virtual-switch**, only **Additional Host Details** can be viewed in the Host Summary table.

**Step 3**

Click **Install Capabilities**. Based on the host type, it installs the host agent / VTF on the host.

See the Status column for the installation status. The VMM type is also shown once the capabilities get installed.

**Note**

While installing capabilities for a host, if the selected VMM is **openstack-liberty-centos** and the mode for VTF deployment is **vtf-vhost**, VTF installation has to be done manually.

---

**Viewing the IOS XRv to VTF Mapping**

Go to **Inventory > Virtual Forwarding Groups**. The Inventory / Virtual Forwarding Groups window appears. The canvas displays the number of VTFs that are attached to the IOS XRvs. The table on the right hand side shows the VTFs.
Migrating from vPC to ESI

This section provides details about the generic procedure to migrate from Virtual Port Channel (vPC) to Ethernet Segment Identifier (ESI).

Before you begin, ensure that the following TCAM regions are carved on Cisco Nexus 9000 series switch:

```plaintext
hardware access-list tcam region vpc-convergence 256
hardware access-list tcam region arp-ether 256
```

To migrate from vPC to ESI:

**Step 1**
In case of IOS XRv HA, bring down the IOS XRv.

**Step 2**
Upgrade VTS to a version which supports ESI.

**Step 3**
Perform a port-detach operation to remove the relevant service configurations provisioned on the TORs.

**Step 4**
Remove the TORs from Admin Domain in VTS GUI.

**Step 5**
If the TCAM regions, as mentioned above, are not already carved on Cisco Nexus 9000 series switch, add the lines and save as running config.

```plaintext
hardware access-list tcam region vpc-convergence 256
hardware access-list tcam region arp-ether 256
```

**Note**
Do not reboot device (as the TOR will be rebooted in the next step).

**Step 6**
Upgrade TORs to a new Cisco Nexus 9000 image, which has ESI feature. This will automatically cause device to reboot.

```plaintext
copy run start
install all nxos bootflash:/nxos.7.0.3.Itc5.0.100.bin (or newer n9k image)
```

**Step 7**
Upgrade Cisco ASR 9000 series DCIs to an ESI supporting image.

**Step 8**
Once the setup is up then remove feature VPC and configure ESI on the required TORs that you are planning to convert to ESI.

<table>
<thead>
<tr>
<th>Remove VPC</th>
<th>no feature vpc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove other VPC related configuration under port channel and Ethernet Interfaces</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Configuration</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| Remove secondary interface from loopback | interface loopback0  
no ip address 44.44.44.44/32 secondary |
| Enable ESI | evpn esi multihoming |
| Create nve | interface nve1  
no shutdown  
source-interface loopback0  
host-reachability protocol bgp |
| Enable core links | interface Ethernet1/35  
Description " Connected with Spine"  
no switchport  
evpn multihoming core-tracking <<< Add here  
ip address 16.1.1.2/24  
ip router ospf 100 area 0.0.0.0  
ip pim sparse-mode  
no shutdown |
| Add Ethernet-segment and system-mac address in the port-channel | interface port-channel220  
switchport mode trunk  
switchport trunk allowed vlan none  
ethernet-segment 220  
system-mac eeee.1111.2222 |
| Apply the channel group to the TORs interface which are connected to compute. | interface Ethernet1/5  
switchport trunk allowed vlan none  
channel-group 220 mode active |
| Verify whether the ESI is up. | tor1# show nve ethernet-segment |

## ESI Database

| ESI: 03aa.bbcc.ddee.ee00.002d,  
Parent interface: port-channel30,  
ES State: Up  
Port-channel state: U  
NVE Interface: nve1  
NVE State: Up  
Host Learning Mode: control-plane  
Active Vlans: 1001  
DF Vlans: 0-4095  
Active VNIs: 30001  
Number of ES members: 1  
My ordinal: 0  
DF timer start time: 00:00:00  
Config State: config-applied  
DF List: 1.1.1.1  
ES route added to L2RIB: True  
EAD routes added to L2RIB: True |

---

The provided configuration commands are designed to enable multihoming and ESI functionalities, ensuring proper networking connectivity and redundancy. The specific commands address the removal of secondary interfaces, enabling ESI, creating NVE instances, setting up core links, adding Ethernet segments, applying channel groups, and verifying the ESI status.
Step 9
On Cisco VTS, perform a sync-from operation for the TORs that have ESI enabled.

Step 10
Redeploy inventory from Cisco VTS only for devices that have new ESI configuration. This is to make sure that Cisco VTS recognizes ESI configuration on Cisco Nexus 9000 series devices. See Redeploying Device Inventory, on page 30 for details.

Step 11
Remove the peer links between previous VPC peer TORs (Inventory > Network Inventory > Fabric Connection).

Step 12
Create a device group (Resource Pools > VLAN Pool), and add the group of ESI enabled devices to the group. Make sure a corresponding VLAN pool/range is also created for the device group.

Step 13
Add the ESI device group to appropriate functional groups in Admin Domain, and also disable ARP suppression in Admin Domain.

Step 14
Upgrade IOS XRv to the latest image.

Step 15
Perform a port-attach from VTS.

Redeploying Device Inventory

You can use the Redeploy feature to recalculate the inventory topology for a particular device. This is important in the context of VPC and ESI.

You need to Redeploy the inventory when device day zero configuration changes for:

- VPC or ESI. For example, vpc id for a port-channel is changed
- port-channel or ether-channel

Redeploy triggers the inventory for a device again. Since inventory reads the data from the device model in the database it is important to perform sync-from before doing a Redeploy.

Note
Redeploy function is different from the sync-from function. Sync-from gets the configurations from the device and updates it in the device model in the database. However, it does not recalculate the topology. That is, the topology would still show old information/configuration. Redeploy recalculates the inventory topology. After you perform a Redeploy, the topology will be updated with the modified configuration.

To redeploy device inventory:

Step 1
Go to Inventory > Network Inventory, perform a sync-from for the device for which the configuration has changed. See Synchronizing Configuration, on page 25 for more details.

Step 2
Select the device, click Redeploy.

Note
Redeploy just recalculates the inventory. Existing ports/VMs belonging to old device configurations, would not be updated or redeployed. You might need to delete and recreate the existing ports. We recommend that you use redeploy only if there are no existing ports/router/router interfaces.
Managing Resource Pools

Cisco VTS enables you to define global and device local resource pools so that the resources can be allocated when VMs or tenants are added.

You can define the multicast addresses that can be allocated sequentially for VXLAN tunnel creation so that you do not have to manage them separately. VNI and multicast pools are global and VLAN pool is for each device. You can define the multicast addresses as global resource pool. These multicast addresses will be allocated sequentially when new VXLAN tunnels are created. Network administrator can define multiple multicast address ranges.

Note
Default resource pools are device-specific VLAN pools that are also created automatically when leafs are added to the inventory. The default VLAN range is from 1001 to 2000. You can modify the range as per your requirement.

You can also specify global VNI pool range and device-specific VLAN pool range.

You can edit the range and also delete any unused ranges.

This chapter has the following sections:

- Specifying Global VNI Pool Range, page 31
- Specifying VLAN Pool Range, page 32
- Specifying Multicast IP Pool, page 33

Specifying Global VNI Pool Range

You can specify the global VNI pool range. To do this:

Step 1
Go to Resource Pools > Global VNI Pool. The Resource Pools / Global VNI Pool window appears. In Global VNI Pool window, the range table lists the following details:

- Range From
• Range To
• Restricted Range - data is Boolean (Yes or No)
• Used
• Available
• Total

Step 2 Click the Add (+) icon. Add VNI Pool popup appears.

Step 3 Specify the ranges, select the Restricted Range radio button to enable or disable the range, and click Save.

Step 4 To edit the range, select the Range From check box, and click the Edit icon as required.
All ranges are editable. Overlapping of range is allowed if Restricted Range field is Yes.

Step 5 To delete the range, select the Range From check box, and click the Delete (X) icon.

Specifying VLAN Pool Range

VLAN pool needs to be created for all the leafs and DCIs. You can create device specific VLAN pools. You can also group devices together, and create a VLAN pool for the group.

Note
We recommend that you check the supported VLAN pool range for the device that is created automatically, and also take a note of the reserved VLAN range. Every device has its own limitation. You need to ensure that you are not using a reserved VLAN range for your particular device.

See the following sections for details:

• Specifying Device VLAN Pool Range, on page 32
• Specifying Group VLAN Pool Range, on page 33

Specifying Device VLAN Pool Range

To specify device VLAN pool:


Step 2 Click Devices.

Step 3 Click the Add (+) icon. The Add Range pop up window appears.

Step 4 Enter the Device details, and specify the From and To values.
The device name should match the leaf name in the inventory. From is VLAN start number and To is VLAN end number to be used for the leaf.

Step 5 Select the Restricted Range radio button to enable or disable the range, and click Save.
To edit a device specific VLAN pool, select the Device check box, and click the **Edit** icon.

To delete a device specific VLAN pool, select the Device check box, and click the **Delete (X)** icon.

### Specifying Group VLAN Pool Range

To specify VLAN pool range for a device group:

2. Click **Groups**.
3. Click the **Add (+)** icon. The Set Range pop up window appears.
4. Enter the Group Name and select the devices that need to be part of the group. Click the help icon for guidelines about the group name.
5. Select the **Restricted Range** radio button to enable or disable the range, and Click **Save**.
6. To view the devices associated with a group, select the group and click **Associated Devices**.
7. Click **Save**. The group gets created and is listed in the table.
8. To add range to the group, select the group and click the **Add (+)** icon.
9. Specify the From and To values.
10. Click **Save**.
11. To edit a device specific VLAN pool, select the Device check box, and click the **Edit** icon. All ranges are editable.
12. To delete a group specific VLAN pool, select the Device check box, and click the **Delete (X)** icon.

### Specifying Multicast IP Pool

You can specify the IP range. The range must be within the multicast IP address range configured on leaf devices via day zero configuration file. The only valid IPv4 address starting with 0 is 239.0.0.0/8.

2. Click the **Add (+)** icon, and enter the Netmask values.
   - Click the **Question Mark (?)** icon to view the Multicast IP address range.
3. Click **Save**.
   - To delete Multicast IP Pool, select the Netmask check box, and click the **Delete (X)** icon.
Creating and Managing Admin Domains

This chapter has the following sections:

- Admin Domain Overview, page 35
- Viewing Admin Domain, page 36
- Creating an Admin Domain, page 36

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

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 DC1 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.
- Ensure that you have discovered the topology and imported the CSV file (after assigning / reviewing device roles). See **Performing Auto Discovery**, on page 20 and **Managing Inventory**, on page 19 sections for details.

**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:

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 DCI</td>
<td>DCI is an external gateway.</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCI</td>
<td>• New or Shared DCI.</td>
</tr>
</tbody>
</table>
| DC GW            | • New or Shared DC GW.  
               | • Control Protocol - BGP EVPN. |
## Functional Group

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Property</th>
</tr>
</thead>
</table>
| L3 GW | • New and Shared L3 GW.  
• Control Protocol - BGP EVPN.  
• 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 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 L2 GW group devices to this L3 GW 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.  
• ARP Suppression - On. |
| L2 GW | • New and Shared L2 GW.  
• Control Protocol - BGP EVPN.  
• Replication Mode - Multicast or Ingress.  
• Distribution Mode - Decentralized.  
• ARP Suppression - On. |

## 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.
Click the icon on the right hand side below **Devices** that shows how many devices are placed in this group or how many devices can be placed in this group. You can see **All** option which 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**
Connect or link the functional groups based on your requirement.

**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.
Managing Templates

A template is a container of configurations, which can be applied to a target such as a router.

Cisco VTS supports the following template types:

• Route templates—A route template is a template that lets you configure static routes and route targets. This template can be applied to a tenant or a router. When it is applied to a tenant, all the routers within that tenant inherit the static route and route target configuration. When it is applied to a router, it overrides the route template that was inherited from the tenant. It is supported in a set up that has only Cisco ASR 9000 Series Aggregation Services Routers as DCI.

Only integrated DCI mode is supported. VRF-peering mode is not supported.

• L3 Service Extension templates—An L3 Service Extension template allows you to extend Cisco VTS Layer 3 service configuration on routers or tenants.

The configuration you define in the service extension template, along with the out-of-the-box Cisco VTS L3 configuration, will be pushed to the device to get the combined configuration on the device. Service extension templates do not allow you to configure any parameter that Cisco VTS configures out-of-the-box.

Multiple L3 Service Extension templates can be attached to a tenant or router. The admin has to ensure that the templates do not have conflicting configuration.

Currently, L3 Service Extension templates are applicable only for Cisco Nexus 9000 series devices.

The template is stored in the Cisco VTS database, and can be used with multiple routers or tenants. You can either associate the template while you create the router or tenant. Or associate a template to a tenant or router you have already created, while you edit the tenant or router.

When you detach the template from the tenant, it cleans up the configuration on the device.

Note

For route templates, you can have only one instance of a template type per tenant/router. For example, let the template types be Temp A and Temp B, and the instance of Temp A be Ins A and that of Temp B be Ins B. Now, Ins A and Ins B can be applied to a tenant/router. However, Ins A and Ins A’, where Ins A’ is a second instance of Temp A, cannot be applied at the same time on the tenant/router.

The following sections provide more details about working with templates:

• Creating Route Templates, page 42
Creating Route Templates

To create templates:

Step 1: Go to **Templates > Template Management**. The Templates / Template Management page appears.

Step 2: Click **+**. The New Template page appears.

Step 3: Enter a name for the template in the Template Name field. Only alphabets, numbers, and special characters . , _ and - are allowed. The maximum character limit is 128.

Step 4: Enter a description for the template, in the Description field. This is optional.

Step 5: Select the template type from the Template Type. For route templates, select Route.

Step 6: Click **Add Configuration**. The New Template page appears.

Step 7: Enter a route target seed. This can be an integer value in the range of 1-16777215. Route Target with seed is pushed to DCI, and Leaf if eBGP is enabled.

Step 8: Enable or Disable the Auto Route Target option. By default, it is enabled. See **Disabling Auto Route Target Configuration**, on page 44 for details.

Step 9: Add Static Routes. See **Adding Static Routes**, on page 42 for details.

Step 10: Add Route Targets. See **Adding Route Targets**, on page 43 for details.

Step 11: Click **Save**. The template is saved and listed in the Template Management page.

Adding Static Routes

You can add static routes to a template while you create the template.

Step 1: In the Template Management page, while you create or modify a template, click the **Static Route** tab.

Step 2: Click **+**. The Add Static Route(s) pop-up appears.

Step 3: Add a Destination IP address and netmask.

Step 4: Add the Next Hop IP address and netmask. Netmask is optional.

Step 5: Click **Add**. The static routes get added to the template.

You can add five static routes at a time.
Adding Route Targets

Step 1  In the Template Management page, while you create or modify a template, click the Route Target tab.

Step 2  Click +. The Add Route Target(s) pop-up appears.

Note  You can add five route targets at a time.

Enter the route targets to be shared across the different VRFs. The valid route target formats are:

- ASN2:NN4
- ASN4:NN2
- IPv4:NN2

Where:

- NN2 and ASN2 has a range of 1-65535
- NN4 and ASN4 has a range of 1-4294967295
- IPv4 is an IPv4 address in the dotted decimal format

Step 3  Specify whether route targets are to be imported or exported. To do this, select the desired value from the Direction drop-down.

Step 4  Specify whether the route target should be imported / exported on leafs or DCI. Select one of the following from the Type drop-down:

- Internal — To import / export on leafs.
- External — To import / export on DCI.
- Both

The following table gives an example of route target configuration based on Type and Direction.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>External</th>
<th>Both (Internal / External)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Internal</td>
<td>External</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>Leaf</td>
<td>DCI</td>
<td>DCI:</td>
</tr>
<tr>
<td></td>
<td>route-target import 8001:8001</td>
<td>import route-target 8001:8001</td>
<td>export route-target 8001:8001 stitching</td>
</tr>
<tr>
<td></td>
<td>route-target import 8001:8001 evpn</td>
<td>8001:8001</td>
<td>Leaf:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>route-target import 8001:8001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>route-target import 8001:8001 evpn</td>
</tr>
<tr>
<td>Direction</td>
<td>Type</td>
<td>Internal</td>
<td>External</td>
</tr>
<tr>
<td>-----------</td>
<td>-----</td>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>

- If Type is Internal and Direction is Import/Export—BGP-EVPN Route Targets are pushed to the leaf where router instances exist, based on the your choice of Direction (Import/Export). This can be used for route sharing/distribution using specific route-targets within the DC fabric.
- If Type is External and Direction is Import/Export—WAN facing L3VPN Route Targets are pushed to DCI for routers which have external gateways attached, based on the your choice of Direction (Import/Export). This can be used for importing or exporting WAN side routes with specific route-targets and stitch it to the DC fabric.
- If Type is Both and Direction is Import—BGP-EVPN Import Route Targets are pushed to the leaf where router instances exist. Fabric facing Stitching Route Targets are exported on the DCI for routers that have external gateways attached. This enables the user to stitch WAN side routes and redistribute it with specific route-targets towards the DC fabric side.
- If Type is Both and Direction is Export—BGP-EVPN Export Route Targets are pushed to the leaf where router instances exist. Fabric facing Stitching Route Targets are imported on the DCI for routers that have external gateways attached. This enables you to export routes with specific route-targets from within the DC and stitch it to the WAN side.

**Step 5**  
Click **Add**.

---

**Disabling Auto Route Target Configuration**

To enable or disable automatic route target configuration, use the Auto Route Target toggle switch in the New Template screen while you create route templates. By default, Auto Route Target (RT) is enabled. When this is enabled, Cisco VTS adds route target configurations automatically, in addition to any static / manual route targets you have defined in route template, while the template configuration is pushed to the VTEPS.

If you choose to disable Auto Route Target, ensure that:

1. At least one import route target and one export route target are defined for internal devices (that is, for leaf switches controlled by Cisco VTS) in the same route template where auto RT gets disabled.
2. When a DCI is present in Admin Domain, and you choose to disable Auto Route Target, ensure that:
   - At least one import route target and one export route target are defined for external devices.
At least one import route target and one export route target are defined for "both".

This is to make sure that when auto RT is disabled, the static route targets defined in the template (which will then be pushed to the DCI) are sufficient to enable the DCI to communicate with the TORs properly. Whenever you enable Auto Route Target again the route targets created using the route target seed (if provided) or ASN# will be pushed to devices. In addition, the RT seed textbox will be enabled again.

Creating L3 Extension Templates

To create L3 Extension templates:

Step 1 Go to Templates > Template Management. The Templates / Template Management page appears.
Step 2 Click +. The New Template page appears
Step 3 Enter a name for the template in the Template Name field. Only alphabets, numbers, and special characters ., _ and - are allowed. The maximum character limit is 128.
Step 4 Enter a description for the template, in the Description field. This is optional.
Step 5 Choose L3 Extension as the template type.
Step 6 Choose the Device Platform. Currently only Cisco Nexus 9000 Series devices are supported.
Step 7 Click Add Configuration to add configuration to the template. The Author Template window appears.
Step 8 Click Configuration icon to get the Add Configuration menu. The flyout menu displays all the configuration options that are available at the root level. You can search for the desired configuration in the Search field. Configuration options available are limited to configuration that Cisco VTS does not provide out of the box. The User Interface(UI) is schema driven and shows the configuration tree based on the device platform selected and the service extension template type, for example, L3 Service Extension Template.
Step 9 Choose the desired configuration. The configuration you chose gets added as a child node in the Config tree, on the left pane. You may add further configuration to the node that you have added by clicking the Configuration icon. If you want to delete the configuration, click the delete (X) icon.

For configuration items which can take multiple instances, the Add Instance button appears in the authoring pane. You can add an instance by clicking Add Instance. Click Add after you add the configuration for the instance.

Note For certain configurations, some of the options that are available for selection have the %v suffix (for example, %vVRF_NAME %vTENANT_NAME, when you choose config > vrf > context and add a new instance). The %v suffix denotes that it is a system variable. If you select a system variable, the value will be resolved in the template when the template is attached to the router. Tenant name, VRF name, and VLAN ID are the supported system variables.

Step 10 Click Save Template.
The template gets added to the Template Management screen. You can click on the template to get a summary of the template, in the Template Summary page. You can expand the Config node to view the template configuration. You can edit the template from the Summary screen, by clicking Edit Template Config.
Editing Templates

You can modify a template that you have created.

Step 1  Go to Templates > Template Management. The Templates / Template Management page lists all the templates you have created.

Step 2  Select the check box corresponding to the template you need to edit, and click the edit icon.

Note  You can also edit a template from the Template Summary screen. Click Edit Template Config button to edit a template.

Based on the template type, the edit template page is displayed. For a Route template, the edit page for that route template is displayed. For a L3 Service Extension templates, the Edit Template page is displayed. You may change the Template Description, if required. Then click Edit Configuration to modify the service extension configuration.

Step 3  Make the desired changes, then click Save.

Copying a Template

You can copy a template and save it with a different name. You can also modify the parameters while you copy.

Step 1  Go to Templates > Template Management. The Templates / Template Management page lists all the templates you have created.

Step 2  Select the check box corresponding to the template you need to copy, and click the copy icon.

Step 3  Modify the details if required, then click Save.

Deleting Templates

You can delete a template that you have created.

Note  You can delete a template only if it is not attached to either a tenant or router. If it is attached to a tenant or router, an error is displayed when you try to delete. You need to detach the template from tenant or router before deleting the template.

Step 1  Go to Templates > Template Management. The Templates / Template Management page lists all the templates you have created.

Step 2  Select the check box corresponding to the template you need to delete, and click the X.
The Delete pop-up appears.

Step 3 Click Delete to delete the template.

Attaching Templates to Tenants

You can attach template to tenants when you create or edit tenants.

- Attaching Template while Adding Tenants, on page 47
- Attaching Template while Editing a Tenant, on page 47

Attaching Template while Adding Tenants

You can attach templates to a Tenant while you add a tenant.

Step 1 When you are adding a new tenant, click the find icon in the Template field. The Select Template pop-up appears.

Step 2 Select the template type, then select the desired template. If you want to create a new template and attach that, click Create New Template.

Step 3 Click Select Devices(s) to select the devices.

Step 4 Click Apply Template(s).

Step 5 Click Save.

Attaching Template while Editing a Tenant

You can also modify an existing tenant to attach a template.

Step 1 Go to Tenants > Tenant Management. The Tenants / Tenant Management page lists all the tenants you have created.

Step 2 Select the check box corresponding to the tenant you need to modify, then click the edit icon.

Step 3 Click the find icon in the Template field. The Select Template pop-up appears.

Step 4 Select the template type from the Template Type drop down list. If you want to create a new template and attach that, click Create New Template.

Step 5 Select the desired template. Then click Select Device(s), to select the devices.

Step 6 From the Select Device(s) popup window, select the devices, then click Apply Template(s).

Step 7 Click Save in the Edit Tenant page.
Detaching Template from Tenants

You can detach a template that you had attached to a Tenant. When you detach a template from a tenant, all the template configuration is removed from the routers that inherited the template.

To detach the template:

Step 1 Go to Tenants > Tenant Management. The Tenants / Tenant Management page lists all tenants.
Step 2 Select the tenant from which you want to detach the template, then click the Edit icon.
Step 3 Click the Find icon in the Templates field. The Select Template popup is displayed.
Step 4 Check the check box.
Step 5 Click Save.

Attaching Templates to Routers

You can attach templates to routers while adding a router or while modifying an existing router. By default, router inherits the template from the tenant. You can override an inherited template while you create or modify a router, by selecting a different template, or creating a new template and attaching to the router.

- Attaching Templates while Adding Routers, on page 48
- Attaching Template while Editing a Router, on page 49

Note

The configuration is pushed to the device only when Port Attach is done. If a router is created and template is applied to the tenant or router, but port is not attached, then the template configuration is not pushed. See Creating a Network using Cisco VTS GUI, on page 57 for details about attaching port.

Attaching Templates while Adding Routers

While you add the router, by default, the router inherits the template from the tenant. The template field displays <template name> (Inherited). You may inherit the template from the tenant or may chose to select a template of your choice.

Step 1 Click the Find icon in the Template selection box. The Select Template popup is displayed.
Step 2 Uncheck the Inherit from Tenant check box. The popup lists all the available templates.
Step 3 Select the desired template, then click Apply. The template gets applied to the router.
If you want to create a new template, click **Create New Template**. You will be redirected to the **Templates > Template Management > New Template** page. After you create the new template, you must select the new template from the Select Template pop up, as described in Step 2 and 3.

**Step 4**
Click **Save** after you complete the router creation procedure.

### Attaching Template while Editing a Router

You can attach a template to a router while you edit a router.

**Step 1**
Go to **Overlay > Router**. The Overlay / Router page lists all the routers.

**Step 2**
Select the Router that you need to modify, then click the edit icon. The template field lists the template that the router has inherited from the tenant.

**Step 3**
Click the Find icon in the Template selection box. The Select Template popup is displayed.

**Step 4**
Uncheck the Inherit from Tenant check box. The popup lists all the available templates.

**Step 5**
Select the template type from the Template Type drop down list.

**Step 6**
Select the desired template, then click **Select Device(s)**
If you want to create a new template, click **Create New Template**. You will be redirected to the **Templates > Template Management > New Template** page. After you create the new template, you must select the new template from the Select Template pop up, as described in Step 2 and 3.

**Step 7**
From the Select Devices popup window, select the device(s) on which you want to apply the template, click **Apply Template(s)**.

**Step 8**
Click **Save**.
Managing Tenants

The Tenant Management page displays a list of all tenants you have created. You can add, modify or delete a tenant. You can also attach templates to tenants.

This chapter has the following sections:

- Adding Tenants, page 51
- Editing Tenants, page 52

Adding Tenants

To add tenants:

**Step 1** Go to Tenants > Tenant Management. The Tenant Management page appears.

**Step 2** Click Add (+) icon.

**Step 3** Enter the following:

- Tenant Name
- Description

**Step 4** If you want to attach template to the tenant, click the find icon in the Template field. See Attaching Templates to Tenants, on page 47 for details about attaching templates.

**Step 5** Click Save.

**Step 6** To add a Zone, click the Add (+) icon. The Add Zone popup appears.

**Step 7** Enter the zone name, and click OK.

**Step 8** Click Save.
Editing Tenants

To edit a tenant:

**SUMMARY STEPS**

1. Go to **Tenants > Tenant Management**. The Tenant Management page appears.
2. Select the tenant, then click the edit icon.
3. Modify the following:
4. If you want to associate a new template or change the existing template, click the find icon in the Template field. See *Attaching Templates to Tenants*, on page 47 for details about associating templates.
5. Click **Save**.
6. To enable or disable network extension, use the **Extend all networks** toggle switch. By default, Extend all networks is **Yes**.
7. Modify the zone details.
8. Click **Save**.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Go to <strong>Tenants &gt; Tenant Management</strong>. The Tenant Management page appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the tenant, then click the edit icon.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Modify the following:</td>
</tr>
<tr>
<td></td>
<td>• Tenant Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td>Step 4</td>
<td>If you want to associate a new template or change the existing template, click the find icon in the Template field. See <em>Attaching Templates to Tenants</em>, on page 47 for details about associating templates.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To enable or disable network extension, use the <strong>Extend all networks</strong> toggle switch. By default, Extend all networks is <strong>Yes</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Modify the zone details.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Provisioning Overlay Networks

This chapter has the following sections:

- Provisioning Overlay Networks Using Cisco Virtual Topology System, page 53
- Creating Overlays, page 54
- Creating Network using VMware, page 55
- Creating Subnetwork using VMware, page 56
- Creating Routers using VMware, page 56
- Attaching Network to Router, page 56
- Attaching a Virtual Machine to Network, page 57
- Creating a Network using Cisco VTS GUI, page 57
- Creating Router using Cisco VTS GUI, page 59
- Assigning BVI Interface IP Address, page 60

Provisioning Overlay Networks Using Cisco Virtual Topology System

Virtual Topology System enables overlay connectivity orchestrated through an SDN-based control plane. This ensures instant availability of computing and application workloads in the virtualized data center, and removes network provisioning challenges.

Cisco VTS uses VXLAN to overcome scale limits in the data center and to segment the network better. VXLAN is designed to provide the same Ethernet Layer 2 network services as VLAN does, but with greater extensibility and flexibility. The dependence on a Layer 3 underlay network allows VXLAN to take complete advantage of Layer 3 routing, equal-cost multipath (ECMP) routing, and link aggregation protocols. Virtual Topology System supports hardware and software VTEPs to segment the data center network.

Virtual Topology System supports both VXLAN overlays using the BGP EVPN control plane and VXLAN overlays using IP Multicast-based techniques.
Implementing VXLANs using MP-BGP EVPN based control plane to manage the VXLAN overlay provides a distributed network database, which enables federation and scaling. The BGP EVPN solution is the preferred option, and it can be flexibly implemented using the infrastructure policy constructs within the Virtual Topology System environment.

Virtual Topology System implements the highly scalable MP-BGP with the standards-based EVPN address family as the overlay control plane to:

- Distribute attached host MAC and IP addresses and avoid the need for unknown unicast, and multicast traffic
- Support multidestination traffic by either using the multicast capabilities of the underlay or using unicast ingress replication over a unicast network core (without multicast) for forwarding Layer 2 multicast and broadcast packets
- Terminate Address Resolution Protocol (ARP) requests early

Control-plane separation is also maintained among the interconnected VXLAN networks. Capabilities such as route filtering and route reflection can be used to provide flexibility and scalability in deployment.

**High-level Workflow for Establishing a VXLAN Overlay Network with Hardware and Software VTEPs using BGP EVPN**

The following steps provide a high-level workflow for establishing a simple VXLAN overlay network with hardware and software VTEPs using a BGP EVPN control plane:

- Prepare the physical environment to be managed by Cisco VTS to build virtual overlays. See the Prerequisites section in the Cisco VTS Installation Guide for details.
- Discover the network topology in the data center. See the Managing Inventory chapter of the Cisco VTS User Guide for details.

After you commit the changes to the network group, Virtual Topology System automatically pushes all the relevant configuration information to the respective leafs, Cisco IOS XRv route reflectors, and DCI gateways. At this point, the Admin Domain is ready to build overlay networks based on the intent defined by the service policy or through a Virtual Machine Manager (VMM) or orchestration environment.

For a detailed, illustrated example, see Cisco Virtual Topology System: Data Center Automation for Next-Generation Cloud Architectures White Paper.

**Creating Overlays**

As part of overlay provisioning, you may need to:

- Create Tenant
- Create Network
- Create Subnet
- Create Router
- Create VM
This can be done using the VMM or Cisco VTS GUI.

**Using OpenStack**

When you use a VMM such as OpenStack or VMware, the plugin will provide integration between the VMM and Cisco VTS. Once Tenant/ Network/ Subnets are created on the VMM, required overlay network(s) will automatically be created by Cisco VTS.

For information about performing these tasks via OpenStack Horizon dashboard, see OpenStack documentation.

**Using VMware**

For information about performing these tasks using VMware, see the following sections:

- Attaching Network to Router, on page 56
- Creating Network using VMware, on page 55
- Creating Subnetwork using VMware, on page 56
- Creating Routers using VMware, on page 56
- Attaching a Virtual Machine to Network, on page 57

**Using Cisco VTS GUI**

For information about creating Network and Router using Cisco VTS GUI, see the following sections:

- Creating a Network using Cisco VTS GUI, on page 57
- Creating Router using Cisco VTS GUI, on page 59

**Creating Network using VMware**

To create a network:

**Step 1**
Select one of the VDS switches you created, then select Manage tab.

**Step 2**
Select the Cisco VTS Network tab and click Add (+) to add the network.

**Step 3**
Select create Tenant and enter Network Name field.

**Step 4**
Click Create to create the network.

**Step 5**
Click the Refresh icon to display the created network.
Creating Subnetwork using VMware

Before you create the subnetwork, you need to create the network in which the subnetwork has to be created.

To create subnetworks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select one of the VDS switches you had created, then click the Manage tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Cisco VTS Network tab, and click the network name in which the subnetwork has to be created.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the subnet name, the network range in CIDR format, and the Gateway IP.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Create Subnet button to create subnetwork.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Refresh button to see the subnetwork.</td>
</tr>
</tbody>
</table>

Creating Routers using VMware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select one of the VDS switches you had created, then click the Manage tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Cisco VTS Router tab, and click Add (+) to add the Router.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Tenant Name and enter the Router Name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Create Router button to create the router.</td>
</tr>
</tbody>
</table>

Attaching Network to Router

To attach a network and subnetwork to a router:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select one of the VDS switches you had created, then click Manage tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select VTS Router tab and click the Router Name where network has to be added. The Router Details pop up appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Network and subnet and click Attach Subnet.</td>
</tr>
</tbody>
</table>
Attaching a Virtual Machine to Network

To create VMs:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create network and subnet using vCenter Cisco VTC plugin. This will create portgroup for the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Create the VM in vCenter and attach the created portgroup to the VM. This will attach the VM to the network created via Cisco VTS.</td>
</tr>
</tbody>
</table>

Creating a Network using Cisco VTS GUI

To create a network from the Cisco VTS GUI:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Go to Overlay &gt; Network. The Overlay / Network window appears. The Network table lists:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Network Name</td>
</tr>
<tr>
<td></td>
<td>• Tenant</td>
</tr>
<tr>
<td></td>
<td>• Zone</td>
</tr>
<tr>
<td></td>
<td>• Admin state</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Subnet</td>
</tr>
<tr>
<td></td>
<td>• Network Type</td>
</tr>
<tr>
<td></td>
<td>• External Network</td>
</tr>
<tr>
<td></td>
<td>• VNI</td>
</tr>
<tr>
<td></td>
<td>• Inherit Extensions - (need more information)</td>
</tr>
<tr>
<td></td>
<td>• Extended - (need more information)</td>
</tr>
</tbody>
</table>
**Note**

- When **Extend all networks** toggle (in Editing Tenant) is set to **YES** at Tenant level, Inherit Extensions column will have toggle as **Yes**, and Extended column will have a **checkmark**.

- When **Extend all networks** toggle (in Editing Tenant) is set to **NO** at Tenant level, Inherit Extensions column will have toggle as **Yes**, and Extended column will have a **crossmark**.

- If Inherit Extensions column will have toggle as **NO**, then Extended column will have **toggle button** instead of a checkmark.

- When you hover over **Show Legend link**, a popup shows various network icons.

---

**Step 2**
Click **Add (+)** icon.

**Step 3**
Select the Tenant for which you to create the network.

**Step 4**
Select the Zone.

**Step 5**
To enable or disable network extension, use the **Extend networks** toggle switch. By default, Extend all networks is **Yes**.

**Step 6**
Enter the network name.

**Step 7**
Select the External Network check box if you need to specify that the network is external. This implies that the network needs to be configured on the Border Leaf and DCI Gateway.

**Step 8**
Click **Save**.
You may also add a subnet, and add port.

---

**Creating a Subnetwork**

To create a subnetwork:

**Step 1**
Click Add Subnet in the Subnet pane of the Add Network popup.

**Step 2**
Enter the subnet name, the network address, and gateway IP, then click OK.

**Step 3**
Click OK to save the subnet information.

---

**Attaching a Port**

To add a port:

**Step 1**
Go to **Overlay > Network**

**Step 2**
Click **Port Attach**, then click the add icon. The Attach Port popup appears.

**Step 3**
Specify whether it is a Physical Device or a Virtual Device, by selecting the appropriate radio button. For Virtual Devices, the MAC address is required. For physical devices, it is optional.
You can use Static VLAN button if you want to specify a certain VLAN to be used for port attach. By default, VTS allocates a free VLAN from its bucket of VLANs, but you may specify one if you wish to.

**Step 4**  
Enable Tagging by selecting the **Tagging** check box.

**Step 5**  
Select the **Device** from the drop-down list.

**Step 6**  
Specify the Interface. Select one of the following:

- Ethernet
- Port Channel
- VPC
- ESI

It lists the available interfaces, based on your selection.

**Note**  
- After importing ESI inventory you must manually create a device group on the VLAN Pool page from VTS GUI, and add the group of ESI devices into that device group. Also make sure a corresponding VLAN pool gets created for the ESI device group.
- Add the ESI device group to L2 and L3 GW groups in Admin Domain.
- ARP suppression needs to be disabled for ESI. It can be done from VTS GUI for L2 GW group in Admin Domain.

**Step 7**  
Choose the desired interface, and click **OK**.

---

**Creating Router using Cisco VTS GUI**

To create a router using Cisco VTS GUI:

**Step 1**  
Go to **Overlay > Router**. The Overlay / Router window appears.

**Step 2**  
Click the **Add (+)** icon. The Add Router window appears.

**Step 3**  
Select the tenant from the **Select Tenant** drop-down list.

**Step 4**  
Select the Zone from the **Select Zone** drop-down list.

**Step 5**  
Enter a VRF name. This is optional. If this is left empty, when the Save button is clicked, a default VRF name will be automatically generated.

- **The custom VRF name accepts up to 24 characters.**
- **If there is no input for custom VRF name, a default VRF name will be generated in form of <tenant-name>-<router-name>. Both tenant-name and router-name accept up to 15 characters.**
  - If Cisco ASR 9000 series router is configured as DCI in the domain, and you have not given a the custom VRF name, then you must ensure that the default VRF name does not exceed 27 characters. Otherwise, the configuration will fail.
  - If Cisco IOS XRv is configured, and you have not given a custom VRF name, then you must ensure that the default VRF name does not exceed 24 characters. Otherwise, the configuration will fail.
• If configuration fails because the default VRF name exceeds the limit, you can choose to use custom VRF name instead.

• If the configuration fails because the default VRF name exceeds 27 characters, an error message appears on the Network > Port Attach screen, which indicates invalid input for “bridge-domain” configured on Cisco ASR 9000 series router.

• For IOS XRv configuration, a similar error is displayed if the default VRF name exceeds 24 characters.

• If you modify the VRF name after saving the router, the Router Gateway IP address will be removed. You can reconfigure it back after saving the VRF name change.

---

**Assigning BVI Interface IP Address**

To assign a Bridge Group Virtual Interface (BVI) IP address:

---

**Step 1** Go to Overlay > Network. The Overlay /Network page appears.
**Step 2** Click the + icon. The Add Network page appears.
**Step 3** Enter the Network name.
**Step 4** Check the External Network check box.
**Step 5** Click the + icon to assign a Subnet to the network created.

1. If a Subnet is assigned to this External Network, assign the Router Gateway IP address for BVI interface from this Subnet under Step 10.
2. If Subnet is not assigned to this External Network, any IP address can be assigned to Router Gateway IP address tab for BVI interface under Step 10.

**Step 6** Go to Overlay > Router. The Overlay /Router page appears.
**Step 7** Click the + icon. The Add Router page appears.
**Step 8** Click the + icon to assign an Interface to the Subnet created.
Note: This subnet belongs to the Internal network, and excludes the External network.

**Step 9** Select an external network from the **Router Gateway** drop-down list. Router Gateway IP address field appears.

**Step 10** Assign the **Router Gateway IP address** for the selected external network for BVI interface and click **Save**.

**Step 11** Verify whether the configuration is pushed to DCI and the IP address is assigned to BVI interface.
Assigning BVI Interface IP Address
Viewing Overlay Details

You can view details about the network at the device, VM, baremetal, network, and router levels. The following sections provide details:

- Viewing Device Details, page 63
- Viewing Virtual Machine Details, page 64
- Viewing Baremetal Details, page 64
- Viewing Network Details, page 65
- Viewing Router Details, page 65

Viewing Device Details

To view details at device level:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Overlay &gt; Device. The Overlay / Device window appears.</td>
<td>Select the Device tab.</td>
</tr>
<tr>
<td>The following details are displayed:</td>
<td>The following details are displayed:</td>
</tr>
</tbody>
</table>

- Device Name - Click the I icon to get the device overview. It displays the following information:
  - Ports
  - Host IP
  - Admin status
  - Oper Status
  - vPC Enabled
  - Number of VMs - Click on the i icon to get more details on the VM.

- Device IP
- Auth Group
Viewing Virtual Machine Details

To view Virtual Machine details:

Go to Overlay > Virtual Machines. The Overlay / Virtual Machines window appears. The following details are displayed:

- VM Name
- IP Address
- Status
- Admin State
- MAC Address
- Network Name
- Host IP - Click the i icon for host details.
- VLAN
- UUID

Viewing Baremetal Details

To view baremetal server details:

Go to Overlay > Baremetal. The Overlay / Baremetal window appears. The following details are displayed:

- UUID
- Name
- Status
Viewing Network Details

To view details about the network:

Go to Overlay > Network. The Overlay / Network window appears. The following details are displayed:

- Router Name
- Tenant
- Zone
- UUID
- Status
- Connected Networks
- VNI
- VRF

To edit the network details, select the Network Name check box and click Edit icon.

To delete the network details, select the Network Name check box and click Delete (X) icon.

Viewing Router Details

To view details about the routers in the network:

Go to Overlay > Router. The Overlay / Router window appears. The following details are displayed:
• Router Name
• Tenant
• Zone
• UUID
• Status
• Connected Networks
• VNI
• VRF

To edit the router details, select the Router Name check box and click **Edit** icon.

To delete the router details, select the Router Name check box and click **Delete (X)** icon.
Administering Cisco VTS

This chapter has the following topics:

- Setting up System, page 67
- Setting Global Route Reflector, page 68
- Registering the Virtual Machine Manager using GUI, page 68
- Backing up and Restoring Database, page 69

Setting up System

To set up the system:

Step 1  Go to Administration > System Settings. The System Settings page appears.
Step 2  Enter the DHCP Server IP.
Step 3  Enter the AnyCast GW Mac.
Step 4  Specify the Out-of-Sync Commit behavior to control the Check Sync feature. See Synchronizing Configuration, on page 25 for details about the synchronizing configuration using the Config Sync feature. Choose one of the following: Choose:
  - Accept—Check sync feature in network inventory will be disabled.
  - Reject—Check sync feature in network inventory will be enabled.

Step 5  Enter the Default Range for VLAN Pools in the Start and End fields. The default range ranges from 2-4094.
Step 6  Click Submit.
Setting Global Route Reflector

This option enables the system to use the devices in the global router reflector. The devices will not be configured at this time. The BGP configuration are performed at the time of Admin domain/ Functional group time.

To set the global route reflector:

**Step 1**  
Go to **Administration > Route Reflector**. The Route Reflector page appears which shows a list of devices that allows you to choose between Global and Inline settings.

**Step 2**  
Set the Global toggle switch to **Yes** to view the list of all devices that is RR capable.  
**Note** If you set the Global toggle switch to **No**, it means that the route reflector setting is Inline and you do not have the option to select the device because the Route Reflector page displays an empty list.

**Step 3**  
From the **Device Name** drop-down list, select or drag the device(s) that you want to assign or set as global route reflector. You can also view the Device Status and the IP Address.

**Step 4**  
Click **Save**.

Registering the Virtual Machine Manager using GUI

You can register the VMM using the VTS GUI. To do this:

**Note**  
To install the Host Agent in case of an OpenStack environment, you can use the Install Capabilities feature.

**Step 1**  
Go to **Administration > Virtual Machine Manager**.

**Step 2**  
Click the Add (+) button. The Add Virtual Machine Manager popup is displayed.

**Step 3**  
Enter the following details:

- **VMM Type**—Specify the VMM type. Choose vcenter or openstack from the drop-down list.
- **Version Name**—Specify the version details. See Note below for details.
- **Description**—Enter a description for the VMM.
- **IP Address-Port**—If you choose vcenter, enter the IP address and the port. The default port is 443. If you choose openstack, enter the IP address.
- **User Name**—Enter the VMM username.
- **Passphrase**—Enter the VMM passphrase.
Note

1. If VMM Type is `openstack` and Version Name is `openstack-liberty-centos`, a new field VTF Deployment Mode appears in the Add VMM popup.

2. VTF Deployment Mode field had two modes: `vtf-vhost` and `vtf-as-vm`.

3. `openstack-liberty-rhel`, `openstack-icehouse`, `openstack-juno`, and `openstack-kilo` support only VM mode.

4. Openstack-liberty-centos supports both vhost and VM modes.

5. In vhost mode VTF installation has to be done manually.

6. VTF deployment mode can be selected at the time of VMM registration and this cannot be changed later.

7. All the compute in a data center should be either in vhost mode (VTF running as a process) or in vNode mode (VTF running as a VM). Currently VTS does not support mixed mode.

Step 4

Click Save.
The VMM you added is listed in the Virtual Machine Manager screen.
You can check the status of VMM registration in the Status column.
To delete a VMM, select the VMM and click X (delete).

Backing up and Restoring Database

The VTS database may be backed up using the ncs-backup command shown below. You may backup the database periodically using a cron job so that there is always a backup in case of a database corruption.

Note

You can only backup and restore the database to and from the same Cisco VTS version.

To perform a back up:

Step 1

Run:

```
admin@vtc20:~$ sudo /opt/ncs/current/bin/ncs-backup
```

```
INFO Backup /var/opt/ncs/backups/ncs-3.3@2015-12-02T07:28:45.backup created successfully
```

Example of shell script for back-up (Place the script in /etc/cron.daily, and set execute permissions chmod 755):

```
#!/bin/sh
/opt/ncs/current/bin/ncs-backup > /dev/null 2>&1
```

Step 2

To restore VTS database using the backup file, for instance, to a newly installed VTC instance, use the `--restore` option of the ncs-backup command:

You must stop VTS before you restore the database, start after the restore is complete.
For example:
admin@vtc20:~$ sudo -u ncs /bin/bash -c '/opt/cisco/package/vtc/bin/ncs stop'
Stopping ncs: .

admin@vtc20:~$ sudo /opt/ncs/current/bin/ncs-backup --restore /var/opt/ncs/backups/ncs-3.3@2015-12-02T07:28:45.backup
Restore /etc/ncs from the backup (y/n)? y
Restore /var/opt/ncs from the backup (y/n)? y
INFO Restore completed successfully
admin@vtc20:~$ sudo -u ncs /bin/bash -c '/opt/cisco/package/vtc/bin/ncs start'
Starting ncs: .

Restoring VTS database on an HA setup

In an HA setup with two VTCs—VTC1 and VTC2, where VTC1 is the active while VTC2 is the standby:

Step 1 Put pacemaker into maintenance mode. This command may be run from either the active or standby.
admin@vtc1:~$ sudo crm configure property maintenance-mode=true

Warnings found during check: config may not be valid

Step 2 Stop NCS on VTC1.
admin@vtc1:~$ sudo -u ncs /bin/bash -c '/opt/cisco/package/vtc/bin/ncs stop'
Stopping ncs: .

Note NCS need not be stopped on VTC2.

Step 3 Use the ncs-backup restore command to restore the database.
admin@vtc1:~$ sudo /opt/ncs/current/bin/ncs-backup --restore /var/opt/ncs/backups/ncs-4.1.1.3@2016-08-31T03:19:07.backup

Restore /etc/ncs from the backup (y/n)? y
Restore /var/opt/ncs from the backup (y/n)? y
INFO Restore completed successfully

Step 4 Restart NCS on VTC1.
admin@vtc1:~$ sudo -u ncs /bin/bash -c '/opt/cisco/package/vtc/bin/ncs start'
Starting ncs: .

Step 5 On VTC1 NCS CLI, set the HA status.
• If this (VTC1) is the master:

```
admin@vtc1:~$ ncs_cli -u admin
admin connected from 192.0.0.1 using ssh on vtc1
admin@ncs> request ha-cluster role-override-master
status override
[ok][2016-08-31 03:31:56]
admin@ncs> request ha-cluster activate
status activated
[ok][2016-08-31 03:32:02]
```

• If this (VTC1) is standby and this is the original standby, run:

```
request ha-cluster role-revert
```

This reverts the HA role to the configured value. Otherwise, run:

```
request ha-cluster role-override-slave
```

This overrides the configured role to standby. This needs to be followed by:

```
request ha-cluster activate
```

**Step 6**  
Check NCS status using `show ha-cluster`.

```
admin@ncs> show ha-cluster
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vtc1</td>
<td>master</td>
</tr>
<tr>
<td>vtc2</td>
<td>slave</td>
</tr>
</tbody>
</table>

**Step 7**  
Take pacemaker out of maintenance mode. This can be run on either the master or slave node.

```
admin@vtc1:~$ sudo crm configure property maintenance-mode=false
```

Warnings found during check: config may not be valid

**Step 8**  
Check pacemaker status using `sudo crm status`.

```
admin@vtc1:~$ sudo crm status
```


Last change: Wed Aug 31 03:36:02 2016 via cibadmin on vtc1

Stack: corosync

Current DC: vtc1 (1073741834) - partition with quorum

Version: 1.1.10-42f2063

2 Nodes configured

3 Resources configured
Online: [ vtc1 vtc2 ]

ClusterIP (ocf::heartbeat:IPaddr2): Started vtc1

Master/Slave Set: ms_vtc_ha [vtc_ha]
  Masters: [ vtc1 ]
  Slaves: [ vtc2 ]