Cisco Virtual Topology System (VTS) 2.1 User Guide

First Published: September 30, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
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 7
Discovery 8
Inventory 9
Using the Expert Mode—Quick Guide 10
Initial Configuration Tasks 10
Important Notes Regarding VMware vSphere Distributed Switch (VDS) 14
  For Non-VPC Specific Configuration 15
  For VPC Specific Configuration 15

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 22
### Contents

#### Chapter 9

- **Viewing Overlay Details** 45
  - Viewing Device Details 45
  - Viewing Virtual Machine Details 46
  - Viewing Baremetal Details 46
  - Viewing Network Details 47
  - Viewing Router Details 47

#### Chapter 10

- **Administering Cisco VTS** 49
  - Setting up System 49
  - Setting Global Route Reflector 49
  - Registering the Virtual Machine Manager using GUI 50
CHAPTER 1

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 2.1 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.

**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, VTFs) 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 2.1 Installation Guide for the detailed procedure about setting up high availability.
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 10
- Important Notes Regarding VMware vSphere Distributed Switch (VDS), page 14

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: https://<IP Address>:8443/VTS. Cisco VTS supports Google Chrome and Mozilla Firefox browsers. Cisco VTS 2.1 has been tested on Google Chrome version <> and Mozilla Firefox version <>.

Step 2 Enter the username and password, and click Login. The default username and password is admin/admin. The Change Password window appears.

You will be required to change the password for the admin account the first time you are logging in. Click the Password guidelines link for details about the password guidelines.

Step 3 Enter the New Password, and reenter the new password in the Confirm New Password field.

Step 4 Click Change Password.

Note  
- To change your password subsequently, click Change Password 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:
Using the Setup Wizard

The Cisco VTS Setup wizard guides you through a series of steps that help 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.
- **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.
- **Password**—Enter the VMM password.

**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.
- **Password**—This is the login password 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 Password**.

**Step 5**

Click **Start Discovery**.

**Note**

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

- **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 25.

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.

*Note*

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 10 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>
<tbody>
<tr>
<td>Administration</td>
<td>• System Settings</td>
<td>• Setting up System, on page 49</td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine Manager</td>
<td>• Registering the Virtual Machine Manager using GUI, on page 50</td>
</tr>
<tr>
<td>Set up Inventory</td>
<td>• Discover Devices</td>
<td>• Managing Inventory, on page 19</td>
</tr>
<tr>
<td>Admin Domains</td>
<td>Create Admin Domains</td>
<td>Creating an Admin Domain, on page 32</td>
</tr>
<tr>
<td>Set up Tenants</td>
<td>Add Tenants</td>
<td>Adding Tenants, on page 37</td>
</tr>
<tr>
<td>Set up Overlay</td>
<td>• Add Network</td>
<td>Provisioning Overlay Networks, on page 39</td>
</tr>
<tr>
<td></td>
<td>• Define Baremetal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add Routers</td>
<td></td>
</tr>
</tbody>
</table>

**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>
<tr>
<td></td>
<td></td>
<td>For more information about creating authorization group, see Managing Users and Groups, on page 17</td>
<td></td>
</tr>
<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, 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, 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, see Administering Cisco VTS, on page 49.</td>
<td></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>5</td>
<td>Perform IOS XRv and VTF Registration. <strong>Note</strong> This step is required only if you have a VTF-based deployment.</td>
<td>See the <em>Installing the Virtual Topology Forwarder</em> section in the <em>Cisco VTS 2.1 Installation Guide</em>.</td>
<td>IOS XRv takes a few minutes to boot. Register the VTF only after you see the VFG group on the GUI. To verify that the VFG group is created, go to Inventory &gt; Virtual Forwarding Groups.</td>
</tr>
<tr>
<td>6</td>
<td>Login into the IOS XRv and verify that the network-controller config is pushed. <strong>Note</strong> This step is required only if you have a VTF-based deployment.</td>
<td></td>
<td></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>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>
</tbody>
</table>
|          | Create resource pools | • Resource Pools > Global VNI Pool  
• Resource Pools > Device Specific VLAN Pools  
• Resource Pools > Multicast IP Pool |  For more information about creating an admin domain, see Managing Resource Pools, on page 27 |
| 8        | Create an Admin Domain | Admin Domains > Domains  
For more information about creating an admin domain, see Creating and Managing Admin Domains | Properties for the L2/L3 Gateway Group are as follows:  
• Control Protocol: BGP-EVPN  
• Replication Modes: Multicast and Ingress  
• Distribution Mode: Decentralized |
Important Notes Regarding VMware vSphere Distributed Switch (VDS)

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

- 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.</td>
</tr>
<tr>
<td></td>
<td>See VMware documentation for the detailed procedure.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a Link Aggregation Group for each VDS.</td>
</tr>
<tr>
<td></td>
<td>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>
CHAPTER 3

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

To create users:

Step 1 Click Administration > User Management. The Administration / User Management window appears.

Step 2 Click Add (+) icon. The Add New User popup window appears.

Step 3 Enter the User Name and Password, and then select the desired role from the Role drop down list.

Step 4 Click Save.

The user details get added to the Users 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 passwords). 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/password 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 22
- Viewing Network Inventory, page 23
- Viewing Host Inventory, page 24
- Viewing the IOS XRv to VTF Mapping, page 26

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.
- **Password**—This is the login password 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 password to each host entry. This update is required for installation of the host-agent (in case of OpenStack) and any subsequent password 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 Password**.

**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.

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

---

**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.

**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**.

**Note**  
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 14 section for details.

---

**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. 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`.

---

**Viewing the Network Topology**

Topology window provides a view of the data center fabric controlled by Cisco VTS. It displays the leaves, 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.

---

**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.

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

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.

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 25.

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
- Host Interface
- Host IP Address
- Device Port Name
- Connection ID
• Capability—The host capability - Physical or Virtual.

• Status—Shows the installation status.

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 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 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
    • Host Interface
    • Device Port Name
    • Capability—Specify whether it is a virtual-switch ir not.
    • Username
    • Password

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

  ° VTF IP—The IP address of the VTF.
  ° Subnet Mask
  ° Gateway
Tenant Bridge—Name of the tenant network port group/bridge on the binding-host to which VTF is attached.

Underlay Bridge—Name of the underlay network portgroup/bridge on the binding-host to which VTF is attached.

Datastore

Username

Password

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

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.

---

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.
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 27
- Specifying VLAN Pool Range, page 28
- Specifying Multicast IP Pool, page 29

### Specifying Global VNI Pool Range

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

**Step 1**

**Step 2**
Click the **Add (+) icon**. Specify the ranges, and click **Save**.
To edit the range, select the Range From check box, and click the **Edit** icon as required.
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 28
- Specifying Group VLAN Pool Range, on page 29

Specifying Device VLAN Pool Range

To specify device VLAN pool:

Step 1

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
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:

Step 2  Click Groups
Step 3  Click the Add (+) icon. The Add Group pop up window appears.
Step 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.
To view the devices associated with a group, select the group and click Associated Devices.
Step 5  Click Save. The group gets created and is listed in the table.
Step 6  To add range to the group, select the group and click the Add (+) icon.
Step 7  Specify the From and To values.
Step 8  Click Save.
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.

Step 2  Click the Add (+) icon, and enter the Netmask values.
Click the Question Mark (?) icon to view the Multicast IP address range.
Step 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 31
- Viewing Admin Domain, page 32
- Creating an Admin Domain, page 32

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

See for detailed information about creating Admin Domains.

The design validated in this release has:

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

**Viewing Admin Domain**

The Admin Domains home page lists all the Admin Domains that you have created. It provides the option to create a new Admin Domain. It also displays the status of the Admin Domains. You can also edit an Admin Domain.

To view admin domains:

---

**Step 1**

Go to **Admin Domains > Domains**.
The Admin Domains / Domains window appears.
You can see two types of views on the Admin Domain page. The two types of views are as follows:

- List view
- Tree view

**Step 2**

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

---

**Creating an Admin Domain**

To create an admin domain:

**Before You Begin**

- Ensure that you have created authorization groups populated with the correct credentials.
- 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>

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 DC GW</td>
<td>DC GW is a border leaf. <strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 L3 GW</td>
<td>A group of all L3 devices that can be within an admin domain and that particular device share a particular property or same functionalities. <strong>Note</strong> An admin can create a logical L3 groups and map devices that will exhibit a similar policy behavior under this group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 L2 GW</td>
<td>A group of all L2 devices that can be within an admin domain and that particular device share a particular property or same functionalities. <strong>Note</strong> An admin can create a logical L2 groups and map devices that will exhibit a similar policy behavior under this group.</td>
</tr>
</tbody>
</table>

**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>
<tr>
<td>DC GW</td>
<td>• New or Shared DC GW. • Control Protocol - BGP EVPN.</td>
</tr>
</tbody>
</table>
### Functional Group

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

### L2 GW

<table>
<thead>
<tr>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New and Shared L2 GW.</td>
</tr>
<tr>
<td>• Control Protocol - BGP EVPN.</td>
</tr>
<tr>
<td>• Replication Mode - Multicast or Ingress.</td>
</tr>
<tr>
<td>• Distribution Mode - Decentralized.</td>
</tr>
<tr>
<td>• ARP Suppression - On.</td>
</tr>
</tbody>
</table>

---

**Step 6**

Assign Devices for each function 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 Tenants

This chapter has the following section:

- Adding Tenants, page 37

Adding Tenants

To add tenants:

Step 1  Go to Tenants > Tenant Management. The Tenant Management window appears.
Step 2  Click Add (+) icon.
Step 3  Enter the following:
    - Name
    - Description
Step 4  Click Save.
Step 5  To add a Zone, click the Add (+) icon. The Add Zone popup appears.
Step 6  Enter the zone name, and click OK.
Step 7  Click Save.
Provisioning Overlay Networks

This chapter has the following sections:

- Provisioning Overlay Networks Using Cisco Virtual Topology System, page 39
- Creating Overlays, page 40
- Creating Network using VMware, page 41
- Creating Subnetwork using VMware, page 42
- Creating Routers using VMware, page 42
- Attaching Network to Router, page 42
- Attaching a Virtual Machine to Network, page 43
- Creating a Network using Cisco VTS GUI, page 43
- Creating Router using Cisco VTS GUI, page 44

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 2.1 Installation Guide for details.
- Discover the network topology in the data center. See the Managing Inventory chapter of the Cisco VTS 2.1 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 leaves, 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 42
• Creating Network using VMware, on page 41
• Creating Subnetwork using VMware, on page 42
• Creating Routers using VMware, on page 42
• Attaching a Virtual Machine to Network, on page 43

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 43
• Creating Router using Cisco VTS GUI, on page 44

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:

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

Creating Routers using VMware

Step 1  Select one of the VDS switches you had created, then click the Manage tab.
Step 2  Select Cisco VTS Router tab, and click Add (+) to add the Router.
Step 3  Select Tenant Name and enter the Router Name.
Step 4  Click Create Router button to create the router.

Attaching Network to Router

To attach a network and subnetwork to a router:

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

To create VMs:

**Step 1** Create network and subnet using vCenter Cisco VTC plugin. This will create portgroup for the network.

**Step 2** 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.

Creating a Network using Cisco VTS GUI

To create a network from the Cisco VTS GUI:

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

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

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

**Step 4** Select the Zone.

**Step 5** Enter the network name.

**Step 6** 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 7** 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.
Attach a Port

To add a port:

Step 1  Click Port Attach. The Add Port popup appears.
Step 2  Specify whether it is a Physical Device or a Virtual Device, by selecting the appropriate radio button.
Step 3  Enable Tagging by selecting the Tagging check box.
Step 4  Select the device from the drop-down list.
Step 5  Select the Port, then click OK.

Creating Router using Cisco VTS GUI

To create a router using Cisco VTS GUI:

Step 1  Go to Overlay Provisioning > 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 the Router Name.
Step 6  Select the router gateway from the Router Gateway drop-down list.
        You can also add multiple interfaces and select the subnet you need to add an interface to.
Step 7  Click Add (+) icon. The Add Interface popup appears.
Step 8  Select the subnet from the drop down list, and click OK.
Step 9  Click Submit in the Add Router window to save the router and its interface.
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 45
- Viewing Virtual Machine Details, page 46
- Viewing Baremetal Details, page 46
- Viewing Network Details, page 47
- Viewing Router Details, page 47

Viewing Device Details

To view details at device level:

Step 1  Go to Overlay > Device. The Overlay / Device window appears.
Step 2  Select the Device tab.

The following details are displayed:

- 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
• Admin State
• Network Name
• IP Address
• Binding Host
• VLAN Number
• Tenant Name

**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:
Viewing Router Details

- 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.
This chapter has the following topics:

- Setting up System, page 49
- Setting Global Route Reflector, page 49
- Registering the Virtual Machine Manager using GUI, page 50

### Setting up System

To set up the system:

**Step 1**
Go to Administration > System Settings.
The System Settings page appears.

**Step 2**
Enter the Domain ID.

**Step 3**
Enter the DHCP Server IP.

**Step 4**
Enter the AnyCast GW Mac.

**Step 5**
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. See *Installing OpenStack Host Agent and VTF using GUI*, on page 25 for details.

**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.
- **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.
- **Password**—Enter the VMM password.

**Step 4**
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.
To delete a VMM, select the VMM and click **X** (delete).