Provisioning Overlay Networks

This chapter has the following sections:

- Provisioning Overlay Networks Using Cisco Virtual Topology System, page 1
- Creating Overlays, page 2
- Creating Network using VMware, page 4
- Creating Subnetwork using VMware, page 4
- Creating Routers using VMware, page 4
- Attaching Network to Router, page 5
- Attaching a Virtual Machine to Network, page 5
- Creating a Network using Cisco VTS GUI, page 5
- Creating Router using Cisco VTS GUI, page 7
- Assigning BVI Interface IP Address, page 9
- Extending Layer 2 Network Across Data Centers, page 9
- Enabling Global Route Leaking Service, page 10
- Enabling L3VPN to EVPN Route Stitching, page 12

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 multideestination 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, VTSR, 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.

Cisco VTS supports dual stack IPv4 and IPv6 addressing for overlay provisioning.

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 5
• Creating Network using VMware, on page 4
• Creating Subnetwork using VMware, on page 4
• Creating Routers using VMware, on page 4
• Attaching a Virtual Machine to Network, on page 5

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 5
• Creating Router using Cisco VTS GUI, on page 7
## Creating Network using VMware

To create a network:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select one of the vDS switches you created, then select Manage tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the Cisco VTS Network tab and click Add (+) to add the network.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select create Tenant and enter Network Name field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Create to create the network.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the Refresh icon to display the created network.</td>
</tr>
</tbody>
</table>

## 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 1</th>
<th>Select one of the vDS switches you had created, then click the Manage tab.</th>
</tr>
</thead>
<tbody>
<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 1</th>
<th>Select one of the vDS switches you had created, then click the Manage tab.</th>
</tr>
</thead>
<tbody>
<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:

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

**Step 3** Click **Add (+)** icon.

**Step 4** Enter the network name. This is mandatory.

**Step 5** Specify whether you want this to be an external network using the External Network toggle switch.

**Step 6** From the **Extend Network** drop down, select L2 or L3, depending on your requirement. If you select L2, VPN Service becomes available for use. For the L2 Extended Network, click the **L2VPN** tab and enter the EVI number. This can be an integer between 1 and 65534. Select the Load Balance Per EVI check box to introduce the load balance CLI in the device. See Extending Layer 2 Network Across Data Centers, on page 9. To extend an L3 network, choose L3 from the drop-down.
Creating a Subnetwork

To create a subnetwork:

Step 1 Click Add (+) in the Subnet pane of the Add Network page.
Step 2 Enter the subnet name. Only IPv4 / IPv6 addresses, alphabets, space, numbers, and special characters /, -, and _ are allowed.
Step 3 Enter the IP details. You can enter an IPv4 or IPv6 address. You must ensure that the network address and the gateway IP are in sync.
Step 4 Click OK.
The table displays the Subnet Name, Network Address, Gateway IP, and the IP Version (whether IPv4 or IPv6).

Attaching a Port

To do a port attach:

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 at the device level to be used for port attach. By default, VTS allocates a free VLAN from its pool 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**
- If the device is a Cisco Nexus 7000 series switch, the Interface VLAN column appears in the table. You can provide the interface VLAN you have specified in the Resources > Device > Interfaces page. If you do not specify an interface VLAN, Cisco VTS automatically chooses a VLAN from its pool.
- 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 the Static VNI. This can be an integer number between 4096 and 65535

**Step 6** Enter the **Router Name**.

**Step 7** Select a template that you might want to associate with the router, using the find icon in the Template field. See [Attaching Templates while Adding Routers](#) for details.

**Step 8** 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 VTSR 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 VTSR configuration, a similar error is displayed if the default VRF name exceeds 24 characters.

• VRF name change from VTS GUI is not supported for VTSR. Cisco VTS does not allow changing the name of a router if it connects to a port on a V node. (A V node is compute node where there is a VTF present, and the workload is behind a VTF where the VXLAN Tunnel originates.)

• 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.

Step 9
Select the router gateway from the **Router Gateway** drop-down list. When you select External GW from dropdown, two additional fields for Router Gateway IPv4 and Router Gateway IPv6 get displayed. These are optional.

When you select Router Gateway, the Advertise Default Route toggle switch is displayed. It is enabled by default. When it is enabled, the default routes are pushed on the DC gateway device in VRF-Peering mode and on the DCI device in integrated mode. For example:

```bash
router static
vrf t1-rout
  address-family ipv4 unicast
    0.0.0.0/0 Null0 254
  exit
  exit
router bgp 100
vrf t1-rohi-rout
  rd 2.2.2.11:10009
  address-family ipv4 unicast
    label mode per-vrf
    maximum-paths ebgp 2
    maximum-paths ibgp 2
    network 0.0.0.0/0
    aggregate-address 3.2.3.0/24 summary-only
    redistribute connected
  exit
address-family ipv6 unicast
  label mode per-vrf
  redistribute connected
```

When set to No, the default routes are not pushed.

Step 10
If the router is used to add shared networks from different tenants as interfaces, set the **Provider Router** toggle switch to Yes.

Step 11
Click **Add (+) icon**. The Add Interface popup appears.

Step 12
Select the subnet from the drop down list, and click **OK**.

Step 13
Click **Save** in the Add Router window to save the router and its interface.
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.

Extending Layer 2 Network Across Data Centers

If there are multiple data center PODs managed separately, (one instance of Cisco VTS managing only one POD) and connected over the WAN/core using a BGP-EVPN MPLS cloud, the L2VNI routes can be distributed from within the BGP-EVPN VXLAN fabric by stitching them to BGP-EVPN MPLS routes over the WAN/core side. On the other side (POD) the BGP-EVPN MPLS routes can be stitched onto BGP-EVPN VXLAN routes.

To complete the L2VNI extension workflow:
Enabling Global Route Leaking Service

The global route leaking feature enables you to provide internet/external connectivity to the host inside the Data Center. This feature allows associating/dissociating of Global Route Leaking (also known as Global Routing Table [GRT]) Service to/from the Overlay Router. Once the Overlay Router gets realized (that is, when port attach happens on interface), VTS pushes the policies configured as part of GRT associated to a router. Route policies for core facing/external facing routes and route policies for fabric facing/internal routes will be pushed.

Note
Global Route Leaking feature is available only when an external router gateway is selected.

Router cannot get deleted if the GRT is still attached. Admin needs to disassociate the GRT profile before deleting the router.

You can add create and enable global route leaking service while you create a router, or at any other point in time.

Step 1 Configure the import and export route policy on DCI and perform a sync from. For example:

```
route-policy data-center-vrf-export-policy
  if destination in (101.1.1.0/24 eq 32, 102.1.1.0/24 eq 32, 103.1.1.0/24 eq 32, 104.1.1.0/24 eq 32, 105.1.1.0/24 eq 32) then
```
Provisioning Overlay Networks

Enabling Global Route Leaking Service

```
  pass
def if destination in (60.0.0.0/24) then
    pass
  end-if
end-policy
```

See Synchronizing Configuration for details about performing a sync from operation.

**Step 2**  
Create Fabric and Core Facing Route Policy (underlay policy for Internet connectivity). This is not mandatory. For example:
```
route-policy vts-route-policy
  pass
end-policy
```

**Step 3**  
Create Profile for Internet from Admin Domains > DCI Interconnect Profiles. See Creating DCI Interconnect Profiles.

**Step 4**  
Attach the internet profile to DCI in the admin domain. Configuration is pushed by VTS on saving the admin domain. For example, the below configuration, which has the neighbor details, will be pushed under router BGP on the DCI.
```
router bgp 200
  bgp router-id 18.18.18.18
  neighbor 5.1.1.1
    remote-as 400
    ebgp-multihop 255
    update-source Loopback2
    address-family ipv4 unicast
      route-policy vts-route-policy in
      route-policy vts-route-policy out
```

**Step 5**  
Go to Overlay > Router. The Overlay / Router window appears.

**Step 6**  
Click Add (+). The Add Router page is displayed.

**Step 7**  
Click Global Route Leaking tab. 

*Note*  
Ensure that you have chosen an external router gateway as the Router Gateway.

**Step 8**  
Click Add (+). The New Global Route Leaking popup window appears.

**Step 9**  
Enter a name (this is mandatory), and description.

**Step 10**  
In the Policies pane, enter at least one policy for the address family. 

*Note*  
Ensure that this policy exists on the device. Policy names will be validated from the device. If policy names are wrong, VTS will throw an error.
- Import Policy Name—Route policy to control import of routes from Global Routing Table (GRT).
- Export Policy Name—Route policy to control export of routes to GRT.

**Step 11**  
Click Add. The Global Route Leaking service gets added. You can click on the name to get a summary of the global route leaking service you created.

**Step 12**  
Click Save. Once the service is attached to the router, all the networks for the router will be leaked outside. To disassociate the service you need to select the Detach button and save the edit.
Enabling L3VPN to EVPN Route Stitching

L3VPN to EVPN route stitching feature provides the capability to exchange the routes from core towards the data center and vice versa. EVPN is used inside the data center whereas L3VPN is used as an interconnect between two data centers.

**Note**
As a prerequisite, you must create an external network and extend to L3. You must then attach the router interfaces to the external network. See [Creating a Network using Cisco VTS GUI](#) on page 5 and [Creating Router using Cisco VTS GUI](#) on page 7 sections for details.

---

**Step 1**
Configure BGP VPNv4/v6 neighbor using Device Templates. A single template can be used for all the neighbors, or you can have a template each for each neighbor. Create the template at [Templates > Device Template Management](#). Attach the template to the DCI. See [Managing Templates](#) chapter for details.

**Step 2**
Create an External Route Stitching Template. Choose the routes which you want to leak between your core and EVPN, or vice versa. Create the template at [Templates > Overlay Template Management](#) (use the Fabric External RT option). Attach the template to the DCI.