Configuring Layer 2 Features on Virtual Networks

This chapter contains the following sections:

Configuring Private VLANs

Information About Private VLANs

Private VLANs are implemented in OpenStack by configuring provider network and policy profiles. The primary VLAN should be specified by the provider network profile, while the secondary VLAN should be specified in the policy profile. When the policy profile is selected for a VM interface, the interface is attached to the corresponding secondary VLAN.

Configuring a Private VLAN

The following section guides you through the private VLAN configuration process. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Procedure

Step 1 Enable or disable the PVLAN feature globally. For more information, see the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide*.

Step 2 Configure one or more VLANs as primary VLAN(s) on the VSM. For more information, see the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide*.

Step 3 Configure a VLAN as a secondary VLAN on the VSM. For more information, see the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide*.

Step 4 Associate secondary VLANs to a PVLAN. For more information, see the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide*.

Step 5 Configure PVLAN port profiles for each secondary VLAN on the VSM. For more information, see the *Cisco Nexus 1000V for KVM Port Profile Configuration Guide* .

Step 6 Create a network segment in OpenStack for each PVLAN. For more information, see Creating a Primary VLAN in OpenStack, on page 2.

Guidelines and Limitations

Private VLANs in OpenStack have the following configuration guidelines and limitations:

- Restrict the policy profile scope to tenants unless the usage of policy profiles can be validated by the orchestration system.

- When a PVLAN policy profile is selected, the association between the secondary VLAN in the policy profile to the primary VLAN in the network is not validated.

- Do not publish policy profiles without secondary VLAN configuration on regular tenants in a PVLAN environment unless it can be validated by the orchestration system. Using policy profiles without secondary VLANS on primary VLAN segments result in promiscuous access to the VLAN.

Creating a Primary VLAN in OpenStack

Command	Purpose
For Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.2) and higher: **neutron cisco-net-create** *name* **--provider:network_type vlan --provider:physical_network** *network* **--provider:****segmentation_id vlan_id* For all other releases: **neutron cisco-network-profile-create** *name* **vlan --segment_range***private-VLAN **--physical_network** *network*	Creates a VLAN network profile. For more information about this command, see the cisco-network-profile-create command reference page. You can also create the network profile using the OpenStack dashboard. For more information, see Creating a Network Profile Using the OpenStack Dashboard.

Command	Purpose
neutron net-create *name* **--n1kv:profile_id** *networkProfileId***--shared** **Note** Starting from Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.2), **--n1kv:profile_id** has been replaced with **--n1kv:profile**.	Creates a network with a primary VLAN as the network ID and makes the network available to all tenants. For more information about this command, see the net-create command reference page. You can also create the network using the OpenStack dashboard. For more information, see Creating a Network Using the OpenStack Dashboard.
neutron subnet-create *network-name IP-address-range* **--name** *subnet-name*	Attaches a subnet to the network. For more information about this command, see the OpenStack documentation. You can also create a subnet using the OpenStack dashboard. For more information, see Creating a Subnet for a Network Using the OpenStack Dashboard.

Before You Begin

Create a primary VLAN on the VSM. For more information, see the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide*.

The following example shows how to create a Primary VLAN network of VLAN 100 with subnet 10.10.10.0/24:

```
$
$ neutron cisco-network-profile-create primary100pool vlan --segment_range 100-100
--physical_network physnet1
$ neutron net-create primary100 --n1kv:profile_id a9355268-5aed-8030-f3ab-e367ef4c9acc
--shared
$ neutron subnet-create primary100 10.10.10.0/24 --name subnet1
$
```

Note   The profile_id in the neutron net-create command refers to the network profile ID. The profile_id in the neutron port-create command refers to the policy profile ID.

Associating a Feature Profile of a Secondary VLAN to a Tenant

You can limit the scope of a feature profile to selected tenants by setting the restrict_policy_profiles variable in the cisco_plugins.ini file. For more information on how to set this variable in OpenStack, see the OpenStack documentation.

Tenants can access the secondary VLANs that are associated with the other tenants. Hence, in a private VLAN environment, it is recommended to associate a feature profile to selected tenants unless the orchestration system can perform the validation of policy-profile usage by a tenant.

Before You Begin

- Create a feature profile for the secondary VLAN on the VSM. For information on how to create a feature profile, see the Configuring a Port Profile as a Private VLAN section in the *Cisco Nexus 1000V for KVM Port Profile Configuration Guide, Release 5.x*.

- Confirm that the feature profile is available in the cisco_plugins.ini file. For more information on the cisco_plugins.ini file, see the Configuring Additional Parameters in the cisco_plugin.ini File section in the *Cisco Nexus 1000V for KVM Installation Guide, Release 5.2(1)SK3(2.1)*.

Procedure

	Command or Action	**Purpose**
Step 1	**neutron cisco-policy-profile-update** *feature_profile_name* **--add-tenant** *tenant-id*	Associates the feature profile to the tenant. For more information on this command or to disassociate the feature profile from a tenant, see the cisco-policy-profile-update command reference page. **Note** This command is not available in Cisco Nexus 1000V Release 5.2(1)SK3(2.2).

The following example shows how to associate the secondary101 feature profile to the tenant ID 8d53387cb36e4475813b09bd53beaa00:

```
$
$ neutron cisco-policy-profile-update secondary101 --add-tenant
8d53387cb36e4475813b09bd53beaa00
$
```

Note   The same feature profile can be associated with multiple tenants by issuing the same command for each tenant. This is useful if the secondary VLAN is an isolated VLAN.

Feature History for Private VLAN

Feature Name	Release	Feature Information
Private VLANs	5.2(1)SK3(2.1)	This feature was introduced.

Configuring VLAN Trunk vEthernet Ports

The following section guides you through the VLAN trunk configuration process for vEthernet ports. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Procedure

Step 1 Create a vEthernet trunk port profile. See the "Configuring a Trunk Policy Profile for a vEthernet Port" section in the *Cisco Nexus 1000V Port Profile Configuration Guide* .

Step 2 Create a VLAN network in OpenStack. See Configuring Virtual Networks Using OpenStack.

Step 3 Configure a VM or Cisco Cloud Services Router (CSR) interface and specify the trunk port profile and network you configured in the previous steps. Note that the native VLAN of the trunk port will be set to the segment ID of the VLAN network that was created in Step 2.

After the VM or CSR port appears in the VSM and VEM, the port is identified as a trunk port and can carry traffic for all the tenant VLANs.

Note
- The native VLAN of the trunk port will be set to the segment ID of the VLAN network created in Step 2.

- Trunk native VLAN configuration in policy profile is not supported. If configured, the effective native VLAN for a vEthernet trunk port is set to the segment ID of the VLAN network created in Step 2.