Configuring VLANs

This chapter contains these sections:

- About Private VLANs over VXLAN, on page 1
- Guidelines and Limitations for Private VLANs Over VXLAN, on page 2
- Configuration Example for Private VLANs, on page 2

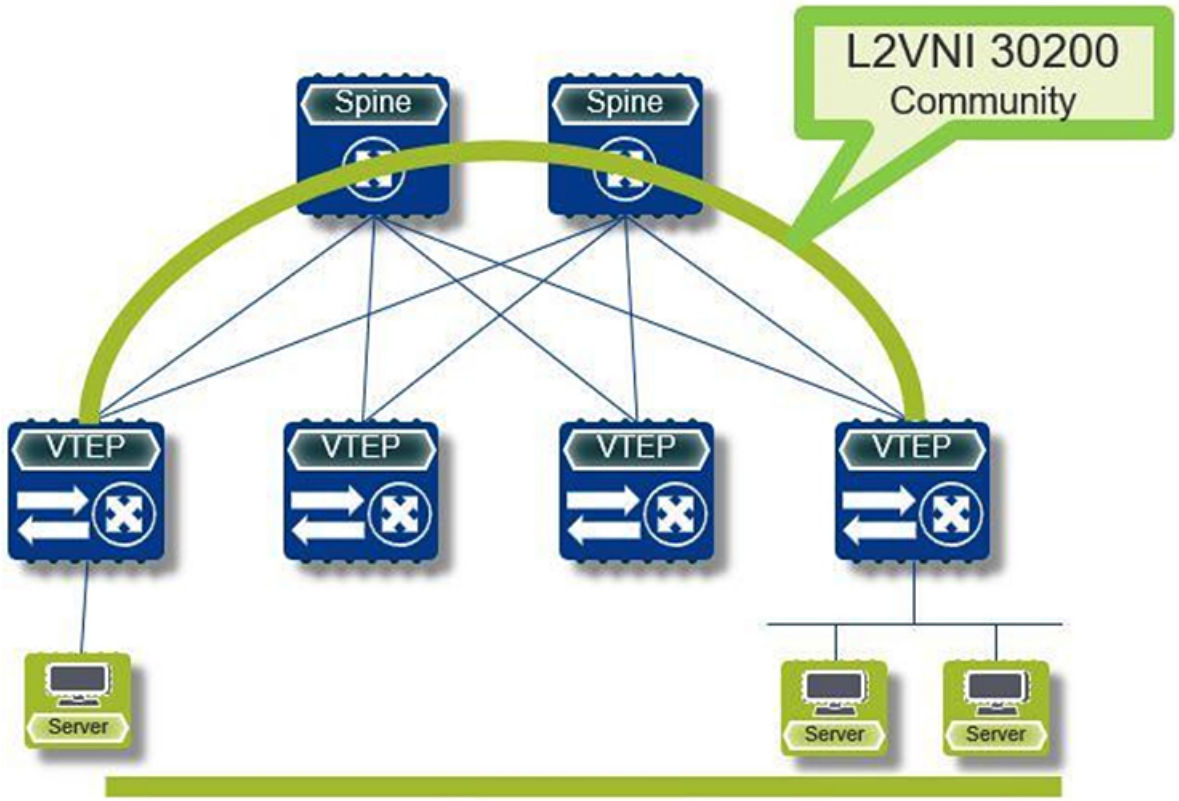
About Private VLANs over VXLAN

Beginning with Cisco NX-OS Release 9.2(3), support added for vPC Fabric Peering. For more information, see the Configuring vPC Fabric Peering chapter.

The private VLAN feature allows segmenting the Layer 2 broadcast domain of a VLAN into subdomains. A subdomain is represented by a pair of private VLANs: a primary VLAN and a secondary VLAN. A private VLAN domain can have multiple private VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

Private VLANs over VXLAN extends private VLAN across VXLAN. The secondary VLAN can exist on multiple VTEPs across VXLAN. MAC address learning happens over the primary VLAN and advertises via BGP EVPN. When traffic is encapsulated, the VNI used is that of the secondary VLAN. The feature also supports Anycast Gateway. Anycast Gateway must be defined using the primary VLAN.

Figure 1: L2VNI 30200 Community



Guidelines and Limitations for Private VLANs Over VXLAN

Configuration Guidelines and Limitations

Follow these guidelines and limitations when configuring Private VLANs over VXLAN.

- The following platforms support private VLANs over VXLAN:
  - Cisco Nexus 9300-EX platform switches
  - Cisco Nexus 9300-FX/FX2 platform switches
- Flood and learn underlay is not supported.
- Fabric Extenders (FEX) VLAN cannot be mapped to a private VLAN.
- vPC Fabric Peering supports private VLANs.

Configuration Example for Private VLANs

This section provides a configuration example for private VLANs.

This section describes a sample configuration for private VLANs, including primary, isolated, and community VLANs, as well as interface and NVE settings.

- The configuration includes definitions for primary, isolated, and community VLANs, and their associations.
- Interface and NVE settings are shown for mapping and forwarding traffic in a private VLAN environment.

```
vlan 500
  private-vlan primary
  private-vlan association 501-503
  vn-segment 5000
vlan 501
  private-vlan isolated
  vn-segment 5001
vlan 502
  private-vlan community
  vn-segment 5002
vlan 503
  private-vlan community
  vn-segment 5003

vlan 1001
  !L3 VNI for tenant VRF
  vn-segment 900001

interface Vlan500
  no shutdown
  private-vlan mapping 501-503
  vrf member vxlan-900001
  no ip redirects
  ip address 50.1.1.1/8
  ipv6 address 50::1:1:1/64
  no ipv6 redirects
  fabric forwarding mode anycast-gateway

interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  no ip redirects
  ip forward
  ipv6 forward
  ipv6 address use-link-local-only
  no ipv6 redirects

interface nve 1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback0
  member vni 5000
    mcast-group 225.5.0.1
  member vni 5001
    mcast-group 225.5.0.2
  member vni 5002
    ingress-replication protocol bgp
  member vni 5003
    mcast-group 225.5.0.4
member vni 900001 associate-vrf
```

Note If you use an external gateway, the interface towards the external router must be configured as a PVLAN promiscuous port

```
interface ethernet 2/1
switchport
switchport mode private-vlan trunk promiscuous
switchport private-vlan mapping trunk 500 199,200,201
exit
```