



Traffic Inspection with Smart Switches in VXLAN EVPN Fabric

- [Traffic Inspection with Smart Switches in VXLAN EVPN fabric, on page 1](#)

Traffic Inspection with Smart Switches in VXLAN EVPN fabric

The N9300 Smart Switch can be used as a leaf switch in VXLAN EVPN fabrics to inspect unicast IPv4 and IPv6 traffic (in service VRFs or VLANs) arriving from hosts, remote leaf switches or border gateways. Smart Switches may also be used as border leaf switches or Multi-Site Border Gateways to inspect traffic arriving from remote sites.

When Smart Switches are used as VXLAN leaf switches, traffic for service VRFs and VLANs, arriving from the hosts, is inspected at the encapsulating smart-switch VTEP. After traffic inspection, the traffic is encapsulated and forwarded through the fabric to the destination VTEP. The destination smart-switch VTEP, decapsulates the traffic and then inspects the traffic for the service VRFs and VLANs. After traffic inspection, traffic is forwarded as usual to the destination hosts. Transit traffic arriving on fabric-facing interfaces is not subjected to traffic redirection.

In VXLAN EVPN topologies, the default VRF serves as the underlay VRF. This VRF is reserved for the transport of VXLAN-encapsulated traffic; it is not designed to support tenant endpoint connectivity. Consequently, we recommend not configuring the default VRF as a service VRF for Smart Switches. However, if you configure the default VRF as a service VRF, these limitations apply:

- Network connectivity for tenant VRFs and VLANs that do not require traffic inspection can be disrupted due to VRF isolation mechanisms.
- vPC fabric peering does not function correctly in this configuration.
- Inter-VRF traffic filtering between hosts in the default VRF and the non-default VRF does not work.

For more information about VXLAN EVPN fabric support, refer to the *Configure VXLAN BGP EVPN* chapter in the [Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide](#).

