

Configure DHCP Snooping

 For supported software information, click [here](#).

You can configure Dynamic Host Control Protocol (DHCP) snooping on Layer 2 devices to identify and monitor unauthorized DHCP servers and prevent them from offering IP addresses to DHCP clients.

DHCP snooping classifies ports as either trusted or untrusted. A trusted port is one that is identified as having legitimate DHCP servers attached to it and is thus allowed to send DHCP requests and acknowledgements. An untrusted port is one that can only forward DHCP requests. By default, Layer 2 ports are untrusted. You must configure them to be DHCP trusted ports.

When you configure an incoming port as a DHCP trusted port, the port accepts DHCP response and acknowledgement (ACK) packets from the DHCP server. If the incoming port is not a trusted port, DHCP snooping does not forward DHCP server packets to clients. Instead, the port drops the packets and raises an alarm.

DHCP snooping inspects DHCP messages sent from untrusted hosts and builds a DHCP snooping table (also called a binding table), which lists the bindings between IP addresses and MAC addresses. The switch then uses the entries in the DHCP snooping table to filter DHCP server messages from untrusted ports so that it can protect the integrity of legitimate DHCP servers.

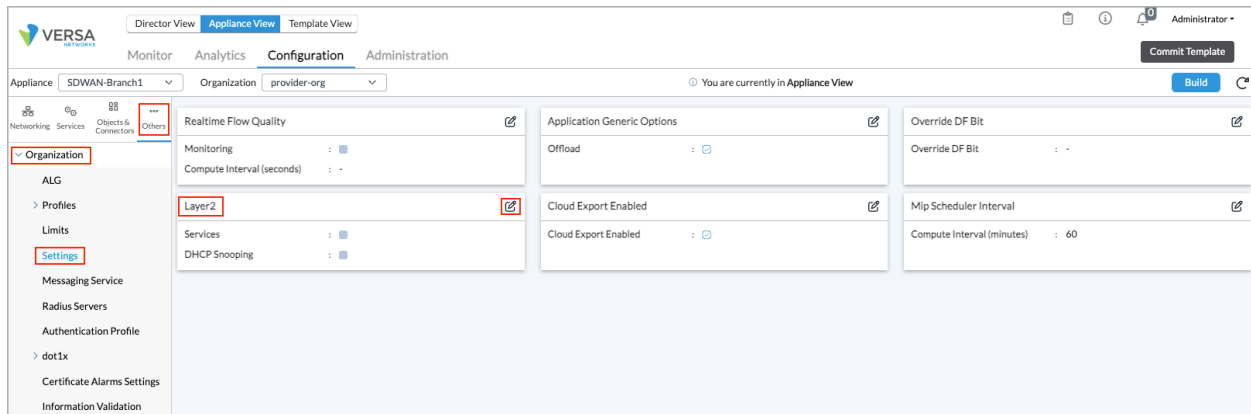
A Versa Operating System™ (VOS™) device validates all DHCP packets that it receives from both the client and DHCP server before forwarding them to the DHCP server.

Enable Layer 2 Services

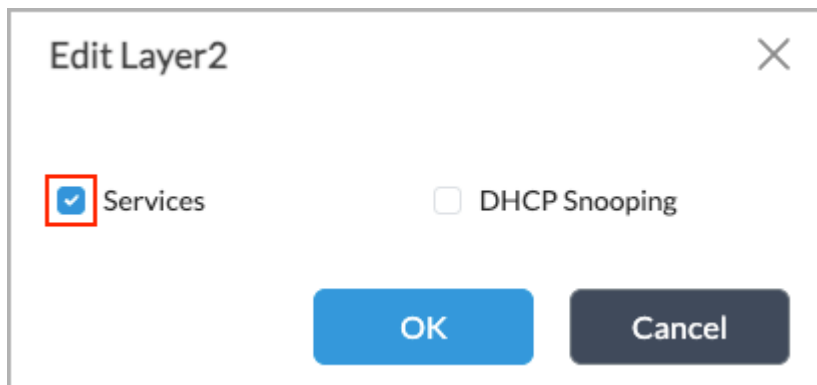
Before you configure DHCP snooping, you must enable Layer 2 services at the organization level.

To enable Layer 2 services:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select Configuration in the top level menu.
3. Select Others > Organization > Settings in the left menu bar.



4. Click the  Edit icon in the Layer 2 pane. The Edit Layer 2 popup window displays.



5. Click Services.
6. Click OK.

Configure DHCP Snooping for a Virtual Switch

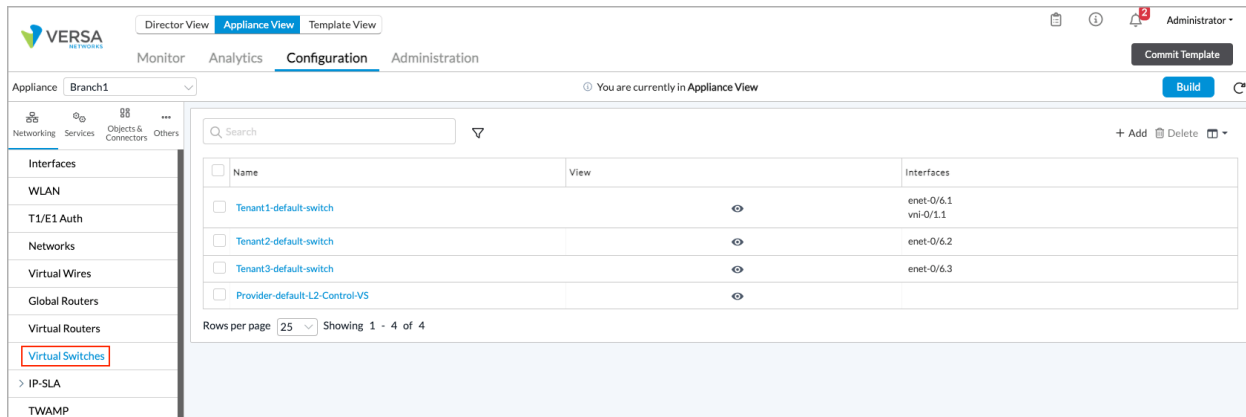
For Releases 22.1.4 and later.

You can configure DHCP snooping for virtual switches and bridge domains. If you configure DHCP snooping for both, the bridge domain configuration takes precedence.

To configure DHCP snooping for a virtual switch:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Switches in the left menu bar. The main pane displays a list of virtual switches that are already configured.




4. Click the **+** Add icon. In the Configure Virtual Switch popup window, select the Virtual Switch Details tab, and then enter information for the following fields.

The 'Configure Virtual Switch' popup window is shown with the 'Virtual Switch Details' tab selected. The form contains the following fields and sections:

- Instance Name ***: Text input field.
- Description**: Text input field.
- Instance type**: Dropdown menu with 'Virtual Switch' selected.
- EVPN Service Type**: Dropdown menu with 'VLAN Aware Bundle' selected.
- Route Distinguisher**: Text input field.
- VRF Import Target**: Text input field.
- VRF Export Target**: Text input field.
- VRF Both Target**: Text input field.
- DHCP Snooping**: Section with a red border containing:
 - ☐ Enable
 - ☐ Verify MAC Address
- MPLS Services**: ☐ MPLS Services
- Interfaces**: Section with a red border containing:
 - ☐ Interfaces
 - Interfaces Not Configured
- Bridge Domains**: Section with a red border containing:
 - ☐ Bridge Domain Name
 - VLAN ID
 - No Bridge Domains Added

At the bottom right, there are 'OK' and 'Cancel' buttons.

Field	Description
DHCP Snooping (Group of Fields)	
◦ Enable	Click to enable or disable DHCP snooping.
◦ Verify MAC Address	Click to enable or disable MAC address verification. If you enable MAC address verification, if the switch receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, the packet is dropped. The source MAC address is in the Ethernet packet header, and the client hardware address is a field in the DHCP packet payload.

5. To configure DHCP snooping for a bridge domain, click the  Add icon in the Bridge Domains field. The Add Bridge Domains popup window displays.

Add Bridge Domains

Bridge Domain Name *

VLAN ID *

VXLAN VNI

Routing Interface

DHCP Snooping

☐ Enable
☐ Verify MAC Address

L2 Learning

☒ MAC Learning

☒ MAC Move

MAC Limit

MAC Table Aging Time(seconds)

☐ Suppress Unknown Unicast
☐ ARP Suppression
☐ IP Source Guard

BD Interfaces For VLAN Translation

Interfaces

--Select--

+

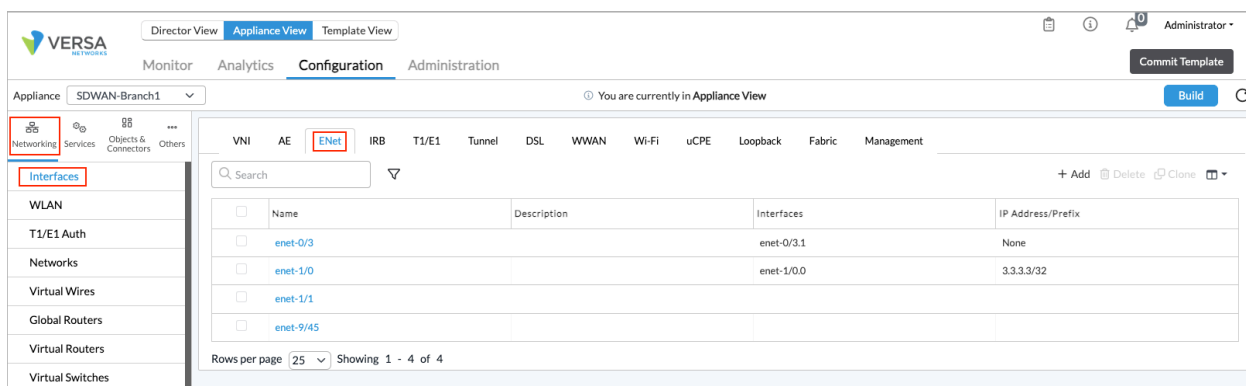
No Records to Display

6. Enter the information as described in [Step 4](#), above.
7. Click OK.

For more information about configuring virtual switches, see [Configure a Virtual Switch with Bridge Domains and Bridge Interfaces](#).

Configure a DHCP Trusted Interface

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar. The following screen displays.



4. Select the ENet tab in the horizontal menu, and then click an enet interface. The Edit ENet Interface screen displays.

Interface *

enet - 0 / 3 ☐ Disable

Description Tags

☐ Promiscuous ☐ Virtual Wire ☐ Mirror Interface ☐ PPPoE base Interface ☒ DHCP Trusted

Native VLAN ID MTU Outer TPID

Bandwidth | Others | Hold Time | PoE | Multihoming

Uplink (Kbps) Downlink (Kbps)

OK Cancel

5. Select the General tab, and then click DHCP Trusted.
6. Click OK.

Monitor DHCP Snooping

For Releases 22.1.4 and later.

1. In Director view, select the Monitor tab in the top menu bar.
2. Select an organization in the Organization field.
3. Select the Devices tab in the horizontal menu bar.
4. Select a device in the main pane.
5. Select the Networking tab in the horizontal menu bar, and then select DHCP Snooping. Select the Statistics tab to view DHCP snooping statistics. If you select the Statistics tab, a screen similar to the following displays.

Organization: Tenant1

Total Appliances: 5

SDWAN-Branch1 | 1 Hacker Way, Menlo Park, CA, USA 94025
Mgmt. Address: 10.192.118.142
System Bridge Address: 0A:00:8B:76:CF:00

Summary Services **Networking** System Tools

Configuration Shell Config Status* Upgrade Subscription

Binding Statistics

Org Name	Invalid Message Parsing Failed Drop	Server Message Untrusted Drop	Client Message MAC Mismatch Drop	Client Message Interface Mismatch Drop	Client Message With Relay IP Drop
Tenant1	0	0	0	0	0

6. Select the Binding tab to view binding information.

Organization: Provider-org

Total Appliances: 13

CSX04300 | Flat No 204, Mahaveer Fair Oaks, Narayanappa Garden Whitefield, Bangalore, Karnataka, India 560066
Mgmt. Address: 10.0.0.22
System Bridge Address: 0A:8F:C3:F0:30:00

Summary Services **Networking** System Tools

Configuration Shell Config Status* Upgrade Subscription

Binding Statistics

MAC Address	IP Address	Lease Expiration	Interface	VLAN ID	Type
00:00:00:00:00:01	1.1.1.1	Wed May 15 11:15:45 2024	enet-0/24	40	Configured

Supported Software Information

Releases 22.1.3 and later support all content described in this article, except:

- Release 22.1.4 adds support for configuring DHCP snooping at the virtual switch and bridge domain levels; adds support for monitoring DHCP snooping.

Additional Information

[Configure DHCP](#)

[Configure Interfaces](#)

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_DHCP...

Updated: Wed, 23 Oct 2024 08:20:13 GMT

Copyright © 2024, Versa Networks, Inc.

[Configure a Virtual Switch with Bridge Domains and Bridge Interfaces](#)