Revised: May 30, 2025

Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF, Release 17.16.x

Control Connections to Cisco Catalyst SD-WAN Manager

In an SD-Routing network, any WAN interface associated with a VRF establishes a control connection to the Cisco Catalyst SD-WAN Manager.

You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic.

Types of WAN Interfaces for Control Connections

You can create custom VRFs in the Transport and Management profile and attach multiple WAN interfaces to it. These interfaces can be of type:

- All types of physical ethernet interface
- Unbound loopbacks
- Bounded loopbacks
- Port-channels

These interfaces when configured can establish control connections to the Cisco Catalyst SD-WAN Manager.

Preference Value for Control Connection

If you have configured multiple WAN interfaces for a one or more VRFs, you can set a preference for which of these multiple WAN interfaces form a control connection with Cisco Catalyst SD-WAN Manager.

This preference is set using the **Connection Preference** value in Cisco Catalyst SD-WAN Manager. This preference value determines the order in which each of the multiple WAN interfaces can form a control connection with the Cisco Catalyst SD-WAN Manager.

Steps to Set Up WAN Interfaces with a Custom VRF

Configuring WAN interfaces with a custom VRF involves these steps:

- Configure a Custom VRF, on page 1
- Add Interfaces to a Custom VRF, on page 5
- Associate the Service Profile to a Configuration Group

Configure a Custom VRF

You can create custom VRFs with one or more WAN interfaces.

Note

To specify a value for the parameters required for configuring a VRF, choose **Global**, or **Device Specific** from the drop-down list and then proceed with specifying the required value.

Step 1 On the Cisco Catalyst SD-WAN Manager, select **Configuration** > **Configuration Groups**. Select the solution type as **SD Routing**.

Step 2 Select a configuration group from the list that is displayed. Create a new Transport and Management profile or select an existing profile. Select the profile, click on **…** and select **Edit**.

Step 3 Click **Add New Feature**, and select **VRF** to create a custom VRF. Click **Add New** to enter these details:

Tip To specify a value for the parameters required for configuring a VRF, choose **Global**, or **Device Specific** from the drop-down list.

Basic Configuration

Option	Description
VRF Name	Specify an identifier for the VRF.
RD	Specify a route distinguisher for the VRF or use the system default. A route distinguisher helps distinguish the distinct virtual private network routes of customers who connect to the provider.

DNS

Option	Description
IP address	Enter the IP address of the primary DNS server in this VRF. This IP address is used for resolving the Cisco SD-WAN Validator hostname.

Host Mapping

Option	Description
Hostname	Enter the hostname of the DNS server. The limit is 128 characters.
List of IP Address	Enter IP addresses to associate with the hostname. Separate the entries with commas.

IPv4 Static Route

Option	Description
Network Address	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, to configure the VRF.
Subnet Mask	Enter the subnet mask for the prefix or the IP address. You can also choose a subnet mask from the drop-down list.
Gateway	Choose one of the following options to configure the Next Hop to reach the static route: • **Next Hop**: When you choose this option and click **Add** , the following fields are displayed : • **Address**: Specify the next-hop IPv4 address.

Option	Description
	• **Administrative distance**: Specify the administrative distance for the route. • **Object Tracker/Object Tracker Group**: Object tracking is a mechanism for tracking an object to take any client action on another object as configured by the client. You can identify each tracked object by a unique name that is specified by the track parameter. Select an object from the drop-down list. • **Null 0**: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **Administrative distance:** Specify the administrative distance for the route. • **dhcp** • **Administrative distance**: Enter the administrative distance for the route. • **Interface**: Click **Add** and specify the following details: • **Interface Name**: Specify a valid interface or choose a value from the drop-down list. • **Add Next Hop**: • **Address**: Specify the next-hop IPv4 address. • **Administrative distance**: Specify the administrative distance for the route.

IPv6 Static Route

Option	Description
Prefix	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VRF.
Gateway	Choose one of the following options to configure the Next Hop to reach the static route: • **Next Hop**: Select this option and click **Add**,the following fields are displayed : • **Address**: Specify the next-hop IPv4 address. • **Administrative distance**: Specify the administrative distance for the route. • **Null 0**: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **Administrative distance:** Specify the administrative distance for the route. • **Interface**: Click **Add** and specify the following details: • **Interface Name**:Specify a valid interface or choose a value from the drop-down list. • **Next Hop**: • **Address**: Specify the next-hop IPv4 address.

Option	Description
	• **Administrative distance**: Specify the administrative distance for the route.

NAT

Option	Description
NAT Enable	Click on the toggle button to enable NAT.
Add NAT Interfaces	Specify how internal users and external users should access internet or exchange information with devices on the internet.
Static NAT	Add a static NAT mapping. This creates a static translation of real addresses to mapped addresses.
Static NAT Subnet	Add subnet details for static NAT mapping. Define the subnet for the NAT mapping.
NAT Port Forward	Add NAT port forwarding rules to define how to direct traffic coming to a specific port on a public IP address to a specific internal IP address and port within the local network. This allows external users to access services hosted on devices within a private network.
Dynamic NAT	Add Dynamic NAT rules. This defines how local address is mapped to a global address dynamically. Unlike static mapping, there is no manual definition of mapping between a private and public address.

Route Leak from Global VRF

Option	Description
Route Protocol	Choose a protocol from the drop-down list. This protocol is used to leak routes from global VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list to define the routes for route leak.

Redistribution (in VRF)

Option	Description
Protocol	Choose a protocol from the drop-down list to redistribute the leaked routes.
Select Route Policy	Choose a route policy from the drop-down list.

Route leak to Global VRF

Option	Description
Route Protocol	Choose a protocol from the drop-down list. This protocol is used to leak routes from global VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.

Redistribution (in VRF)

Option	Description
Protocol	Choose a protocol from the available options to redistribute the leaked routes.

Option	Description
Select Route Policy	Choose a route policy from the drop-down list.

Route Leak from other Service VRF(s)

Option	Description
Source VRF	Choose a VRF from the drop-down list.
Route Protocol	Choose a protocol from the available options to leak routes from the source service VRF to the service VRF that you are configuring.
Select Route Policy	Choose a route policy from the drop-down list.

Redistribution (in Service VRF)

Option	Description
Protocol	Choose a protocol from the available options to redistribute the leaked routes.
Select Route Policy	Choose a route policy from the drop-down list.

Step 4 Click **Save**.

Step 5 Repeat the process to create additional custom VRFs.

What's next

After configuring the custom VRF, proceed with Adding WAN interfaces to the custom VRF.

Add Interfaces to a Custom VRF

Before you add WAN interfaces, make sure to complete the steps in Configure a Custom VRF, on page 1.

Tip

To specify a value for the parameters required for configuring an interface, choose **Global**, or **Device Specific** from the drop-down list .

Step 1 Select the custom VRF and click the + symbol.

Step 2 Select **Ethernet Interface** to create a new WAN interface for this custom VRF.

Step 3 Specify the details for the WAN interface:

Option	Description
Name	Name of the ethernet interface.
Description	Description of the ethernet interface.
Shutdown	Click the toggle button to enable the interface.
Control Connection	Click the toggle button to enable control connections**.** By default, the control connections are turned off. Set a numerical value for **Connection Preference**. The range is from 0

Option	Description
	to 8 with 8 being the highest priority for this interface to establish control connections with Cisco Catalyst SD-WAN Manager. The default value is 5.
Bind Interface	In case of bind mode, each loopback is bound to a physical interface and traffic destinated to loopback is carried to and from mapped physical interface. This can be used when customers have connected subnets on transport side, and can use loopback to form control connections and data tunnels.
Connection Preference	Set a numerical value for **Connection Preference**. The range is from 0 to 8 with 8 being the highest priority for this interface to establish control connections with Cisco Catalyst SD-WAN Manager. The default value is 5.
Interface name	Specify a name for the interface.
Description	Specify a description for the interface.

IPV4 /IPv6 Settings

Option	Description
IPv4 / IPv6	Decide the IP addressing format for the interface. Click **IPv4** or **IPv6**.
Dynamic	Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.
DHCP Dynamic Distance	Optionally, specify an administrative distance value for routes learned from a DHCP server. Default is 1.
DHCP Helper	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers.
Static	Click **Static** to enter an IP address that doesn't change.
IPv4 Address	Specify a static IPv4 address.
IPv6 Address	Specify a static IPv6 address.
Secondary Address IPv4	Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.
Secondary Address IPv6	Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.

BFD

Option	Description
Enable BFD	Click the toggle button to enable BFD. The function of BFD is to detect path liveliness and also perform quality measurements for application-aware routing, like loss, latency, and jitter.
Minimum Receive Interval (Milliseconds) **And Transmit Interval**	Specify the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable

Option	Description
Multiplier	Specify the number of times the poll interval should be multiplied by the indicated number. The Multiplier value specifies how many consecutive BFD probes can be lost before declaring the tunnel to be down.

ARP (Optional)

Option	Description
IP Address	Specify the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Specify the MAC address in colon-separated hexadecimal notation.

ACL (Optional)

Option	Description
Ingress ACL - IPv4	Specify the name of an IPv4 access list to packets being received on the interface.
Egress ACL - IPv4	Specify the name of an IPv4 access list to packets being transmitted on the interface.
Ingress ACL - IPv6	Specify the name of an IPv6 access list to packets being received on the interface.
Egress ACL - IPv6	Specify the name of an IPv6 access list to packets being transmitted on the interface.

Advanced

Option	Description
Duplex	Specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 . Default value is 1500 bytes.
Interface MTU	Specify the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet). Default: 1500 bytes.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes.
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, 1000, 2500, or 10000 Mbps.
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. ARP timeout controls how long we maintain the ARP cache on a router. Range: 0 through 2147483 seconds. Default: 1200 seconds.

Option	Description
Autonegotiate	Toggle this option to turn on autonegotiation.
Media Type	Specify the physical media connection type on the interface. Choose one of the following: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media.
Load Interval	Specify an interval value for interface load calculation.
IP Directed Broadcast	Toggle the button to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet
ICMP Redirect Disable	Toggle the button to enable IP Directed Broadcast. ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

Step 4 Click **Save**.

Step 5 Repeat the process to create additional WAN interfaces.

Associate and deploy the configuration group to an SD-Routing device

This task involves associating the configured profile to a configuration group and provisioning the changes to one or more SD-Routing devices.

Ensure that the configuration group you select is created for SD-Routing devices.

Step 1 On Cisco SD-WAN Manager, select the **Configuration Group** created earlier.

Step 2 Click **+ Add** and select the devices from the list. Click **Save** to attach the configuration group to the selected devices.

Step 3 To provision the configuration changes, click **Deploy**.

a) Select the device on which you want to provision the configuration changes. Click **Next**.

b) For each device, review or update the IP address, hostname. Specify the password to access these devices. Click **Next**.

c) If you want to review the configuration changes, click **Preview CLI**. Select the device to view the configuration changes either inline or side by side. The configurations that are removed are highlighted in red and the new configuration is highlighted in green. To remove or add any device from the list of selected devices, **click Edit Device List**

d) Click **Deploy** to provision the configuration changes on the devices.

Monitor Custom VRF

This section provides details on how to monitor a custom VRF using commands and Cisco Catalyst SD-WAN Manager.

Monitor Custom VRF Using Cisco Catalyst SD-WAN Manager

The Monitor dashboard helps you monitor the different components and services of an SD-Routing network

Step 1 On the Cisco Catalyst SD-WAN Manager, choose **Monitor** > **Devices**. Select a device from the list.

Step 2 Select **Control Connections** to view information about the control connections from the SD-Routing device to the Cisco Catalyst SD-WAN Manager.

Step 3 To view the control connections in real time, select choose **Real Time** from the left pane. From **Device Options**, select the parameter you want to view. For example, to view real time information about control connections, choose one of these parameters.

- Control Connections
- Control Connections History
- Control Local Properties
- Control Summary
- Control Statistics
- Control WAN Interface Information.

Monitor Custom VRF Sessions Using Commands

Use these commands to monitor the global VRF, custom VRFs and the associated WAN interfaces.

Use command	To
show sd-routing control connections summary	display active control plane connections to Cisco Catalyst SD-WAN Manager.
show sd-routing control local-properties wan ipv4	display IPv4 related information about local control properties of WAN interfaces.
show platform software sd-routing vdaemon vrfs	display all the VRFs configured for the device.
show sd-routing control local-properties wan detail	display detailed information about local control properties of WAN interfaces.