Revised: October 30, 2026

VRF and mData Header for Cisco 8000 Series Secure Routers using Cisco Meraki Dashboard

Feature history of VRF and mData header support

Table 1: Feature history: VRF and mData header support

Feature Name	Release	Feature Information
VRF and mData Header Support for VRF	Cisco IOS XE 26.2.1 Release	VRF and mData header support for VRF provides end-to-end VRF propagation across VPN tunnels for Cisco IOS XE Secure routers managed by the Cisco Meraki Dashboard. The feature allows customers to define custom VRFs, associate VRF context with VLANs and L3 interfaces, and preserve VRF information across AutoVPN tunnels.

VRF and mData Header Support

You can define custom VRFs and associate them with VLANs and L3 interfaces.

VRF support is also added to ping tools, ARP table, route table filtering, VLANs, and L3 interface pages. Route table support includes a VRF filter so you can retrieve routes under a selected VRF. The default route-table view shows routes available in the default LAN VRF first, and user-defined VRFs are available for selection when configured.

mData header support is enabled for AutoVPN peers. VRF propagation through the mData header across AutoVPN tunnels is supported. The header is carried within the IPsec packet between the outer ESP information and the inner IP packet. Its `DST_VRF` mData element carries the VPN or VRF context for interoperability between peers.

Configure VRF

Choose one of the options to configure VRF:

- VRF configurations on Cisco Meraki Dashboard
- VRF configurations on Cisco Secure Routers

Configure VRFs from the Cisco Meraki Dashboard

For information about Cisco Meraki Dashboard configuration steps, refer to VRF for WAN Appliances.

Step 1 From the Cisco Meraki Dashboard, click **Organization** on the left menu, then click on **VRFs**.

Step 2 Click **Enable VRF** on WAN to allow creation of VRFs for WAN appliances.

Step 3 Click **Add VRF**.

VRF Name: A name for the VRF. VRF name must be unique within the organization, must not contain spaces, must be at most 32 characters, and must not use the reserved name Default.

Description: A name/description for the VRF.

Route Distinguisher: Assign a route distinguisher (RD) for the VRF that helps identify a virtual routing domain in a provider's network and allows for overlapping IP space. The route distinguisher must be a unique value within the organization and on the router for each VRF.

Format requirements: Route distinguisher is generally expressed in the format of ASN Number:Unique number. Example: 65000:10. However, following are the format requirements. The format consists of two parts separated by a colon (:)

First part can be one of the three formats:

- Two decimal numbers separated by a dot, each number having 1 to 10 digits (e.g., 123.456).
- A single decimal number with 1 to 10 digits (e.g., 22 or 1234567890).
- A valid IPv4 address in dotted decimal notation.

The second part after the colon is a decimal number with 1 to 10 digits (e.g., 22 or 1234567890).

Route Target: Assign a route target (RT) to control the redistribution of routes between different VRFs. RTs identify which VRF a route belongs to, allowing for selective sharing of routes between VRFs.

Format requirements: Same as the requirements for Route distinguisher.

Enable for WAN appliances: Check box to enable the VRF to be used for WAN appliances.

Step 4 Click **Save**.

VRF-aware routing configurations on Cisco Secure Routers

Note

The router configurations are not manually set on the router, instead, all the configurations are automatically pushed from the Cisco Meraki cloud.

VRF definitions and LAN interfaces

```
vrf definition VRF-2
 rd 20000:1
 address-family ipv4
  route-target export 20000:1
  route-target import 20000:1
 exit-address-family
 address-family ipv6
  route-target export 20000:1
  route-target import 20000:1
 exit-address-family
!
vrf definition VRF-31
 rd 310000:1
 address-family ipv4
  route-target export 310000:1
  route-target import 310000:1
 exit-address-family
!
mpls label mode all-vrfs protocol all-afs per-vrf
```

Representative LAN interface configurations

VLAN SVI:

```
interface Vlan<ID>
 vrf forwarding <vrf-name>
 ip address <svi-ip> <subnet-mask>
 no shutdown
```

Physical routed L3 LAN interface:

```
interface <physical-l3-interface>
 vrf forwarding <vrf-name>
 ip address <l3-ip> <subnet-mask>
 no shutdown
```

LAN subinterface:

```
interface <physical-l3-interface>.<subinterface-id>
 encapsulation dot1Q <vlan-id>
 vrf forwarding <vrf-name>
 ip address <subinterface-ip> <subnet-mask>
 no shutdown
```

Subinterfaces under the same physical interface can belong to different VRFs.

Add VRF instance in MP-BGP for AutoVPN

The following representative configuration is generated by the Dashboard. It uses per-VRF BGP network statements to advertise applicable VLAN, physical-L3, static-route, and hub-default prefixes.

```
router bgp 64512
 bgp router-id interface Loopback2147483647
 bgp log-neighbor-changes
 bgp listen range 169.254.128.0/17 peer-group SPOKES
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 64512
 neighbor SPOKES update-source Loopback2147483647
 timers bgp 5 15
 address-family ipv4
  neighbor SPOKES activate
 exit-address-family
 address-family vpnv4
  neighbor SPOKES activate
  neighbor SPOKES next-hop-self all
  neighbor SPOKES route-reflector-client
  neighbor SPOKES send-community extended
 exit-address-family
 address-family ipv4 vrf CLOUD_DEFAULT_VRF
  network 192.168.146.0
  network 0.0.0.0
 exit-address-family
 address-family ipv4 vrf t182575066-fw-rollback
  network 0.0.0.0
 exit-address-family
 address-family ipv4 vrf vrf18
  network 0.0.0.0
 exit-address-family
 address-family ipv4 vrf vrf20
  network 0.0.0.0
 exit-address-family
 address-family ipv4 vrf vrf23
  network 0.0.0.0
 exit-address-family
 address-family ipv4 vrf vrf24
```

```
 network 0.0.0.0
exit-address-family
address-family ipv4 vrf vrf70
 network 0.0.0.0
exit-address-family
```

Verify VRF configurations

Use the following commands to validate VRF configuration, AutoVPN session state, vpnv4 route propagation, route lookup, interface counters, and packet path.

VRF and AutoVPN verification commands

```
show crypto autovpn session
show vrf VRF-2
show bgp vpnv4 unicast all
show ip cef vrf VRF-2 <dst-route>
show interface <Virtual-Access/uplink>
show ip interface brief
show ip route vrf <vrf-name>
show running-config
show interface <lan-intf> switchport
```