



Virtual Routing and Forwarding

- [Information About VRF Support, on page 1](#)
- [Use Cases, on page 2](#)
- [Guidelines and Restrictions for VRF Support, on page 2](#)
- [Create a VRF Instance, on page 3](#)
- [Map VRF to SVI, on page 3](#)
- [Adding VRF Name Through Option 82 for DHCP Relay, on page 4](#)
- [Adding VRF Name to DHCP Server for DHCP Relay, on page 5](#)
- [Verify VRF Support, on page 6](#)

Information About VRF Support

Virtual Routing and Forwarding (VRF) is a logical representation or grouping of Layer 3 entities, such as IP address, routes, and so on. The VRF Support feature provides the controller with the capability to split the control plane and data plane into multiple segregated logical instances within the same controller platform and make these planes VRF aware.

VRF plays a crucial role in the following use cases:

- Enabling flexible routing in infrastructure services such as AAA, DHCP, DNS, and more.
- Facilitating support for overlapping IP addresses.



Note Direct route leakage between VRFs is not permitted. It should proceed from VRF A to GRT, then to the intended destination, VRF B.

For a multitenant network such as an airport, this allows you to provide wireless services to different tenants (including airlines and shops) at the airport by supporting two clients with different MAC addresses using the same IP address. With VRF support, AP in local mode or AP in FlexConnect mode with central switching policy can have two clients with the same IP even if they belong to different VRFs.



-
- Note**
- From Cisco IOS XE Dublin 17.12.1, overlapping IP address can be supported without disabling device tracking, by using VRF.
 - The configuration of VRF is not exclusive to this release, but its effectiveness begins from this release.
-

VRFs Supported Per Platform

- Cisco Catalyst 9800-80 Wireless Controller: 8181
- Cisco Catalyst 9800-40 Wireless Controller: 8181
- Cisco Catalyst 9800-L Wireless Controller: 8181
- Cisco Catalyst 9800 Wireless Controller for Cloud: 4096

Use Cases

Route leak between two VRFs (VRF-A and VRF-B) is possible using a Global Routing Table (GRT). That is, you can permit the traffic from VRF-A to VRF-B using GRT.



-
- Note** The direct route leak between VRFs are not supported.
-

Guidelines and Restrictions for VRF Support

- Supports only Local mode and FlexConnect mode (central DHCP and central switching).
- Supports only one VRF per WLAN.



-
- Note** The maximum number of VRFs supported on a platform depends on the number of WLANs supported on the hardware platform.
-

- Supports static VRF ID allocation. All the configured VRFs should be associated with an SVI.
- Supports switch virtual interfaces (SVI) other than Wireless Management Interface (WMI).
- Supports only external DHCP servers.
- mDNS gateway is not supported.
- We recommend using commands to configure the feature because all VRF configurations are currently not supported through GUI.

Create a VRF Instance

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	vrf definition <i>vrf-name</i> Example: Device(config)# vrf definition red-vrf	Configures a VRF instance and enters VRF configuration mode.
Step 3	address-family ipv4 Example: Device(config-vrf)# address-family ipv4	Sets an IPv4 address family.
Step 4	exit-address-family Example: Device((config-vrf-af)# exit-address-family	Exits from VRF address-family configuration submode.
Step 5	address-family ipv6 Example: Device(config-vrf)# address-family ipv6	Sets an IPv6 address family.
Step 6	exit-address-family Example: Device((config-vrf-af)# exit-address-family	Exits from VRF address-family configuration submode.
Step 7	end Example: Device(config-vrf)# end	Returns to privileged EXEC mode.

Map VRF to SVI

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	<code>Device# configure terminal</code>	
Step 2	interface <i>interface-type-number</i> Example: <code>Device(config)# interface vlan181</code>	Configures VLAN to be associated with the VRF and enters the interface configuration mode.
Step 3	vrf forwarding <i>vrf-name</i> Example: <code>Device(config-if)# vrf forwarding red-vrf</code>	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface.
Step 4	no ip proxy-arp Example: <code>Device(config-if)# no ip proxy-arp</code>	Disables proxy ARP.
Step 5	no shutdown Example: <code>Device(config-if)# no shutdown</code>	Enables the interface.
Step 6	end Example: <code>Device(config-if)# end</code>	Returns to privileged EXEC mode.

Adding VRF Name Through Option 82 for DHCP Relay

To enable the transmission of VRF name through Option 82 during DHCP relay, follow this procedure.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>Device# configure terminal</code>	Enters global configuration mode.
Step 2	wireless profile policy <i>policy-name</i> Example: <code>Device(config)# wireless profile policy red-vrf</code>	Enables configuration for the specified profile policy.
Step 3	shutdown Example: <code>Device(config-wireless-policy)# shutdown</code>	Shuts down the wireless profile policy.
Step 4	ipv4 dhcp opt82 VRF Example:	Enables VRF based Sub Option 151.

	Command or Action	Purpose
	Device(config-wireless-policy)# ipv4 dhcp opt82 VRF	
Step 5	no shutdown Example: Device(config-wireless-policy)# no shutdown	Enables the wireless profile policy.
Step 6	end Example: Device(config-wireless-policy)# end	Returns to privileged EXEC mode.

Adding VRF Name to DHCP Server for DHCP Relay

When implementing DHCP relay, this procedure allows you to configure the DHCP server's VRF separately from the VRF of the client.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>policy-name</i> Example: Device(config)# wireless profile policy red-vrf	Enables configuration for the specified profile policy.
Step 3	shutdown Example: Device(config-wireless-policy)# shutdown	Shuts down the wireless profile policy.
Step 4	ipv4 dhcp server <i>ip-address vrf vrf-name</i> Example: Device(config-wireless-policy)# ipv4 dhcp server 1.2.3.4 vrf red-vrf	Configures the WLAN's IPv4 DHCP server IP address and VRF name.
Step 5	no shutdown Example: Device(config-wireless-policy)# no shutdown	Enables the wireless profile policy.
Step 6	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-wireless-policy)# end	

Verify VRF Support

Use the following commands to verify the VRF support.

```
Device# show wireless client mac-address aaaa.facc.cccc detail
```

```
Client MAC Address : aaaa.facc.cccc
Client MAC Type : Locally Administered Address
Client DUID: NA
Client IPv4 Address : 10.240.128.1
Client IPv6 Addresses : 2010::1:200:axx:fe04:68a
Client Username: N/A
Client VRF Name: red-vrf
AP MAC Address : 0j0b.0b00.0100
AP Name: AP6B8B4567-0001
AP slot : 0
Client State : Associated
Policy Profile : flex-central-auth-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id: 8
WLAN Profile Name: wpa3sae
Wireless LAN Network Name (SSID): wpa3sae
BSSID : 0a0b.0c00.0100
Connected For : 1055 seconds
```

```
Device# show wireless device-tracking database mac
```

```
MAC          VLAN  IF-HDL      VRF-Name  IP
-----
6c40.088c.a452  16    0x9040000e  red-vrf   9.10.16.64
```

```
Device# show wireless profile policy detailed test
```

```
Policy Profile Name      : test
Description              :
Status                   : ENABLED
VLAN                     : 20
.
.
.
Profile Name             : Not Configured
Accounting list
  Accounting List        : Not Configured
DHCP
  required                : DISABLED
  server address         : 0.0.0.0
VRF Name                : red-vrf
Opt82
  DhcpOpt82Enable        : DISABLED
  DhcpOpt82Ascii         : DISABLED
  DhcpOpt82Rid           : DISABLED
  APMAC                  : DISABLED
  SSID                   : DISABLED
  AP_ETHMAC              : DISABLED
  APNAME                 : DISABLED
```

```

POLICY TAG                : DISABLED
AP_LOCATION                : DISABLED
VLAN_ID                   : DISABLED
VRF                      : ENABLED
Exclusionlist Params
  Exclusionlist            : ENABLED
  Exclusion Timeout       : 60
.
.
.

```

To check VRF and client overlap IP address, use the following commands:

```
Device# show wireless device-tracking database mac
```

```
MAC VLAN IF-HDL IP ZONE-ID/VRF-NAME
```

```
-----
```

```
6038.e0dc.317e 172 0x90400004 172.172.172.254 red-vrf
```

```
60f8.1dce.39b0 173 0x90000006 172.172.172.254 blue-vrf
```

```
Device# show wireless cli summary detail
```

```
Number of Clients: 2
```

MAC Address	SSID	AP Name	State	IP Address	Device-type	VLAN	VRF Name	BSSID
		Auth Method	Created					
6038.e0dc.317e	UI_172	AP9120	Run	172.172.172.254	172		red-vrf	
7c21.0d31.dcef	[PSK]		02:09:08					
60f8.1dce.39b0	UI_173	AP2702I	Run	172.172.172.254	173		red-vrf	
80e0.1d81.c64f	[PSK]		07:41					

Connected	Protocol	Channel	Width	SGI	NSS	Rate	CAP	Username	Rx packets	Tx packets	Rx bytes	
		6E capability										
02:09:11	11n(5)		36	40/40	Y/Y	2/2	m15	E	19214	12028	2300155	
1939782	N											
07:44	11ac		36	20/80	Y/Y	3/3	m8ss3	E	29165	25429	5110	
	N											

