Virtual Routing and Forwarding

VRF support

Virtual Routing and Forwarding (VRF) support is a logical representation feature that

- groups Layer 3 entities such as IP addresses and routes
- provides the controller with the capability to split the control plane and data plane into multiple segregated logical instances within the same controller platform
- makes these planes VRF aware.

VRF use cases

VRF plays a crucial role in these use cases:

- Enabling flexible routing in infrastructure services such as AAA, DHCP, DNS, and more.
- Facilitating support for overlapping IP addresses.
- Permitting traffic from VRF-A to VRF-B using GRT. Route leak between two VRFs (VRF-A and VRF-B) is possible using a Global Routing Table (GRT). The direct route leak between VRFs are not supported.

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

Guidelines and restrictions for VRF support

Follow these guidelines and restrictions when implementing 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

Create a VRF instance to enable network virtualization and traffic isolation within a single physical device.

VRF (Virtual Routing and Forwarding) instances allow you to create multiple virtual routers within a single physical router, providing network segmentation and isolation. This is useful for service providers or enterprises that need to maintain separate routing domains.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a VRF instance and enter VRF configuration mode.

Example:

```
Device(config)# vrf definition vrf-name
```

Example:

```
Device(config)# vrf definition red-vrf
```

Step 3 Set an IPv4 address family.

Example:

```
Device(config-vrf)# address-family ipv4
```

Step 4 Exit from VRF address-family configuration submode.

Example:

```
Device((config-vrf-af)# exit-address-family
```

Step 5 Set an IPv6 address family.

Example:

```
Device(config-vrf)# address-family ipv6
```

Step 6 Exit from VRF address-family configuration submode.

Example:

```
Device((config-vrf-af)# exit-address-family
```

Step 7 Return to privileged EXEC mode.

Example:

```
Device(config-vrf)# end
```

The VRF instance is created with both IPv4 and IPv6 address families configured, providing isolated routing tables for network segmentation.

Map VRF to SVI

Associate a VRF with a VLAN interface to enable Layer 3 separation and routing isolation.

Mapping a VRF to an SVI allows you to create isolated routing domains where traffic from different VRFs remains separated. This configuration is used when implementing network segmentation or multi-tenancy scenarios.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the VLAN interface to be associated with the VRF. Enter the interface configuration mode for the specified VLAN interface.

Example:

```
Device(config)# interface interface-type-number
```

Example:

```
Device(config)# interface vlan181
```

Step 3 Associate the VRF with the Layer 3 interface.

Example:

```
Device(config-if)# vrf forwarding vrf-name
```

Example:

```
Device(config-if)# vrf forwarding red-vrf
```

This command activates multiprotocol VRF on the interface.

Step 4 Disable proxy ARP.

Example:

```
Device(config-if)# no ip proxy-arp
```

Step 5 Enable the interface.

Example:

```
Device(config-if)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-if)# end
```

The VRF is now mapped to the SVI, and the interface is configured for VRF-aware routing with proxy ARP disabled.

Add VRF name through Option 82 for DHCP relay

Enable the transmission of VRF name through Option 82 during DHCP relay operations.

VRF-based Sub Option 151 allows DHCP relay agents to include VRF information in Option 82, helping DHCP servers identify the originating VRF for client requests. This configuration is performed on wireless profile policies.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable configuration for the specified profile policy.

Example:

```
Device(config)# wireless profile policy policy-name
```

Example:

```
Device(config)# wireless profile policy red-vrf
```

Step 3 Shut down the wireless profile policy.

Example:

```
Device(config-wireless-policy)# shutdown
```

Step 4 Enable VRF-based Sub Option 151.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp opt82 VRF
```

Step 5 Enable the wireless profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The wireless profile policy is now configured to transmit VRF name through Option 82 during DHCP relay operations.

Add VRF name to DHCP server for DHCP relay

Enable separate VRF configuration between the DHCP server and client in DHCP relay scenarios.

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

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable configuration for the specified profile policy.

Example:

```
Device(config)# wireless profile policy policy-name
```

Example:

```
Device(config)# wireless profile policy red-vrf
```

Step 3 Shut down the wireless profile policy.

Example:

```
Device(config-wireless-policy)# shutdown
```

Step 4 Configure the WLAN's IPv4 DHCP server IP address and VRF name.

Example:

```
Device(config-wireless-policy)# ipv4 dhcp server ip-address vrf vrf-name
```

Example:

```
Device(config-wireless-policy)# ipv4 dhcp server 1.2.3.4 vrf red-vrf
```

Step 5 Enable the wireless profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The DHCP server VRF is now configured separately from the client VRF, enabling proper DHCP relay functionality between different VRF domains.

VRF support verification

To verify the VRF support, use these commands:

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

Client MAC Address : MAC XX
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : IP XX
Client Username : vrf1
AP MAC Address : aaa.bbb.ccc
AP Name: VRF_TEST_AP
AP slot : 1
Client State : Associated
Policy Profile : VRF_TEST_1
Flex Profile : N/A
Wireless LAN Id: 111
WLAN Profile Name: VRF_TEST_1
Wireless LAN Network Name (SSID): VRF_TEST_1
BSSID : aaa.bbb.ccc
Connected For : 543 seconds
Protocol : 802.11ax - 5 GHz
Channel : 44
Client IIF-ID : xxx
Association Id : 2
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 43200 sec (Remaining time: 42670 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
```

```
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m11 ss2
Supported Rates : 24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream             : 0 (kbps)
QoS Realtime Average Data Rate Upstream    : 0 (kbps)
QoS Burst Data Rate Upstream               : 0 (kbps)
QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
QoS Average Data Rate Downstream           : 0 (kbps)
QoS Realtime Average Data Rate Downstream  : 0 (kbps)
QoS Burst Data Rate Downstream             : 0 (kbps)
QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
Move Count                  : 0
Mobility Role               : Local
Mobility Roam Type          : None
Mobility Complete Timestamp : 01/09/2025
Client Join Time:
Join Time Of Client : 01/09/2025
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time :
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN Override after Webauth : No
VLAN : VRF_TEST_1
Multicast VLAN : 0
VRF Name : VRF_TEST_1
```

```
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_vrf
Description                         :
Status                              : ENABLED
VLAN                                : 1
Multicast VLAN                      : 0
OSEN client VLAN                    :
Wireless management interface VLAN  : 40
Multicast Filter                    : DISABLED
QBSS Load                           : ENABLED
Passive Client                      : DISABLED
```

```
ET-Analytics                          : DISABLED
StaticIP Mobility                     : DISABLED
WLAN Switching Policy
Flex Central Switching                : ENABLED
Flex Central Authentication           : ENABLED
Flex Central DHCP                     : ENABLED
Flex NAT PAT                          : DISABLED
WLAN Flex Policy
VLAN based Central Switching          : DISABLED
WLAN ACL
IPv4 ACL                              : Not Configured
IPv6 ACL                              : Not Configured
Layer2 ACL                            : Not Configured
Preauth urlfilter list                : Not Configured
Postauth urlfilter list               : Not Configured
WLAN Timeout
Session Timeout                       : 28800
Idle Timeout                          : 300
Idle Threshold                        : 0
Guest LAN Session Timeout             : DISABLED
WLAN Local Profiling
Subscriber Policy Name                : Not Configured
RADIUS Profiling                      : DISABLED
HTTP TLV caching                      : DISABLED
DHCP TLV caching                      : DISABLED
DOT11 TLV accounting                  : DISABLED
CTS Policy
Inline Tagging                        : DISABLED
SGACL Enforcement                     : DISABLED
Default SGT                           : 0
WLAN Mobility
Anchor                                : DISABLED
AVC VISIBILITY                        : Disabled
IPv4 Flow Monitors
Ingress
Egress
IPv6 Flow Monitors
Ingress
Egress
NBAR Protocol Discovery               : Disabled
Reanchoring                           : Disabled
Classmap name for Reanchoring
Reanchoring Classmap Name             : Not Configured
QOS per SSID
Ingress Service Name                  : Not Configured
Egress Service Name                   : Not Configured
QOS per Client
Ingress Service Name                  : Not Configured
Egress Service Name                   : Not Configured
Umbrella information
Cisco Umbrella Parameter Map          : Not Configured
DHCP DNS Option                       : ENABLED
Mode                                  : ignore
Autoqos Mode                          : None
Call Snooping                         : Disabled
Tunnel Profile
Profile Name                          : Not Configured
Calendar Profile
Fabric Profile
Profile Name                          : Not Configured
Accounting list
Accounting List                       : Not Configured
DHCP
required                              : DISABLED
```

```
server address                    : 1.2.3.4
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_NAME                          : ENABLED
.
.
.
```

To check VRF and client overlap IP address, use these 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    SSIDAP 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
 Tx 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
```