VRF-Aware Services

Feature History for VRF-Aware Services

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	VRF-Aware Services: IP services have been enhanced to be VRF-aware, which means they can now operate within multiple routing instances (VRFs).	Cisco C9350 Series Switches Cisco C9610 Series Switches

VRF-Aware services

IP services traditionally run on global interfaces within the global routing instance, meaning they operate in a single, shared routing context. However, these IP services have been enhanced to be VRF-aware, which means they can now operate within multiple routing instances (VRFs). This enhancement allows any configured VRF in the system to be specified for a VRF-aware service, enabling the service to run independently within that VRF's routing context.

VRF-aware services are implemented in platform-independent modules, but each platform has a limit on the number of supported VRFs. While the VRF-aware functionality works uniformly across platforms, the actual number of VRFs you can configure depends on the hardware or software platform capabilities of the platform.

VRF-aware services have the following characteristics:

- The user can ping a host in a user-specified VRF.
- Address Resolution Protocol (ARP) entries are learned in separate VRFs. The user can display ARP entries for specific VRFs.

Configure VRF-aware services

These sections provide configuration information about VRF-aware services.

Configure VRF-Aware services for SNMP

Perform this task to configure VRF-aware services for SNMP.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **snmp-server trap authentication vrf**

Example:

```
Device(config)# snmp-server trap authentication vrf
```

Enables SNMP traps for packets on a VRF.

Step 4 **snmp-server engineID remote** *host* **vrf** *vpn-instance engine-id string*

Example:

```
Device(config)# snmp-server engineID remote 172.16.20.3 vrf vpn1 80000009030000B064EFE100
```

Configures a name for the remote SNMP engine on a switch.

- *host*: Specifies the IP address or hostname of the remote SNMP entity whose engine ID is being defined.
- *vpn-instance*: Specifies the VPN instance to create separate routing and forwarding tables, allowing for network virtualization.
- *engine-id*: A unique identifier for an SNMP entity.
- *string*: This would be the actual hexadecimal string value that represents the engine ID.

Step 5 **snmp-server host** *host* **vrf** *vpn-instance* **traps** *community*

Example:

```
Device(config)# snmp-server host 172.16.20.3 vrf vpn1 traps comaccess
```

Specifies the recipient of an SNMP trap operation and specifies the VRF table to be used for sending SNMP traps.

Step 6 **snmp-server host** *host* **vrf** *vpn-instance* **informs** *community*

Example:

```
Device(config)# snmp-server host 172.16.20.3 vrf vpn1 informs comaccess
```

Specifies the recipient of an SNMP inform operation and specifies the VRF table to be used for sending SNMP informs.

Step 7 **snmp-server user** *user group* **remote** *host* **vrf** *vpn-instance security model*

Example:

```
Device(config)# snmp-server user abcd remote 172.16.20.3 vrf vpn1 priv v2c 3des secure3des
```

Adds a user to an SNMP group for a remote host on a VRF for SNMP access.

Step 8 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Configure VRF-aware services for NTP

Perform this section to configure VRF-aware services for NTP

VRF-aware services for NTP comprise the following:

- Configure VRF-aware services for NTP on NTP client
- Configure VRF-aware services for NTP on NTP server

Before you begin

Ensure connectivity between the NTP client and servers. Configure a valid IP address and subnet on the client interfaces that are connected to the NTP servers.

Configure VRF-aware services for NTP on NTP client

Perform this task to configure VRF-aware services for NTP on NTP client.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *interface-id*

Example:

```
Device(config)# interface gigabitethernet1/0/1
```

Specifies the Layer 3 interface to be associated with the VRF, and enters the interface configuration mode.

Step 4 **vrf forwarding** *vrf-name*

Example:

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

Associates the VRF with the Layer 3 interface.

Step 5 **ip address** *ip-address subnet-mask*

Example:

```
Device(config-if)# ip address 1.1.1.1 255.255.255.0
```

Enter the IP address for the interface.

Step 6 **no shutdown**

Example:

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

Enables the interface.

Step 7 **exit**

Example:

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

Exits the interface configuration mode.

Step 8 **ntp authentication-key** *number* **md5** *md5-number*

Example:

```
Device(config)# ntp authentication-key 1 md5 cisco123
```

Defines the authentication keys. The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key number** command.

Note
The authentication key number and the MD5 password must be the same on both the client and server.

Step 9 **ntp authenticate**

Example:

```
Device(config)# ntp authenticate
```

Enables the NTP authentication feature.

Note
NTP authentication is disabled by default.

Step 10 **ntp trusted-key** *key-number*

Example:

```
Device(config)# ntp trusted-key 1
```

Specifies one or more keys that an NTP server must provide in its NTP packets in order for the NTP client to synchronize to it. The range for trusted keys is from 1 to 65535. This command provides protection against accidentally synchronizing the NTP client to an NTP server that is not trusted.

Step 11 **ntp server vrf** *vrf-name*

Example:

```
Device(config)# ntp server vrf A 1.1.1.2 key 1
```

Configures NTP server in the specified VRF.

Configure VRF-aware services for NTP on the NTP server

Perform this task to configure VRF-aware services for NTP on NTP server.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ntp authentication-key** *number* **md5** *password*

Example:

```
Device(config)# ntp authentication-key 1 md5 cisco123
```

Defines the authentication keys.

The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key number** command.

Note
The authentication key number and the MD5 password must be the same on both the client and server.

Step 4 **ntp authenticate**

Example:

```
Device(config)# ntp authenticate
```

Enables the NTP authentication feature. NTP authentication is disabled by default.

Step 5 **ntp trusted-key** *key-number*

Example:

```
Device(config)# ntp trusted-key 1
```

Specifies one or more keys that an NTP server must provide in its NTP packets in order for the NTP client to synchronize to it.

The range for trusted keys is from 1 to 65535.

This command provides protection against accidentally synchronizing the NTP client to an NTP server that is not trusted.

Step 6 **interface** *interface-id*

Example:

```
Device(config)#interface gigabitethernet 1/0/3
```

Specifies the Layer 3 interface to be associated with the VRF, and enters the interface configuration mode.

Step 7 **vrf forwarding** *vrf-name*

Example:

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

Associates the VRF with the Layer 3 interface.

Step 8 **ip address** *ip-address subnet-mask*

Example:

```
Device(config-if)# ip address 1.1.1.2 255.255.255.0
```

Enter the IP address for the interface.

Step 9 **exit**

Example:

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

Exits the interface configuration mode.

Configure VRF-aware services for uRPF

Perform this task to configure VRF-aware services for uRPF.

uRPF can be configured on an interface assigned to a VRF, and source lookup is done in the VRF table.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *interface-id*

Example:

```
Device(config)# interface gigabitethernet1/0/1
```

Specifies the Layer 3 interface to be associated with the VRF, and enters the interface configuration mode.

Step 4 **no switchport**

Example:

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

Removes the interface from Layer 2 configuration mode if it is a physical interface.

Step 5 **ip vrf forwarding** *vrf-name*

Example:

```
Device(config-if)# ip vrf forwarding vpn2
```

Configures VRF on the interface.

Step 6 **ip address** *ip-address*

Example:

```
Device(config-if)# ip address 10.1.5.1
```

Enters the IP address for the interface.

Step 7 **ip verify unicast reverse-path**

Example:

```
Device(config-if)# ip verify unicast reverse-path
```

Enables uRPF on the interface.

Step 8 **end**

Example:

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

Returns to privileged EXEC mode.

Configure VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. The switch supports the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration commands, as described in the Per VRF AAA Feature Guide.

Configure VRF-aware services for syslog

Perform this task to configure VRF-aware services for syslog.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **logging on**

Example:

```
Device(config)# logging on
```

Enables or temporarily disables logging of storage router event message.

Step 4 **logging host** *ip-address***vrf** *vrf-name*

Example:

```
Device(config)# logging host 10.10.1.0 vrf vpn1
```

Specifies the host address of the syslog server where logging messages are to be sent.

Step 5 **logging buffered** *logging buffered size* **debugging**

Example:

```
Device(config)# logging buffered critical 6000 debugging
```

Logs messages to an internal buffer.

Step 6 **logging trap debugging**

Example:

```
Device(config)# logging trap debugging
```

Limits the logging messages sent to the syslog server.

Step 7 **logging facility** *facility*

Example:

```
Device(config)# logging facility user
```

Sends system logging messages to a logging facility.

Step 8 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Configure VRF-Aware services for traceroute

Perform this task to configure VRF-aware services for traceroute.

Procedure

Step 1 ***enable***

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **traceroute vrf** *vrf-name ipaddress*

Example:

```
Device(config)# traceroute vrf vpn2 10.10.1.1
```

Specifies the name of a VPN VRF in which to find the destination address.

Configure VRF-aware services for FTP and TFTP

Perform this task to configure VRF-aware services for FTP and TFTP.

To ensure FTP and TFTP operations are VRF-aware on Cisco devices, specify the interface whose VRF routing table is used for packet forwarding. Use these commands:

- **ip tftp source-interface** *interface*
- **ip ftp source-interface** *interface*

For example, if you want to use a VRF table that is attached to an interface, say E1/0, you need to configure the **ip tftp source-interface E1/0** or the **ip ftp source-interface E1/0** command to inform TFTP or FTP server to use a specific routing table. In this example, the VRF table is used to look up the destination IP address.

These changes are backward-compatible and do not affect existing behavior. You can use the source-interface CLI to send packets out a particular interface, even if no VRF is configured on that interface

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 Choose one of the following:

- **ip ftp source-interface** *interface-type interface-number*
- **ip tftp source-interface** *interface-type interface-number*

Example:

```
Device(config)# ip ftp source-interface gigabitethernet 1/0/2
OR

Device(config)# ip tftp source-interface gigabitethernet 1/0/2
```

Specifies the source IP address for FTP or TFTP connections.

Step 4 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.