VPN Routing and Forwarding (VRF)-Lite Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)

First Published: March 2014

OL-31240-01

With the VRF-lite feature, the Connected Grid 1000 Series Router (hereafter referred to as CGR 1000) supports multiple VPN routing and forwarding (VRF) instances to provide traffic isolation in an enterprise network. In this implementation, VRFs are used to segment a private physical infrastructure into virtual, isolated networks.

This document addresses both IPv4 and IPv6 VRF-lite.

Note The CGR 1000 does not use Multiprotocol Label Switching (MPLS) for VRF-lite.

This chapter includes the following topics:

Cisco Systems, Inc.
www.cisco.com

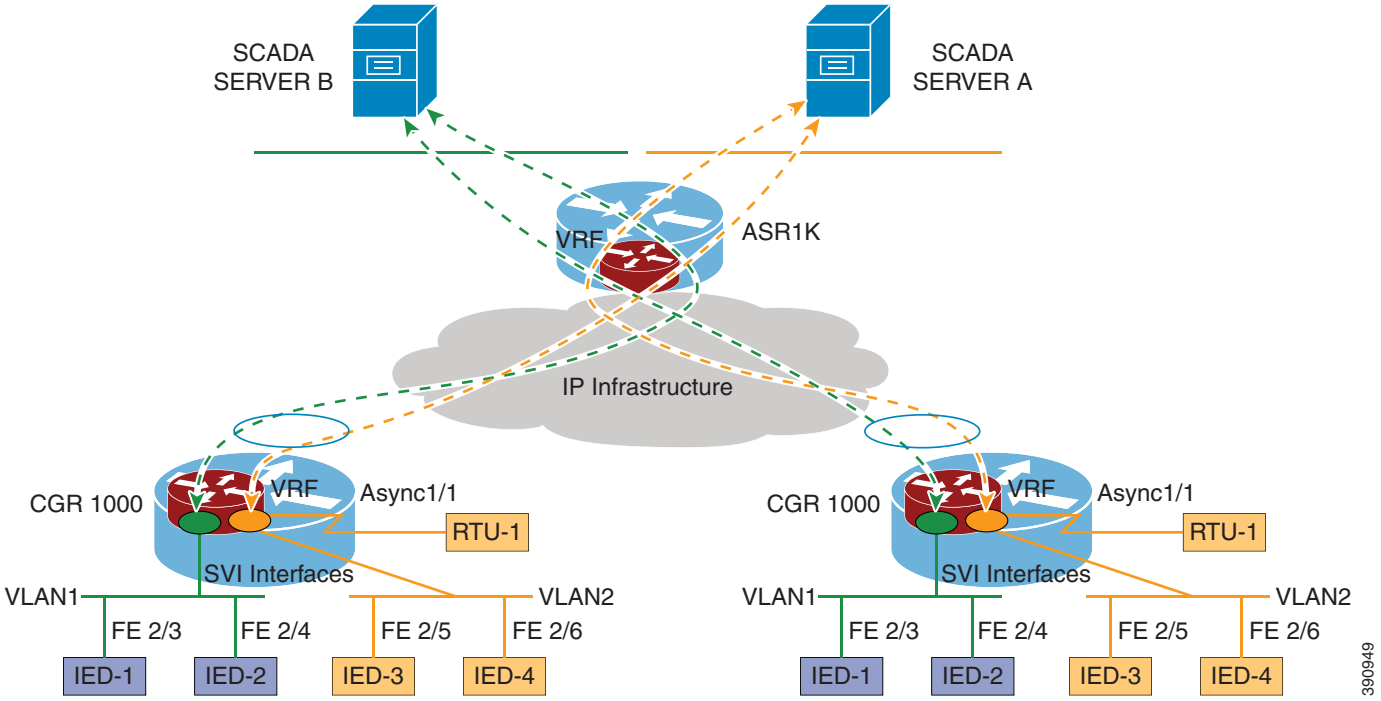
Information About VRF-lite

VRF-lite provides traffic isolation by using input interfaces to distinguish routes for different VLANs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs and loopback interfaces, but a Layer 3 interface cannot belong to more than one VRF at any time.

Note VRF-lite interfaces must be Layer 3 interfaces.

Figure 1 shows an example of a VRF-lite implementation for the CGR 1000.

Figure 1 VRF-lite Example



In Figure 1, two CGR 1000 routers are connected to the head-end router in a FlexVPN hub-and-spoke configuration. VRF Green is mapped to VLAN1, and VRF Orange is mapped to VLAN2. Each router has a serial interface, associated with a local IP address, to transport raw socket traffic from Remote Terminal Units (RTUs). Ethernet ports in VLAN2 and the loopback interface used by raw socket on each CGR 1000 are configured in VRF Orange so that traffic from those interfaces can be isolated and routed to SCADA Server A according to the FlexVPN tunnel configuration.

For more information about FlexVPN, see *FlexVPN Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)*.

VRF-Aware Services

VRF-Aware services are services that run on multiple routing instances and that can be configured on a per-VRF basis. A VRF-aware service uses a VRF table rather than the global routing table for routing traffic associated with the service. Any configured VRF in the system can be specified for a VRF-aware service.

VRF-aware services are implemented in platform-independent modules. Each platform has its own limit on the number of VRFs it supports.

VRF-aware Domain Name System (DNS) is an example of a VRF-aware service. In VRF-aware DNS, a VRF table can be configured so that DNS can forward queries to name servers using the VRF table rather than the named DNS server in the global IP address space.

Ping is another example of a VRF-aware service. You can ping a host in a user-specified VRF.

In addition to services such as DNS and ping, the following CGR 1000 features are VRF-aware:

- Raw Socket Transport
- T101-T104 and DNP3-DNP3/IP protocol translation

Prerequisites

Planning for the network, including IP addressing, interface and VLAN details, traffic types, etc. must be completed.

Guidelines and Limitations

IPv4 and IPv6

- VRF-lite interfaces must be Layer 3 interfaces.
- Multiple VLANs share a router with VRF-lite, and each VLAN is associated with a VRF.
- VRF-lite on the CGR 1000 does not support MPLS.
- The CGR 1000 supports configuring VRF by using physical ports, VLAN SVIs, loopback interface, or a combination. You can connect SVIs through an access port or a trunk port.
- A single VRF can be configured for both IPv4 and IPv6.
- You can associate an interface with only one VRF. You cannot configure a VRF for IPv4 and a different VRF for IPv6 on the same interface.
- IPv4 and/or IPv6 routing for a given VRF needs to be configured. You can use most routing protocols (BGP, OSPF, EIGRP, RIP and static routing).

IPv4-Specific

- VRF-lite does not support IGRP and ISIS.

IPv6-Specific

- VRF-aware ISISv6, RIPng, IPv6 Multicast Routing (MVRF), and PIMv6 are not supported.

Default Settings

If no commands have yet been entered to specify a VRF, the system's default configuration is as follows:

Feature	Default Setting
VRF	Disabled. No VRFs are defined.
Maps	No import maps, export maps, or route maps are defined.
VRF maximum routes	None.
Forwarding table	The default for an interface is the global routing table.

Configuring VRF-lite

In earlier Cisco IOS releases, you created a VRF to be applied only to an IPv4 address family (single-protocol VRF) by entering the **ip vrf** command. To activate the single-protocol VRF on an interface, you entered the **ip vrf forwarding** (interface configuration) command.

You can now define multiple address families under the same VRF or configure separate VRFs for each IPv4 or IPv6 address family by entering the **vrf definition** command. To activate the multiprotocol VRF on an interface, you enter the **vrf forwarding** command. A given VRF, identified by its name and a set of policies, can apply to both an IPv4 VPN and an IPv6 VPN at the same time. This VRF can be activated on a given interface, even though the routing and forwarding tables are different for the IPv4 and IPv6 protocols.

The procedure and examples in this document use the multiprotocol CLI.

Note You can still use the single-protocol CLI to define an IPv4 address within a VRF and an IPv6 address in the global routing table on the same interface.

BEFORE YOU BEGIN

Review the information in the "Information About VRF-lite" section on page 2 and "Guidelines and Limitations" section on page 3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ipv6 unicast-routing**	Enables IPv6 routing. This command is mandatory for IPv6 routing; IPv4 routing is enabled by default.
Step 3	**vrf definition** *vrf-name*	Names the VRF and enters VRF configuration mode.

	Command	Purpose
Step 4	**rd** *route-distinguisher*	(Optional) Creates a VRF table by specifying a route distinguisher. Enter either an Autonomous System number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Step 5	**address-family** *ipv4* | *ipv6*	(Optional) IPv4 by default. You must specify **ipv6** for IPv6 VRFs.
Step 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	(Optional) Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y). **Note** This command is effective only if BGP is running.
Step 7	**exit-address-family**	Exits from address-family configuration mode.
Step 8	**import map** *route-map*	(Optional) Associates a route map with the VRF.
Step 9	**interface** {*interface-id* | *subinterface-id* | *vlan-id*}	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 10	**vrf forwarding** *vrf-name*	Associates the VRF with the Layer 3 interface.
Step 11	**end**	Returns to privileged EXEC mode.
Step 12	**show vrf [ipv4 | ipv6] [interface | brief | detail | id | select | lock]** [*vrf-name*]	Displays information about the configured VRFs.
Step 13	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no vrf definition** *vrf-name* global configuration command to delete a VRF and to remove all interfaces from it.

Use the **no vrf forwarding** interface configuration command to remove an interface from the VRF.

EXAMPLE

This example configures an IPv6 VRF on an Ethernet interface:

```
Router# configure terminal
Router(config)# ipv6 unicast-routing
Router(config)# vrf definition red
Router(config-vrf)# rd 100:1
Router(config-vrf)# address family ipv6
Router(config-vrf-af)# route-target both 200:1
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# interface Ethernet0/1
Router(config-if)# vrf forwarding red
Router(config-if)# ipv6 address 5000::72B/64
```

This example configures an IPv4 VRF on an Ethernet subinterface:

```
Router# configure terminal
Router(config)# ip routing
Router(config)# vrf definition vrf1
Router(config-vrf)# rd 100:1
Router(config-vrf)# address family ipv4
Router(config-vrf)# route-target export 100:1
Router(config-vrf-af)# exit-address-family
```

```
Router(config-vrf)# interface Fa0/0.1
Router(config-subif)# vrf forwarding vrf1
Router(config-subif)# end
```

This example configures an IPv6 VRF on a VLAN:

```
Router(config)# ipv6 routing
Router(config)# vrf definition red
Router(config-vrf)# rd 100:1
Router(config-vrf)# address family ipv6
Router(config-vrf-af)# route-target both 200:1
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# interface vlan vlan1
Router(config-if)# vrf forwarding red
Router(config-if)# ipv6 address 5000::72B/64
```

Verifying Configuration

Command	Purpose
show vrf [ipv4 | ipv6] [interface | brief | detail | id | select | lock] [*vrf-name***]**	Displays information about the defined VRF instances.
show ip protocols vrf *vrf-name*	Displays routing protocol information associated with a VRF.
show ip route vrf *vrf-name* [**connected] [***protocol* [*as-number*] [**list [***list-number*]] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**][**supernets-only**]	Displays IP routing table information associated with a VRF.
show ipv6 route vrf { *vrf-name* | *vrf-number* } [**tag** { *tag-value* | *tag-value-dotted-decimal* [*mask*] }]	Displays the routing protocol information associated with a VRF.

When you configure VRF table “a” with the IPv6 address family and attach the VRF to the interface with IPv6 address 1::2/64, the **show ipv6 route vrf a** command displays the following output:

```
Router# show ipv6 route vrf a
IPv6 Routing Table - a - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   1::/64 [0/0]
     via GigabitEthernet7/1, directly connected
L   1::2/128 [0/0]
     via GigabitEthernet7/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
Router#
```

Configuration Example

This section shows an example VRF-lite configuration with FlexVPN tunnels. In this example, a CGR 1000 acts as the FlexVPN spoke where end devices such as meters and RTUs are attached. The CGR is connected to redundant ASR hubs and has the following VRFs defined:

- VRF METER is defined for forwarding IPv6 traffic from smart meters through a GRE IPv4 over FlexVPN tunnel.
- VRF RTU is defined for IEC 101 to 104 protocol translation and TCP raw socket traffic. This configuration uses the VRF-aware and VRF-lite features to forward the RTU traffic to redundant hubs over IPSec tunnels.
- VRF CC is defined for forwarding the protocol translation traffic to the SCADA control center.

```
vrf definition METER
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition RTU
 rd 1:5
 !
 address-family ipv4
 exit-address-family
!
vrf definition CC
 rd 1:1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
enable password cisco
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
!
!
!
aaa session-id common
!
!
!
!
!
!
!


!
```

```
!
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username cisco privilege 15 password 0 cisco
!
redundancy
!
crypto ikev2 authorization policy METER-POL
 route set interface
 route set access-list 90
 route set access-list ipv6 IPV6_Default_Route
!
crypto ikev2 authorization policy CC-POL
 route set interface
 route set access-list 90
!
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
 group 2
!
no crypto ikev2 policy default
crypto ikev2 policy p1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile CC
 match fvrf any
 match identity remote address 0.0.0.0
 identity local fqdn 1.scada.com
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 aaa authorization group psk list default CC-POL
 virtual-template 32
!
crypto ikev2 profile METER
 match fvrf any
 match identity remote address 0.0.0.0
 identity local fqdn 1.ams.com
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 aaa authorization group psk list default METER-POL
 virtual-template 2
```

```
!
!
crypto ikev2 dpd 10 3 periodic
!
!
!
!
crypto logging session
!
!
crypto ipsec transform-set trans esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile AMI
 set transform-set trans
 set ikev2-profile METER
!
crypto ipsec profile METER
 set transform-set trans
 set ikev2-profile METER
!
crypto ipsec profile CC
 set transform-set trans
 set ikev2-profile CC
!
!
no crypto ipsec profile default
!
!
!
!
!
!
interface Loopback10
 vrf forwarding METER
 ip address 209.165.200.225 255.255.255.254
 ipv6 address 2001:DB8:1::1/128
 ipv6 enable
!
interface Tunnel0
 no ip address
 shutdown
!
interface Tunnel1
 description Tunnel to ASR-1 for METER
 vrf forwarding METER
 ip address 10.12.8.2 255.255.255.0
 ip tcp adjust-mss 1360
 ipv6 address FE80::10 link-local
 ipv6 enable
 tunnel source GigabitEthernet2/1
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile METER
!
interface Tunnel2
 description Tunnel to ASR-2 for METER
 vrf forwarding METER
 ip address 10.12.9.2 255.255.255.0
 ip tcp adjust-mss 1360
 ipv6 address FE80::20 link-local
 ipv6 enable
 tunnel source GigabitEthernet2/1
 tunnel destination 172.16.1.0
 tunnel protection ipsec profile METER
```

```
!
!
interface Tunnel31
 description Tunnel to ASR-1 for CC
 vrf forwarding RTU
 ip address 10.1.1.1 255.255.255.0
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet2/1
 tunnel mode ipsec ipv4
 tunnel destination 172.17.0.1
 tunnel protection ipsec profile CC
!
interface Tunnel32
 description Tunnel to ASR-2 for CC
 vrf forwarding RTU
 ip address 10.1.20.2 255.255.255.0
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet2/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile CC
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Dot11Radio2/1
 no ip address
 shutdown
 no mop enabled
 no mop sysid
!
interface FastEthernet2/3
 no ip address
!
interface FastEthernet2/4
 no ip address
!
interface FastEthernet2/5
 no ip address
!
interface FastEthernet2/6
 no ip address
!
interface FastEthernet2/7
 no switchport
 vrf forwarding RTU
 ip address 10.31.7.17 255.255.255.252
!
interface FastEthernet2/8
 no ip address
!
interface GigabitEthernet2/1
 no switchport
 ip address dhcp
 duplex auto
 speed auto
 service-policy output OUTBOUND
!
interface GigabitEthernet2/2
 no switchport
 ip address 10.108.1.27 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface Virtual-Template1 type tunnel
 vrf forwarding METER
 ip unnumbered Tunnel1
 ip mtu 1400
 ip tcp adjust-mss 1360
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile AMI
!
interface Virtual-Template2 type tunnel
 vrf forwarding METER
 ip unnumbered Tunnel2
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile AMI
!
interface Virtual-Template31 type tunnel
 vrf forwarding CC
 ip unnumbered Tunnel31
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile CC
!
interface Virtual-Template32 type tunnel
 vrf forwarding CC
 ip unnumbered Tunnel32
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile CC
!
interface Vlan1
 no ip address
!
! Interface used for TCP Raw-sockets
!
interface Async1/1
 vrf forwarding RTU
 ip address 10.31.7.28 255.255.255.252
 encapsulation raw-tcp
 async mode interactive
!
! Interface used for IEC 60870-101 to 104 conversion
!
interface Async1/2
 vrf forwarding CC
 encapsulation scada
 frame-size 512
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
ipv6 access-list FlexVPN_Client_v6_LAN
```

```
 sequence 20 permit ipv6 2001:DB8:0:1:FFFF:1234::/64 any
 permit ipv6 host 2001:DB8:1::1 any
!
ipv6 access-list IPV6_Default_Route
 permit ipv6 2001:DB8:2::1/48 any
!
control-plane
!

!
scada-gw protocol t101
 channel t101_ch1
  link-addr-size two
  bind-to-interface Async1/2
 session t101_ch1_ss1
  attach-to-channel t101_ch1
  link-addr 21
 sector t101_ch1_ss1_sc1
  attach-to-session t101_ch1_ss1
  asdu-addr 21003
scada-gw protocol t104
 channel t104_ch1
  t3-timeout 20
  tcp-connection 0 local-port default remote-ip 10.31.7.49/0 vrf CC
 session t104_ch1_ss1
  attach-to-channel t104_ch1
 sector t104_ch1_ss1_sc1
  attach-to-session t104_ch1_ss1
  asdu-addr 21003
  map-to-sector t101_ch1_ss1_sc1
scada-gw enable
!
!
!
!
line con 0
line 1/1
 raw-socket tcp client 10.31.7.3 5001
 transport preferred none
 transport input all
 parity even
 stopbits 1
line 1/2
 transport preferred none
 transport input all
 stopbits 1
line 1/3 1/4
 transport preferred none
 transport input all
 transport output none
 stopbits 1
line 1/5 1/6
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 password cisco
 transport input all
line vty 5 15
 transport input none
!
!
!
end
```

Related Documents

- FlexVPN Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)
- Cisco IOS Master Command List, All Releases
- IP Routing: BGP Configuration Guide, Cisco IOS Release 15M&T
- IP Routing: OSPF Configuration Guide, Cisco IOS Release 15M&T

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documents" section.