Configuring Route Leaking and Redistribution

This chapter contains the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Route Leaking and Redistribution

Overview of Route Leaking and Redistribution

Route leaking between the global or default VRF (transport VPN) and service VPNs allows you to share common services that multiple VPNs need to access. With this feature, routes are replicated through bidirectional route leaking between the global VRF (also known as transport VPN) and service VPNs. Route leaking between VRFs is done using Routing Information Base (RIB).

Note In the context of Cisco SD-WAN, the terms VRF and VPN are used interchangeably. Although Cisco IOS XE SD-WAN devices use VRFs for segmentation and network isolation, the VPN feature template is used to configure them using Cisco vManage. When you use Cisco vManage to configure VPNs for Cisco IOS XE SD-WAN devices, Cisco vManage automatically converts the VPN configuration to VRF configuration.

To apply the leaked routes to the routing neighbors, you can redistribute the leaked routes between the global VRF and service VPNs. In addition to running multiple routing protocols simultaneously, you can redistribute routes from one routing protocol to another.

Features of Route Leaking and Redistribution

- Leak routes between the global VRF and service VPNs directly.

- Leak multiple service VPNs to the global VRF.

- Apply different route policies using route-map during route replication and redistribution.

- Use route-maps to filter routes using match operations before leaking them.

- Configure these features using both—Cisco vManage and CLI.

- When routes are leaked and redistributed between the global VRF and service VPNs, route properties such as metric, source VPN information, tags, administrative distance, and route origin are retained and carried to the destination protocol.

Typical Use Cases and Benefits

- **Service Provider Central Services:** SP Central services under MPLS can be directly accessed without having to duplicate them for each VPN. This makes accessing central services easier and more efficient.

- **Migration:** With route leaking, branches that have migrated to Cisco SD-WAN can directly access non-migrated branches bypassing the hub, thus providing improved application SLAs.

- **Centralized Network Management:** You can manage the control plane and service-side equipment through the underlay.

How Route Preference is Determined

If a route is replicated or leaked between the global VRF and service VPNs, the following rule determines the route preference.

For a device that receives a route from two sources in which both these routes use the same source VRFs, if one of these routes is replicated, then the non-replicated route is preferred.

If the aforementioned rule doesn't apply, the following rules determine the order of route preference:

1. Prefer the route with smaller administrative distance.

2. Prefer the route with smaller default administrative distance.

3. Prefer a non-replicated route over a replicated route.

4. Compare original VRF-names. Prefer the route with the lexicographically smaller VRF-name.

5. Compare original subaddress families. Prefer unicast routing over multicast routing.

6. Prefer the oldest route.

Supported Protocols

The following protocols are supported for route leaking between the global VRF and service VPNs.

- Connected

- Static

- BGP

- OSPF

- EIGRP

The following protocols are the supported destination and source protocols for route redistribution between the service VPNs and global VRF.

Source Protocols

- Connected

- Static

- BGP

- OSPF

- EIGRP

Destination Protocols

- BGP

- OSPF

- EIGRP

Note   The EIGRP protocol can be used only on service VPNs and not on the global VRF. Therefore, route leaking is supported only for routes from the global VRF to service VPNs.

Restrictions for Route Leaking and Redistribution

- The EIGRP protocol can be used only on service VPNs and not on the global VRF. Therefore, route leaking isn't supported for routes from service VPNs to the global VRF and between service VPNs for the EIGRP protocol.

- Service-side NAT isn't supported with route leaking between the global VRF and service VPNs.

- This feature is specific to leaking routes between the global VRF and service VPNs only and doesn't support route leaking from a service VPN to another service VPN.

- IPv6 address family isn't supported.

- Only prefix-lists, tags, communities, and metrics can be matched in route maps that are used to filter leaked routes.

- While configuring route leaking for a VRF, the `route-replicate` command under the **global-address-family ipv4** command shouldn't have the keyword **all** specified as the protocol for the unicast option to prevent route looping.

```
global-address-family ipv4
   route-replicate from vrf <vrf> unicast all
```

- In this example, the keyword all should be replaced with specific protocol name as shown here:

```
global-address-family ipv4
   route-replicate from vrf <vrf> unicast connected
```

How to Configure Route Leaking and Redistribution

You can leak routes in the global routing table (global VRF) or service VPN, and then redistribute these routes. The following scenarios are supported:

- Leaking and redistribution of routes from a service VPN into the global VRF

- Leaking and redistribution of routes from the global VRF into a service VPN

Configuring Route Leaking and Redistribution from Service VPN into Global VRF

The following procedure shows how to leak and redistribute routes from a service VPN into the global VRF in the BGP protocol.

```
configure terminal
 global-address-family ipv4 unicast
  route-replicate from vrf src-vrf-name unicast src_protocol [src_protocol_id] [route-map
route-map-name]

 router bgp router_instance_id
  address-family ipv4
   redistribute vrf src-vrf-name src_protocol [src_protocol_id] [route-map route-map-name]
```

Note Use the **router ospf** command instead of the **router bgp** command to configure a routing process for the OSPF routing protocol.

The following procedure shows how to leak and redistribute routes from a service VPN into the global VRF in the EIGRP protocol.

```
configure terminal
 global-address-family ipv4 unicast
  route-replicate from vrf src-vrf-name unicast src_protocol [src_protocol_id] [route-map
route-map-name]

 router eigrp autonomous-system-number
  address-family ipv4
   redistribute vrf src-vrf-name src_protocol [src_protocol_id] [metric bandwidth-metric
```

```
delay-metric reliability-metric effective-bandwidth-metric mtu-bytes] [route-map
route-map-name]
```

✎

Note The *src_protocol_id* is optional because static and connected routes do not have the instance IDs. However, BGP, OSPF, and EIGRP have these instance IDs.

Configuring Route Leaking and Redistribution from Global VRF into Service VPN

The following procedure shows how to leak and redistribute routes from the global VRF into a service VPN in the BGP protocol.

```
configure terminal
 vrf definition vrf_name
  address-family ipv4
   route-replicate from vrf global unicast src_protocol [src_protocol_id] [route-map
route-map-name]

 router bgp router_instance_id
  address-family ipv4 vrf vrf_name
   redistribute vrf global src_protocol [src_protocol_id] [route-map route-map-name]
```

The following procedure shows how to leak and redistribute routes from the global VRF into a service VPN in the OSPF protocol.

```
configure terminal
 vrf definition vrf_name
  address-family ipv4
   route-replicate from vrf global unicast src_protocol [src_protocol_id] [route-map
route-map-name]

 router ospf router_instance_id vrf vrf_name
   redistribute vrf global src_protocol [src_protocol_id] [route-map route-map-name]
```

The following procedure shows how to leak and redistribute routes from the global VRF into a service VPN in the EIGRP protocol.

```
configure terminal
 vrf definition vrf_name
  address-family ipv4
   route-replicate from vrf global unicast src_protocol [src_protocol_id] [route-map
route-map-name]

 router eigrp autonomous-system-number
  address-family ipv4 vrf vrf_name
   redistribute vrf global src_protocol [src_protocol_id] [metric bandwidth-metric
delay-metric reliability-metric effective-bandwidth-metric mtu-bytes] [route-map
route-map-name]
```

✎

Note The *src_protocol_id* is optional because static and connected routes do not have the instance IDs. However, BGP, OSPF, and EIGRP have these instance IDs.

Examples: Configure Route Leaking and Redistribution

Example: Leak Routes between Global VRF and Service VPNs

These examples show how to configure route leaking between a global VRF and a service VPN. In this example, VRF 103 is the service VPN. This example shows that the connected routes are leaked into VRF 103 from the global VRF, similarly, the same connected routes are leaked from VRF 103 to the global VRF.

```
vrf definition 103
 !
  address-family ipv4
   route-replicate from vrf global unicast connected
!
global-address-family ipv4
  route-replicate from vrf 103 unicast connected
  exit-address-family
```

Verify Configuration

The following examples shows how to view the leaked routes.

Note In the output, leaked routes are represented by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O 10.1.14.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.15.0/24 is directly connected, GigabitEthernet1
L 10.1.15.15/32 is directly connected, GigabitEthernet1
O 10.1.16.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.17.0/24 is directly connected, GigabitEthernet2
L 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
[170/10880] via 192.168.24.17(103), 01:04:13, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C + 192.0.2.0/24  is directly connected, GigabitEthernet5.103
L & 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 203.0.113.0/24 is directly connected, GigabitEthernet6
L 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
C 198.51.100.0/24 is directly connected, GigabitEthernet7
L 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
O E2 100.100.100.100 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets
O E2 172.16.255.14 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
```

View Routes Leaked From Global VRF to Service VPN

Use the **show ip route vrf** *<vrf id>* command to view the routes leaked from the global VRF to the service VPN.

Note   In the output, leaked routes are denoted by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route vrf 103
Routing Table: 103
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C + 10.0.1.0/24 is directly connected, GigabitEthernet9
L & 10.0.1.15/32 is directly connected, GigabitEthernet9
C + 10.0.20.0/24 is directly connected, GigabitEthernet4
L & 10.0.20.15/32 is directly connected, GigabitEthernet4
C + 10.0.100.0/24 is directly connected, GigabitEthernet8
L & 10.0.100.15/32 is directly connected, GigabitEthernet8
C + 10.1.15.0/24 is directly connected, GigabitEthernet1
L & 10.1.15.15/32 is directly connected, GigabitEthernet1
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
D EX 172.16.20.20
[170/10880] via 192.168.24.17, 01:04:07, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.0/24 is directly connected, GigabitEthernet5.103
L 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 203.0.113.0/24 is directly connected, GigabitEthernet6
L & 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 198.51.100.0/24 is directly connected, GigabitEthernet7
L & 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
```

Example: Filter Routes Before Leaking

To filter the routes leaked between the global VRF and the service VRF, you can apply a route map as shown in this example.

```
vrf definition 103
 !
  address-family ipv4
   route-replicate from vrf global unicast connected route-map myRouteMap permit 10
    match ip address prefix-list pList seq 5 permit 10.1.17.0/24
!
```

Verify Configuration

Note In this output, leaked routes are denoted by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route vrf 103

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C +     10.1.17.0/24 is directly connected, GigabitEthernet2
L &     10.1.17.15/32 is directly connected, GigabitEthernet2
m       10.1.18.0/24 [251/0] via 172.16.255.14, 19:01:28, Sdwan-system-intf
m       10.2.2.0/24 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
m       10.2.3.0/24 [251/0] via 172.16.255.11, 17:26:50, Sdwan-system-intf
C       10.20.24.0/24 is directly connected, GigabitEthernet5
L       10.20.24.15/32 is directly connected, GigabitEthernet5
m       10.20.25.0/24 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
      172.16.0.0/32 is subnetted, 3 subnets
m       172.16.255.112 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
O E2    172.16.255.117 [110/20] via 10.20.24.17, 1d11h, GigabitEthernet5
m       172.16.255.118 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
```

To monitor leaked routes, use the **show ip cef** command. The output shows replicated or leaked routes.

```
Device#show ip cef 10.1.17.0 internal
10.1.17.0/24, epoch 2, flags [rcv], refcnt 6, per-destination sharing
[connected cover 10.1.17.0/24 replicated from 1]
sources: I/F
feature space:
Broker: linked, distributed at 4th priority
subblocks:
gsb Connected receive chain(0): 0x7F6B4315DB80
Interface source: GigabitEthernet5 flags: none flags3: none
Dependent covered prefix type cover need deagg, cover 10.20.24.0/24
```

```
ifnums: (none)
path list 7F6B47831168, 9 locks, per-destination, flags 0x41 [shble, hwcn]
path 7F6B3D9E7B70, share 1/1, type receive, for IPv4
receive for GigabitEthernet5
output chain:
receive
```

Example: Redistribute BGP Route into OSPF and EIGRP Protocols

This example shows how to replicate BGP routes from the global VRF into a service VPN.

```
Device(config)# vrf definition 2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 1
Router(config-ipv4)# commit
```

This example shows how redistribute BGP Routes in the global VRF to EIGRP in the service VPN.

✎

Note The redistribution of BGP routes into other protocols is supported only if the `bgp redistribute-internal` configuration is present in the BGP route.

```
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast vrf 2 autonomous-system 100
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 1 metric 10000 100 200 1
1500
Device(config-ipv4)# commit

* Here we are redistributing BGP routes in global VRF to EIGRP in VRF 2.
* Routes replication must be done before doing inter VRF redistribution.
-----------------------------------------------------------------------------
```

Verify Configuration

View BGP Route is not Present in Global VRF Before Configuring

Use the **show ip route bgp** command to view whether the BGP route is present in the global VRF before configuring.

```
Device#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/9 is subnetted, 1 subnets
B 172.16.255.1 [200/20] via 10.1.15.14, 00:00:25
Device#
```

```
* We have a BGP route in the global VRF.
```

View BGP Route is not Present in Service VPN Before Configuring

Use the **show ip route vrf** *<vrf id>* [**protocol**] command to view the BGP route in the service VPN.

```
Device#show ip route vrf 2 bgp

Routing Table: 2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

Device#

* We do not have any BGP route in VRF 2.
```

View BGP Route After Configuring

Use the **show running config** [*configuration-hierarchy*] | **details** command to verify if the replication configuration exists.

```
Device#show running-config | section vrf definition 2
vrf definition 2
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
  route-replicate from vrf global unicast bgp 1
 exit-address-family
Device#

* We have successfully applied the route-replicate configuration.
* In our example we are replicating bgp 1 routes from global VRF to VRF 2.
-----------------------------------------------------------------------------
```

View BGP Route From Global VRF is Replicated into Service VPN After Configuring

Use the **show ip route vrf** *<vrf id>* [**protocol**] command to view the BGP route in the service VPN.

```
Device#show ip route vrf 2 bgp

Routing Table: 2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
```

```
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

     10.0.0.0/9 is subnetted, 1 subnets
B   +   172.16.255.1 [200/20] via 10.1.15.14, 00:04:01
Device#

* After route replication, we can see that the BGP route in the global VRF has been replicated
 into VRF 2.
* + sign indicates replicated routes.
-------------------------------------------------------------------------------
```

View EIGRP Configuration Without BGP Redistribution Information

```
Device#show running-config | section router eigrp
router eigrp test
 !
 address-family ipv4 unicast vrf 2 autonomous-system 100
  !
  topology base
  exit-af-topology
  network 10.0.0.0
 exit-address-family
Router#
```

View EIGRP Topology Table

Use the **show eigrp address-family ipv4 vrf**<*vrf-num*>**topology** command to view the BGP route in the service VRF table.

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
        Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.0.0/8, 1 successors, FD is 1310720
        via Connected, GigabitEthernet2

Device#

* EIGRP 100 is running on VRF 2.
-------------------------------------------------------------------------------
```

View EIGRP Route After BGP Redistribution

Use the **show eigrp address-family ipv4 vrf**<*vrf-num*>**topology** command to view the BGP route is redistributed into the EIGRP protocol.

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
        Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.0/8, 1 successors, FD is 1310720
        via Connected, GigabitEthernet2
P 172.16.0.0/12, 1 successors, FD is 131072000
        via +Redistributed (131072000/0)

-Device#
```

```
* BGP route has been redistributed into EIGRP.
```
_____

Examples: Configure Route Redistribution

The following is a sample configuration for configuring route redistribution between a global VRF and service VPN.

In this example, VRF 103 and VRF 104 are the service VPNs. The example shows that BGP routes are redistributed from the global VRF to VRF 103 and VRF 104.

```
router bgp 100
 address-family ipv4 vrf 103
  redistribute vrf global bgp 100 route-map test2
!
 address-family ipv4 vrf 104
  redistribute vrf global bgp 100 route-map test2
!
```

The following is a sample configuration for configuring the OSPF internal and external routes that are redistributed from the global VRF 65535 to the service VPN.

In this case, all the OSPF routes are redistributed into the service VPN by using both the **internal** and **external** keywords.

Enter the commands in the configuration mode as follows:

```
router ospf 1
 redistribute vrf global ospf 65535 match internal external 1 external 2 subnets
```

The following is a sample configuration for configuring route redistribution from a service VPN to the global VRF .

```
router bgp 50000
 address-family ipv4
  redistribute vrf 102 bgp 50000 route-map test1
```

The following is a sample configuration for configuring route redistribution of BGP, connected, OSPF, and static protocols from the global VRF to VRF 1 when configuring under the EIGRP routing process.

```
router eigrp 101
 address-family ipv4 vrf 1
  redistribute vrf global bgp 50000 metric 1000000 10 255 1 1500
  redistribute vrf global connected metric 1000000 10 255 1 1500
  redistribute vrf global ospf 65535 match internal external 1 external 2 metric 1000000
10 255 1 1500
  redistribute vrf global static metric 1000000 10 255 1 1500
```

Verify Route Redistribution

The following example shows the output for the **show ip bgp** command using the **internal** keyword. This example shows a route from VRF 102 is redistributed successfully to the global VRF after the route is replicated.

```
Device# show ip bgp 10.10.10.10 internal

BGP routing table entry for 10.10.10.10/8, version 515
Paths: (1 available, best #1, table default)
Not advertised to any peer
```

```
Refresh Epoch 1
700000 70707
10.10.14.17 from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 77775522, metric 7777, localpref 100, weight 32768, valid, sourced,
 replicated, best
Community: 0:7227 65535:65535
Extended Community: SoO:721:75 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB320235DC0, path: 0x7FB320245DF8, pathext: 0x7FB3203A4660
flags: net: 0x0, path: 0x808040003, pathext: 0x81
attribute: 0x7FB38E5B6258, ref: 14
Updated on Jul 1 2021 01:16:36 UTC
vm5#
```

The following example shows the output for the **show ip route** command to view the routes replicated for the redistribution.

```
Device# show ip route 10.10.10.10

Routing entry for 10.10.10.10/8
Known via "bgp 50000", distance 60, metric 7777
Tag 700000, type external,
replicated from topology(102)
Redistributing via ospf 65535, bgp 50000
Advertised by ospf 65535
bgp 50000 (self originated)
Last update from 10.10.14.17 5d15h ago
Routing Descriptor Blocks:
* 10.10.14.17 (102), from 10.10.14.17, 5d15h ago
opaque_ptr 0x7FB3202563A8
Route metric is 7777, traffic share count is 1
AS Hops 2
Route tag 700000
MPLS label: none
```

The following example shows the output for the **show ip bgp vpnv4 vrf** command using the **internal** keyword. In this output, the route is redistributed from the global VRF to VRF 102.

```
Device# show ip bgp vpnv4 vrf 102 209.165.201.0 internal

BGP routing table entry for 1:102:10.10.10.10/8, version 679
BGP routing table entry for 1:209.165.201.0/27, version 679
Paths: (1 available, best #1, table 102)
Advertised to update-groups:
4
Refresh Epoch 1
7111 300000
10.1.15.13 (via default) from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 5755, metric 900, localpref 300, weight 32768, valid, sourced,
replicated, best
Community: 555:666
Large Community: 1:2:3 5:6:7 412789:412780:755
Extended Community: SoO:533:53 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB38E5C5718, path: 0x7FB3202668D8, pathext: 0x7FB38E69E960
flags: net: 0x0, path: 0x808040007, pathext: 0x181
attribute: 0x7FB320256798, ref: 7
Updated on Jul 6 2021 16:43:04 UTC
```

The following example show the output for the **show ip route vrf** *vrf-id* [**protocol**] command. In this output, you can view the leaked routes for redistribution.

```
Device# show ip route vrf 102 209.165.201.0

Routing Table: 102
```

```
Routing entry for 209.165.201.0/27
Known via "bgp 50000", distance 20, metric 900
Tag 7111, type external,
replicated from topology(default)
Redistributing via bgp 50000
Advertised by bgp 50000 (self originated)
Last update from 10.1.15.13 00:04:57 ago
Routing Descriptor Blocks:
* 10.1.15.13 (default), from 10.1.15.13, 00:04:57 ago
opaque_ptr 0x7FB38E5B5E98
Route metric is 900, traffic share count is 1
AS Hops 2
Route tag 7111
MPLS label: none
```

Examples: Configure Route Leaking and Redistribution

This example shows how to leak and redistribute routes from VRF 1 and VRF 2 into Global VRF.

```
configure terminal
 global-address-family ipv4 unicast
  route-replicate from vrf 1 unicast bgp 100 route-map foo1
  route-replicate from vrf 2 unicast bgp 100 route-map foo1

router bgp 100
 address-family ipv4
  redistribute vrf 1 bgp 100 route-map foo1
  redistribute vrf 2 bgp 100 route-map foo1
```

This example shows how to leak and redistribute routes from global VRF into VRF 1 and VRF 2.

```
configure terminal
 vrf definition 1
  address-family ipv4
   route-replicate from vrf global unicast bgp 100 route-map foo1

 vrf definition 2
  address-family ipv4
   route-replicate from vrf global unicast bgp 100 route-map foo1


  router bgp 100
   address-family ipv4 vrf 1
    redistribute bgp 100 route-map foo1

   address-family ipv4 vrf 2
    redistribute bgp 100 route-map foo1
```

Feature Information for Route Leaking and Redistribution Between Global VRF and Service VPNs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information

Feature Name	Release Information	Description
Route Leaking Between Global VRF and Service VPNs	Cisco IOS XE Release 17.3.1a	This feature enables you to leak routes bidirectionally between the global VRF and service VPNs. Route leaking allows service sharing and is beneficial in migration use cases because it allows bypassing hubs and provides migrated branches direct access to non-migrated branches.
Redistribution of Replicated BGP Routes to OSPF, EIGRP Protocols	Cisco IOS XE Release 17.5.1a	This feature allows you to leak (or replicate) BGP routes between the global VRF and service VPNs, and redistribute the leaked BGP routes. The redistribution of the leaked routes to the EIGRP and OSPF protocols occurs after replicating the BGP routes into the corresponding VRF.
Redistribution of replicated routes into BGP	Cisco IOS XE Bengaluru Release 17.6.1	This feature allows you to leak (or replicate) routes between the global VRF and service VPNs, and redistribute the leaked routes into BGP. The redistribution of the leaked routes occurs after replicating the routes into the corresponding VRF.