在IOS XE上配置VRF泄漏

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

场景1 - BGP和IGP之间的VRF路由泄漏(EIGRP)

- 网络图
- 配置
- 验证

场景2 - VRF A和VRF B之间的VRF泄漏

- 网络图
- 配置
- 验证

场景3 — 使用BGP的OSPF(VRF)和EIGRP（全局）之间的VRF泄漏（可选）

- 网络图
- 配置
- 验证

场景4 — 从OSPF到BGP的VRF默认路由泄漏

- 网络图
- 配置
- 验证

其它资源

简介

本文档介绍并提供虚拟路由和转发(VRF)路由泄漏的常用方法的配置示例。

先决条件

要求

Cisco 建议您了解以下主题：

- 边界网关协议 (BGP)
- 路由协议再分配
- VRF
- Cisco IOS® XE软件

有关这些主题的详细信息：

- 重分布路由协议
- 在 EIGRP 与 BGP 之间相互再分配的配置示例
- 了解OSPF路由重分发到BGP

使用的组件

本文档中的信息基于使用Cisco IOS® XE版本16.12.X和17.X的路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

VRF允许路由器为不同的虚拟网络维护单独的路由表。需要例外时，VRF路由泄漏允许在VRF之间路由某些流量，而不使用静态路由。

场景1 - BGP和IGP之间的VRF路由泄漏(EIGRP)

场景1提供在BGP和EIGRP之间泄漏VRF路由的示例。此方法可用于其他IGP。

网络图

图1中的网络图显示了需要路由泄漏的第3层拓扑。

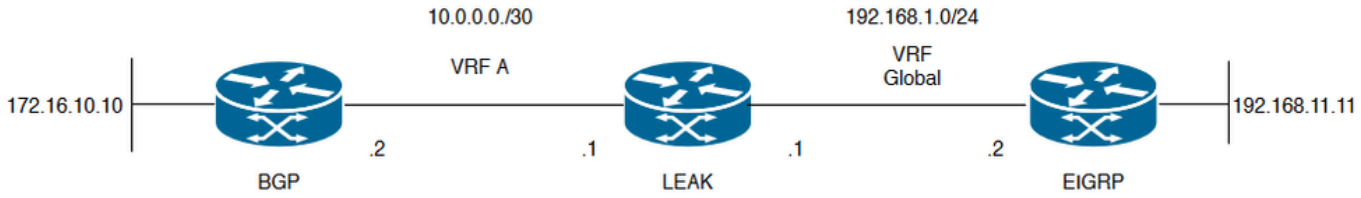


图 1:场景1的路由泄漏拓扑。

路由器泄漏具有到VRF A中邻居的BGP邻居关系，以及全局VRF中的EIGRP邻居关系。设备192.168.11.11必须通过网络连接到设备172.16.10.10。

由于路由位于不同的VRF中，路由器LEAK无法在两者之间进行路由。这些路由表显示每个VRF的当前路由，并指出哪些路由必须在全局VRF和VRF A之间泄漏。

泄漏路由表：

EIGRP路由表（全局路由）

<#root>

LEAK#

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet2
```

```
L 192.168.1.1/32 is directly connected, GigabitEthernet2
192.168.11.0/32 is subnetted, 1 subnets

D 192.168.11.11 [90/130816] via 192.168.1.2, 02:30:29, GigabitEthernet2

>> Route to be exchange to the VRF A routing table.
```

VRF A路由表

<#root>

```
LEAK#

show ip route vrf A



Routing Table: A
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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets

B 172.16.10.10 [200/0] via 10.0.0.2, 01:47:58

>> Route to be exchange to the global routing table.
```

配置

完成创建两个路由表之间泄漏的过程：

<#root>

Step 1.

Create route-maps to filter the routes to be injected in both routing tables.

LEAK(config)#

Route-map VRF_TO_EIGRP

LEAK(config-route-map)#

match ip address prefix-list VRF_TO_EIGRP

LEAK(config-route-map)#

exit

!

Prefix-list created to match the host that is attached to the previous route-map configured

.
!

ip prefix-list VRF_TO_EIGRP permit 172.16.10.10/32

or

LEAK(config)#

Route-map VRF_TO_EIGRP

LEAK(config-route-map)#

match ip address 10

LEAK(config-route-map)#

exit

!

ACL created to match the host that is attached to the previous route-map.
!
LEAK#

show ip access-lists 10

10 permit 172.16.10.10

LEAK(config)#

Route-map EIGRP_TO_VRF

LEAK(config-route-map)#

match ip address prefix-list EIGRP_TO_VRF

LEAK(config-route-map)#

exit

LEAK(config)#
!
Prefix-list created to match the host that is attached to the previous route-map configured

.

!

ip prefix-list EIGRP_TO_VRF permit 192.168.11.11/32

or

LEAK(config)#

Route-map EIGRP_TO_VRF

LEAK(config-route-map)#

match ip address 20

LEAK(config-route-map)#

exit

LEAK(config)#
!
ACL created to match the host that is attached to the previous route-map.
!
LEAK#

show ip access-list 20

10 permit 192.168.11.11

Step 2.

Define the import/export maps and add the route-map names.

LEAK(config)#

vrf definition A

LEAK(config-vrf)#

address-family ipv4

LEAK(config-vrf-af)#

import ipv4 unicast map EIGRP_TO_VRF

>> Import the global routing table routes at the VRF routing table.
LEAK(config-vrf-af)#

export ipv4 unicast map VRF_TO_EIGRP

>> Export the VRF routes to the Global Routing Table.
LEAK(config-vrf-af)#

end

Step 3.

Proceed with the dual redistribution.

Redistribute EIGRP

```
LEAK(config)#
router bgp 1

LEAK(config-router)#
redistribute eigrp 1

LEAK(config-router)#
end
```

Redistribution BGP

```
LEAK(config)#
router eigrp 1

LEAK(config-router)#
redistribute bgp 1 metric 100 1 255 1 1500

LEAK(config-router)#
end
```

验证

<#root>

```
Routing table from VRF A

LEAK#
show ip route vrf A
```

```
Routing Table: A

< Snip for resume >

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets
B 172.16.10.10 [200/0] via 10.0.0.2, 00:58:53
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
B 192.168.1.0/24 is directly connected, 00:01:00, GigabitEthernet2
L 192.168.1.1/32 is directly connected, GigabitEthernet2
192.168.11.0/32 is subnetted, 1 subnets

B 192.168.11.11 [20/130816] via 192.168.1.2, 00:01:00, GigabitEthernet2


 >> Route from global routing table at VRF A routing table.


Global Routing Table (EIGRP)



LEAK#

show ip route



< snip for resume >

Gateway of last resort is not set

172.16.0.0/32 is subnetted, 1 subnets

B 172.16.10.10 [200/0] via 10.0.0.2 (A), 00:04:47


>> Route from VRF A at global routing table.
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet2
L 192.168.1.1/32 is directly connected, GigabitEthernet2
192.168.11.0/32 is subnetted, 1 subnets
D 192.168.11.11 [90/130816] via 192.168.1.2, 01:03:35, GigabitEthernet2
LEAK#
```

场景2 - VRF A和VRF B之间的VRF泄漏

场景2描述了两个不同VRF之间的泄漏。

网络图

本文档介绍了此网络设置的用途：

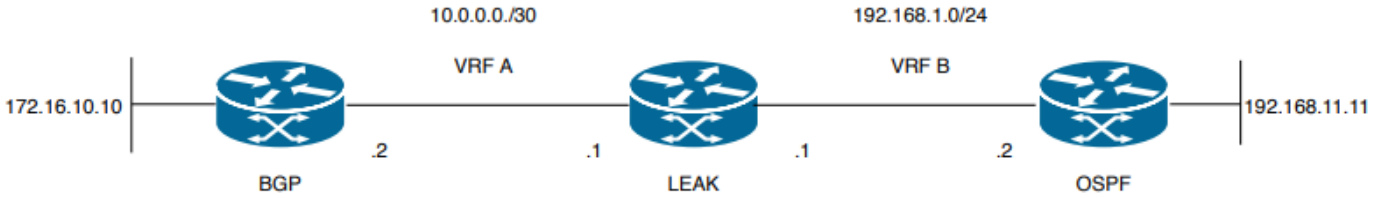


图 2:场景2的路由泄漏拓扑。

路由器泄漏具有到VRF A中邻居的BGP邻居关系，以及VRF B中的OSPF邻居。设备192.168.11.11必须通过网络连接到设备172.16.10.10。

由于路由位于不同的VRF中，路由器LEAK无法在两者之间进行路由。这些路由表显示每个VRF的当前路由，并指明哪些路由必须在VRF A和VRF B之间泄漏。

泄漏路由表：

VRF A路由表

<#root>

LEAK#

show ip route vrf A

```
Routing Table: A
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
```

```
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, Ethernet0/0
L 10.0.0.2/32 is directly connected, Ethernet0/0
172.16.0.0/32 is subnetted, 1 subnets

B 172.16.10.10 [200/0] via 10.0.0.1, 00:03:08

 >> Route to be exchange to routing table VRF B.
```

VRF B路由表

<#root>

```
LEAK#

show ip route vrf B



Routing Table: B
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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/1
L 192.168.1.2/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets

O 192.168.11.11 [110/11] via 192.168.1.1, 00:58:45, Ethernet0/1

 >> Route to be exchange to routing table VRF A

.
```

配置

完成以下步骤以创建两个路由表之间的泄漏：

<#root>

Step 1.

Create route-maps to filter the routes to be injected in both routing tables.

LEAK(config)#

Route-map VRFA_TO_VRFB

LEAK(config-route-map)#

match ip address prefix-list VRFA_TO_VRFB

LEAK(config-route-map)#

exit

!
Prefix-list created to match the host and IP segment that is attached to the previous route-map configu

.

!

ip prefix-list VRFA_TO_VRFB permit 172.16.10.10/32

ip prefix-list VRFA_TO_VRFB permit 10.0.0.0/30

or

LEAK(config)#

Route-map VRFA_TO_VRFB

LEAK(config-route-map)#

match ip address 10

LEAK(config-route-map)#

exit

!
ACL created to match the host and IP segment that is attached to the previous route-map.
!
LEAK#

show ip access-lists 10

10 permit 172.16.10.10
20 permit 10.0.0.0

LEAK(config)#

Route-map VRFB_TO_VRFA

LEAK(config-route-map)#

match ip address prefix-list VRFB_TO_VRFA

LEAK(config-route-map)#

exit

!
Prefix-list created to match the host and IP segment that is attached to the previous route-map configu

.

!

ip prefix-list VRFB_TO_VRFA permit 192.168.11.11/32

ip prefix-list VRFB_TO_VRFA permit 192.168.1.0/24

or

```
LEAK(config)#
```

Route-map VRFB_TO_VRFA

```
LEAK(config-route-map)#
```

match ip address 20

```
LEAK(config-route-map)#
```

exit

```
!
ACL created to match the host and IP segment that is attached to the previous route-map configured.
!
LEAK#
```

show ip access-lists 20

```
10 permit 192.168.11.11
20 permit 192.168.1.0
```

Step 2.

At the VRFs configure the import/export map, use the route-map names to leak the routes.

```
LEAK(config)#
```

vrf definition A

```
LEAK(config-vrf)#
```

address-family ipv4

```
LEAK(config-vrf-af)#
```

export map VRFA_TO_VRFB

```
LEAK(config-vrf-af)#
```

import map VRFB_TO_VRFA

```
LEAK(config)#
vrf definition B

LEAK(config-vrf)#
address-family ipv4

LEAK(config-vrf-af)#
export map VRFB_TO_VRFA

LEAK(config-vrf-af)#
import map VRFA_TO_VRFB
```

Step 3.

Add the route-target to import and export the route distinguisher from both VRFs.

```
! --- Current configuration for VRF A

vrf definition A
rd 1:2
!
address-family ipv4
route-target export 1:2
route-target import 1:1
exit-address-family

! --- Current configuration from VRF B

vrf definition B
rd 2:2
!
address-family ipv4
exit-address-family

! --- Import the routes from VRF  B into VRF A

LEAK(config)#
vrf definition A

LEAK(config-vrf)#
```

address-family ipv4

LEAK(config-vrf-af)#

route-target

import 2:2

! --- Import routes from VRF A to VRF B and export routes from VRF B

LEAK(config-vrf-af)#

vrf definition B

LEAK(config-vrf)#

address-family ipv4

LEAK(config-vrf-af)#

route-target import 1:2

LEAK(config-vrf-af)#

route-target export 2:2

验证

<#root>

Check the Routing Tables

VRF A Routing Table

LEAK#

show ip route vrf A

```
Routing Table: A

< Snip for resume >

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, Ethernet0/0
L 10.0.0.2/32 is directly connected, Ethernet0/0
172.16.0.0/32 is subnetted, 1 subnets
B 172.16.10.10 [200/0] via 10.0.0.1, 00:07:20
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
B 192.168.1.0/24 is directly connected, 00:00:10, Ethernet0/1
L 192.168.1.2/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets
```

B 192.168.11.11 [20/11] via 192.168.1.1 (B), 00:00:10, Ethernet0/1

```
 >> Route from VRF B routing table at VRF A.
```

VRF B Routing Table

```
LEAK#
```

show ip route vrf B

```
Routing Table: B

< Snip for resume >

10.0.0.0/30 is subnetted, 1 subnets
B 10.0.0.0 [200/0] via 10.0.0.1 (A), 00:00:15
172.16.0.0/32 is subnetted, 1 subnets
```

B 172.16.10.10 [200/0] via 10.0.0.1 (A), 00:00:15

```
 >> Route from VRF A routing table at VRF B.
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/1
L 192.168.1.2/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets
O 192.168.11.11 [110/11] via 192.168.1.1, 01:05:12, Ethernet0/1
```

场景3 — 使用BGP的OSPF(VRF)和EIGRP（全局）之间的VRF泄漏（可选）

场景3描述了两个IGP（VRF B和全局VRF）之间的路由泄漏。

网络图

本文档使用以下网络设置：

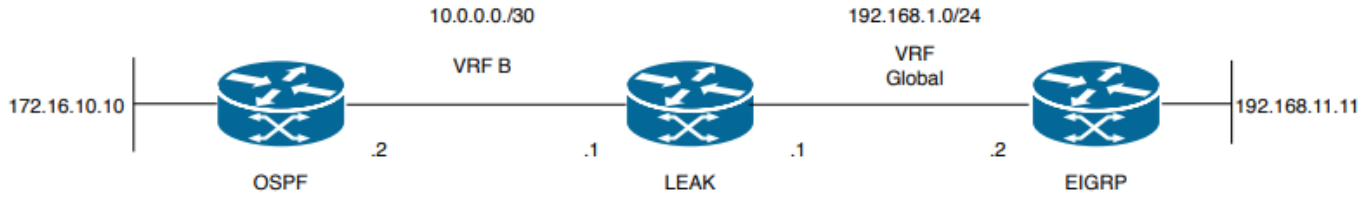


图 3:场景3的路由泄漏拓扑。

路由器泄漏与VRF B中的邻居具有OSPF邻居关系，而全局VRF中具有EIGRP邻居关系。设备172.16.10.10必须通过网络连接到设备192.168.11.11。

路由器LEAK无法连接到这两台主机。这些路由表显示每个VRF的当前路由，并指明哪些路由必须在VRF B和全局VRF之间泄漏。

泄漏路由表：

EIGRP路由表(EIGRP)

<#root>

LEAK#

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/1
L 192.168.1.1/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets
```

D 192.168.11.11 [90/1024640] via 192.168.1.2, 01:08:38, Ethernet0/1 >> Route to be exchange from global

VRF B路由表(OSPF)

<#root>

LEAK#

show ip route vrf B

```
Routing Table: B
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

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, Ethernet0/0
L 10.0.0.2/32 is directly connected, Ethernet0/0
172.16.0.0/32 is subnetted, 1 subnets
```

O 172.16.10.10 [110/11] via 10.0.0.1, 01:43:45, Ethernet0/0 >> Route to be exchange from routing table V

配置

完成以下步骤以创建两个路由表之间的泄漏：

<#root>

Step 1.

Create route-maps for import and export to be injected in both routing tables.

LEAK(config)#

Route-map OSPF_TO_EIGRP

LEAK(config-route-map)#

match ip address prefix-list OSPF_TO_EIGRP

LEAK(config-route-map)#

exit

!
Prefix-list created to match the host that is attached to the previous route-map configured.
!

ip prefix-list OSPF_TO_EIGRP permit 172.16.10.10/32

ip prefix-list OSPF_TO_EIGRP permit 10.0.0.0/30

or

LEAK(config)#

Route-map OSPF_TO_EIGRP

LEAK(config-route-map)#

match ip address 10

LEAK(config-route-map)#

exit

!
ACL created to match the host that is attached to the previous route-map.

!
LEAK#

show ip access-lists 10

10 permit 172.16.10.10
20 permit 10.0.0.0

LEAK(config)#

Route-map EIGRP_TO_OSPF

LEAK(config-route-map)#

match ip address prefix-list EIGRP_TO_OSPF

LEAK(config-route-map)#

exit

!
Prefix-list created to match the host that is attached to the previous route-map configured.
!

ip prefix-list EIGRP_TO_OSPF permit 192.168.11.11/32

ip prefix-list EIGRP_TO_OSPF permit 192.168.1.0/24

or

LEAK(config)#

Route-map EIGRP_TO_OSPF

LEAK(config-route-map)#

match ip address 20

LEAK(config-route-map)#

exit

```
!
ACL created to match the host that is attached to the previous route-map.
!
LEAK#
```

show ip access-lists 20

```
10 permit 192.168.11.11
20 permit 192.168.1.0/24
```

Step 2.

Add the import/export maps in order to match the route-map names.

```
Current configuration
!
vrf definition B
rd 1:2
!
address-family ipv4
exit-address-family
!
!
LEAK(config-vrf)#
```

vrf definition B

```
LEAK(config-vrf)#
```

address-family ipv4

```
LEAK(config-vrf-af)#
```

import ipv4 unicast map EIGRP_TO_OSPF

```
LEAK(config-vrf-af)#
```

export ipv4 unicast map OSPF_TO_EIGRP

Step 3.

To perform the leak is necessary to create a BGP process, in order to redistribute the IGPs protocols.

```
router bgp 1
```

```
bgp log-neighbor-changes
!
```

address-family ipv4 vrf B >> Include the address-family to inject VRF B routing table (OSPF)

```
!
exit-address-family
```

注意：确保VRF配置了路由标识符以避免错误：
%vrf B未配置rd，请在配置导入路由映射之前配置“rd”。

<#root>

Step 4.

Create a Dual Redistribution.

IGPs redistribution.

LEAK(config-router)#

router bgp 1

LEAK(config-router)#

redistribute eigrp 1

```
!
LEAK(config-router)#
```

address-family ipv4 vrf B

LEAK(config-router-af)#

redistribute ospf 1 match internal external 1 external 2

LEAK(config-router-af)#

end

BGP Redistribution

```
LEAK(config)#

router ospf 1 vrf B


LEAK(config-router)#

redistribute bgp 1


!
LEAK(config-router)#

router eigrp TAC


LEAK(config-router)#
LEAK(config-router)#

address-family ipv4 unicast autonomous-system 1


LEAK(config-router-af)#
LEAK(config-router-af)#

topology base


LEAK(config-router-af-topology)#

redistribute bgp 1 metric 100 1 255 1 1500
```

验证

检查路由表：

全局路由表

<#root>

```
LEAK#

show ip route


< Snip for resume >
```

```
172.16.0.0/32 is subnetted, 1 subnets

B 172.16.10.10 [20/11] via 10.0.0.1, 00:14:48, Ethernet0/0 >> Route from VRF B routing table at global r


192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Ethernet0/1
L 192.168.1.1/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets
D 192.168.11.11 [90/1024640] via 192.168.1.2, 02:16:51, Ethernet0/1
```

VRF B路由表

<#root>

```
LEAK#

show ip route vrf B


Routing Table: B

< Snip for resume >

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, Ethernet0/0
L 10.0.0.2/32 is directly connected, Ethernet0/0
172.16.0.0/32 is subnetted, 1 subnets
O 172.16.10.10 [110/11] via 10.0.0.1, 00:34:25, Ethernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
B 192.168.1.0/24 is directly connected, 00:08:51, Ethernet0/1
L 192.168.1.1/32 is directly connected, Ethernet0/1
192.168.11.0/32 is subnetted, 1 subnets

B 192.168.11.11 [20/1024640] via 192.168.1.2, 00:08:51, Ethernet0/1 >> Route from global routing table (
```

场景4 — 从OSPF到BGP的VRF默认路由泄漏

场景4提供了从OSPF到BGP的VRF默认路由泄漏示例。

网络图

图4中的网络图显示了需要默认路由泄漏的第3层拓扑。

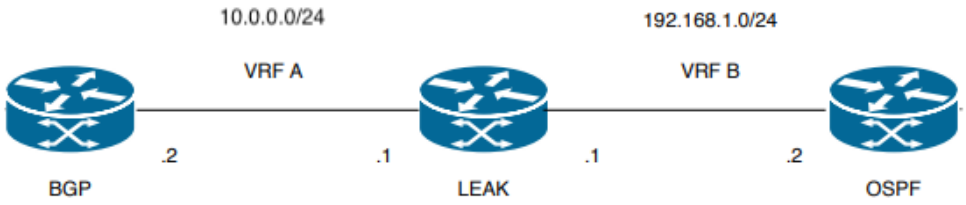


图 4:场景4的路由泄漏拓扑

OSPF和BGP进程在路由器泄漏的其他VRF中运行。路由器OSPF中存在默认路由。路由器泄漏在VRF A中具有与路由器BGP的BGP邻居关系，在VRF B中具有与路由器OSPF的OSPF邻居关系。

在下一个配置步骤中，演示了从OSPF到BGP的默认路由器泄漏到路由器LEAK。

配置

<#root>

Step 1

Check if a static default route is present in Router OSPF.

OSPF#sh ip route

<output snipped>

Gateway of last resort is 192.168.10.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.10.2

>>> default route is present in the routing table.
C 192.168.0.0/24 is directly connected, GigabitEthernet2
L 192.168.0.2/32 is directly connected, GigabitEthernet2
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet1
L 192.168.10.1/32 is directly connected, GigabitEthernet1

Step 2

From the OSPF router, the default route needs to be advertised in OSPF to Router LEAK.

Use the command "default-information originate" on Router OSPF under OSPF process:(if there is static

```
OSPF(config)#router ospf 1
OSPF(config-router)#default-information originate
```

If there is no static route in the Router OSPF routing table then we can generate and advertise a defau

```
OSPF(config)#router ospf 1
OSPF(config-router)#default-information originate always
```

This forces the router to advertise a default route even if it doesn't have one in its routing table.

Step 3.1

Verify on Router LEAK, if an external OE2 route is installed in the VRF B routing table:

```
LEAK#sh ip route VRF B

Routing Table: B

<output snipped>

Gateway of last resort is 192.168.0.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.0.2, 00:05:51, GigabitEthernet2

 >>> OE2 route is installed in the VRF B routing table (This needs to be leaked in BGP)
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet2
L 192.168.0.1/32 is directly connected, GigabitEthernet2
```

Step 3.2

Configure a prefix-list on Router LEAK

```
LEAK# conf t
LEAK(config)# ip prefix-list OSPF_TO_BGP seq 5 permit 0.0.0.0/0
```

Configure a route-map to match the prefix-list.

```
LEAK(config-route-map)#route-map OSPF_TO_BGP permit 10
LEAK(config-route-map)# match ip address prefix-list OSPF_TO_BGP
LEAK(config-route-map)#exit
```

Step 3.3

Verify on Router LEAK, that required VRFs , Route Distinguishers (RD) an Route Targets (RT) are configu

```
LEAK(config)#vrf definition A
LEAK(config-vrf)#rd 1:1
LEAK(config-vrf)#address-family ipv4
LEAK(config-vrf-af)#route-target import 6500:1
```

```
LEAK(config-vrf-af)#exit-address-family
LEAK(config-vrf-af)#end
LEAK#

LEAK(config)#vrf definition B
LEAK(config-vrf)#rd 2:2
LEAK(config-vrf)#address-family ipv4
LEAK(config-vrf-af)#route-target export 6500:1
LEAK(config-vrf-af)#exit-address-family
LEAK(config-vrf-af)#end
LEAK#
```

Step 3.4

Configure import map in VRF A.

```
LEAK#conf t
LEAK(config)#vrf definition A
LEAK(config-vrf)#address-family ipv4
LEAK(config-vrf-af)#import map OSPF_TO_BGP
LEAK(config-vrf-af)#end
LEAK#
```

Step 3.5

Create an address family VRF B in the BGP configuration and advertise “0.0.0.0”

```
LEAK#sh run | sec bgp
redistribute bgp 6501
router bgp 6501
bgp router-id 10.0.0.1
bgp log-neighbor-changes
!
address-family ipv4 vrf A
neighbor 10.0.0.2 remote-as 6500
neighbor 10.0.0.2 activate
exit-address-family
!
address-family ipv4 vrf B
network 0.0.0.0
exit-address-family
```



注意：在BGP内创建地址系列VRF无需激活任何邻居。只需生成BGP进程即可泄露VRF之间的路由。

验证

<#root>

Verify the default route available in BGP.

LEAK#sh ip route vrf A

Routing Table: A

<output snipped>

Gateway of last resort is 192.168.0.2 to network 0.0.0.0

B* 0.0.0.0/0 [20/1] via 192.168.0.2 (B), 00:15:36, GigabitEthernet2

>>> Default route of VRF B routing table in VRF A routing table.
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/24 is directly connected, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1

其它资源

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。