对FlexVPN软的迁移配置示例的DMVPN

目录

简介

本文描述如何进行动态多点VPN (DMVPN)和FlexVPN在同时设备工作，不用需要对于应急方案的*软的*迁移并且提供配置示例。

> **Note**:本文在FlexVPN迁移描述的概念展开：从DMVPN的硬移动到在同样设备和FlexVPN迁移的FlexVPN ：从DMVPN的硬移动到在一台不同的集线器Cisco条款的FlexVPN。这两个文档描述*硬*迁移，导致若干中断流量在迁移时。在这些条款的限制归结于缺乏在当前被纠正的Cisco IOS软件方面。

先决条件

要求

Cisco 建议您了解以下主题：

- DMVPN
- FlexVPN

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成多业务路由器(ISR)版本15.3(3)M或以上
- Cisco 1000系列聚集的服务路由器(ASR1K)版本3.10或以上

> **Note**:不是所有的软件和硬件支持互联网密钥交换版本2 (IKEv2)。参考Cisco Feature Navigator信息。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

其中一个更新的Cisco IOS平台和软件的优点是能力使用下一代加密算法。示例是使用在Galois/计数器模式(GCM)的高级加密标准(AES)加密的在IPsec，如RFC 4106所述。AES GCM准许在一些硬件的更加快速的加密速度。

> **Note**:关于对下一代加密算法的使用和迁移的更多信息，参考下一代加密Cisco条款。

配置

因为两设计类似，运作此配置示例着重从DMVPN相位3配置的迁移到FlexVPN。

	DMVPN第2阶段	DMVPN相位3	FlexVPN
传输	IPSec的GRE	IPSec的GRE	IPSec的GRE， VTI
NHRP使用情况	注册和解决方法	注册和解决方法	解决方法
从分支的下一跳	其他Spoke或集线器	从集线器的摘要	从集线器的摘要
NHRP快捷方式交换	无	是	是(可选)
NHRP重定向	无	是	是
IKE和IPsec	可选的IPsec， IKEv1典型	可选的IPsec， IKEv1典型	IPsec， IKEv2

网络图

此部分提供传输和重叠网络图。

传输网络图表

用于此示例的传输网络包括有连接的两个spoke的一个单台集线器。所有设备通过模拟互联网的网络连接。

重叠网络图

用于此示例的覆盖网络包括有连接的两个spoke的一个单台集线器。 切记DMVPN和FlexVPN同时是活跃的，但是他们使用不同的IP地址空间。

配置

此配置通过增强的内部网关路由选择协议(EIGRP)移植DMVPN相位3的最普遍的部署到与边界网关协议(BGP)的FlexVPN。 因为允许部署扩展更加好，思科推荐使用BGP与FlexVPN。

> **Note**:集线器终止同样IP地址的IKEv1 (DMVPN)和IKEv2 (FlexVPN)会话。这对最近的Cisco IOS版本是仅可能的。

分支配置

这是一个非常基本配置，有允许IKEv1和IKEv2的配合动作的两值得注意的例外，以及使用在IPsec的通用路由封装(GRE)传输为了共存的两个框架。

> **Note**:对互联网安全协会和密钥管理协议(ISAKMP)的相关更改和IKEv2配置用黑体字表示。

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

crypto logging session

crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto isakmp policy 10
encr aes
authentication pre-share
```

```
crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub tunnel
ip address negotiated
ip mtu 1400
 ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2



interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS版本15.3允许您在*通道保护配置里*配合IKEv2和ISAKMP配置文件。 与对代码的一些内部更改一起，这允许IKEv1和IKEv2同时起作用同一个设备。

由于方式Cisco IOS选择配置文件(IKEv1或IKEv2)在版本早于15.3，它导致了一些警告，例如IKEv1启动对IKEv2通过对等体的情况。IKE的分离没有根据配置文件级别当前，没有interface-level，通过新的CLI达到。

在新型Cisco IOS版本的另一升级是*通道密钥的*新增内容。因为DMVPN和FlexVPN使用同一个源接口和同样目的IP地址，这是需要的。使用此到位，没有办法知道的GRE隧道哪个隧道接口用于为了解封装流量。通道密钥允许您区分**隧道0**和**tunnel1**增加一笔小(4字节)开销。 不同的密钥在两个接口可以配置，但是您典型地只需要区分一个通道。

Note:当DMVPN和FlexVPN共享同一个接口时，共享通道保护选项没有要求。

因此，分支路由协议配置基本。EIGRP和BGP分开运作。 EIGRP在隧道接口仅通告为了避免并列在spoke-to-spoke通道，限制可扩展性。 BGP维护一仅关系用中心路由器(**10.1.1.1**)为了通告本地网络(**192.168.101.0/24**)。

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

中心配置

您在集线器端配置必须做相似的变动作为描述的那些在**辐条配置**部分。

Note:对ISAKMP的相关更改和IKEV2配置用黑体字表示。

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
```

```
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

在集线器端，约束在IKE配置文件和IPSec简档之间发生在配置文件级别，不同于辐条配置，这通过**tunnel protection命令**完成。 两个途径是完成此约束的可行的方法。

请注意下一跳解析协议(NHRP)网络ID为DMVPN和FlexVPN是不同的在网云。当NHRP创建在两个框架时的单个域在大多数情况下，它是不理想的。

通道密钥区分DMVPN和FlexVPN通道在Gre级别为了达到在**辐条配置**部分被提及的同一个目标。

在集线器的路由配置相当基本。集线器设备维护与使用EIGRP使用BGP的任何给的分支，一个和一个的两关系。 BGP配置使用侦听范围为了避免较，每分支配置。

summary-address两次介绍。EIGRP配置发送与使用的一摘要**隧道0**配置(Ip summary-address eigrp 100)，并且BGP引入与使用的一摘要aggregate-address。 摘要要求为了保证NHRP重定向发生，和为了简化路由更新。 您能发送指示的NHRP重定向(很象互联网控制消息协议(ICMP)重定向)一更加好的跳是否为指定目的地存在，允许设立的一个spoke-to-spoke通道。 这些摘要也用于为了最小化被发送在集线器和每分支之间，允许设置扩展更加好的相当数量路由更新。

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

router bgp 65001
bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
```

验证

此配置示例的验证划分成几个部分。

预先移植检查

因为DMVPN/EIGRP和FlexVPN/BGP同时运行，您必须验证分支维护在IPsec的一关系与IKEv1和IKEv2，并且适当的前缀在EIGRP和BGP了解。

在本例中，**分支1**显示两会话用中心路由器保养;一使用IKEv1/Tunnel0，并且一个使用IKEv2/Tunnel1。

Note:两个IPSec安全关联(SAS) (一入站和一出站)为其中每一个通道保养。

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

当您检查路由协议时，您必须验证结邻形成，并且了解正确前缀。 这首先检查与EIGRP。验证集线器是可视作为邻居，并且192.168.0.0/16地址(摘要)从集线器了解：

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

其次，请验证BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

输出显示集线器FlexVPN IP地址(10.1.1.1)是一个邻居分支接收一个前缀(192.168.0.0/16)。另外，BGP通知管理员路由信息库(RIB)失败为192.168.0.0/16前缀发生了。此失败发生，因为有在路由表里已经存在的该前缀的一佳路由。此路由由EIGRP产生，并且可以被确认是否检查路由表。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

迁移

前面部分验证IPsec和路由协议配置和工作正如所料。其中一个最简单的方法从DMVPN移植到在同一个设备的FlexVPN是更改管理距离(AD)。 在本例中，内部BGP (iBGP)有AD 200和EIGRP有AD 90。

为了流量能适当地流经FlexVPN， BGP必须有更加好的AD。 在本例中， EIGRP AD更改对230和240为内部和外部路由，分别。 这使BGP AD (200)更可取为192.168.0.0/16前缀。

使用为了达到此的另一个方法将减小BGP AD。然而，运行的协议，在迁移有非默认值后，能影响部署的其他部分。

在本例中， debug ip routing命令是在分支的使用的为了检验操作。

> Note:如果在此部分的信息在生产网络使用，请避免使用调试指令，并且取决于在下一部分列出的显示命令。 并且，分支EIGRP进程必须重建邻接用集线器。

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1
```

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1
```

有三重要操作注意在此输出中：

- 分支注意AD更改，并且禁用邻接。
- 在路由表里， EIGRP前缀被重绑，并且BGP介绍。
- 对集线器的邻接在EIGRP回来联机。

当您更改在设备时的AD，只影响从设备的路径到其他网络;它不影响其他路由器如何执行路由。例如，在EIGRP距离增加对**分支1** (和此使用在网云为了路由流量的FlexVPN)后，集线器维护已配置的(默认)广告。这意味着使用DMVPN为了路由流量回到**分支1**。

在某些情况下，当防火墙期待在同一个接口时的回程数据流这能引起问题，例如。 所以，在您在集线器前，更改它您应该更改在所有spoke的AD。只有一旦这完成，流量由FlexVPN充分地移植。

Eigrp对EIGRP迁移

从DMVPN的迁移到运行仅EIGRP的FlexVPN不是讨论详细的在本文;然而，为完整性被提及在这儿。

它是可能的添加DMVPN和EIGRP到路由实例的同一个EIGRP自治系统(AS)。 使用此到位，路由邻接在网云两个类型设立。 这能造成负载平衡发生，没有典型地推荐。

为了保证FlexVPN或DMVPN选择，管理员能赋予在单个交换面基础上的不同的**延迟值**。 然而，请记住更改不是可能的在虚拟模板接口，当对应的虚拟访问接口存在时。

后移民检查

类似于用于**预先移植的**进程**检查**部分， IPsec，并且必须验证路由协议。

首先，请验证IPsec ：

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
```

```
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

和前面，两会话看到，其中之二有两活动IPSec SAS。

在分支，会聚路由(192.168.0.0/16)从集线器指向和在BGP了解。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

同样地，在集线器被加前缀的分支LAN必须通过EIGRP知道。 在本例中，**分支2** LAN子网被检查：

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

在输出中，转发路径适当地更新并且指出虚拟访问接口。

另外的考虑事项

此部分描述与此配置示例是相关的一些附加区域重要。

现有spoke-to-spoke通道

使用迁移，因为快捷方式交换运转中，从EIGRP到BGP， spoke-to-spoke通道没有被影响。 在分支的快捷方式交换插入有AD的一个更加特定的NHRP路由250。

这是这样路由示例：

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

已迁移和非已迁移Spoke之间的通信

如果分支已经在的FlexVPN/BGP要与迁移进程未开始的设备联络，流量总是漫过集线器。

这是发生的进程：

1. 分支执行目的地的路由查找，通过汇总路由指向由集线器通告。
2. 数据包发送往集线器。
3. 集线器收到数据包并且执行目的地的路由查找，指出另一个接口是一个不同的NHRP域的一部分。

Note:在上一个集线器上配置的NHRP网络ID为FlexVPN和DMVPN是不同的。即使NHRP网络ID统一，问题也许发生被移植的分支路由在FlexVPN网络的地方对象。这包括用于的方针为了配置抄近路交换。非已迁移分支尝试运行在DMVPN网络的对象，以一个特定目标执行快捷方式交换。

故障排除

此部分描述两个类别典型地使用的为了toubleshoot迁移。

与尝试的问题设立通道

如果IKE协商发生故障，请完成这些步骤：

1. 验证当前状态用这些命令：

   show crypto isakmp sa -此命令显示IKEv1会话的数量、来源和目的地。**显示crypto sa-ipsec**此命令显示IPSec SAS的活动。**Note**:不同于在IKEv1，在输出的这中完整转发安全性(PFS) Diffie-Hellman (DH)组的值出现作为**PFS是/否：N， DH组：无**在第一隧道协商时;然而，在重新生成密钥发生后，正确值出现。这不是bug，即使行为在CSCug67056描述。 在IKEv1和IKEv2之间的区别是那在后者， SAS创建作为**验证**交换的部分的孩子。配置在加密映射下在重新生成密钥期间的DH组仅使用。为此，您看到**PFS是/否：N， DH组：什么都**直到第一不重新生成密钥。使用IKEv1，您看到一种不同的行为在快速模式期间，因为SA儿童创建发生，并且指定DH参数为了派生一新建的共享机密的**CREATE_CHILD_SA**消息做好准备为密钥交换有效负载移交。**显示crypto ikev2 sa** -此命令提供输出类似于ISAKMP，但是特定对IKEv2。**显示crypto会话**-此命令在此设备提供加密会话的汇总输出。**显示crypto socket** -此命令显示crypto插槽状态。**show crypto map** -此命令显示IKE和IPSec简档映射对接口。**show ip nhrp** -此命令提供从设备的NHRP信息。这为spoke-to-spoke是有用的在FlexVPN设置，并且对于在DMVPN的spoke-to-spoke和spoke-to-hub捆绑设置。
2. 请使用这些命令为了调试隧道建立：

debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

与路由传播的问题

这是您能使用为了排除故障EIGRP和拓扑的一些有用的命令：

- **show bgp摘要**-请使用此命令为了验证直连的邻居和他们的状态。
- **show ip eigrp neighbor** -请使用此命令为了显示通过EIGRP连接的邻居。
- **show bgp** -请使用此命令为了验证在BGP了解的前缀。
- **show ip eigrp topology** -请使用此命令为了显示通过EIGRP了解的前缀。

知道是重要的一个获知的前缀跟在路由表里安装的前缀不同。 关于此的更多信息，请参考路由选择Cisco路由器Cisco条款或者路由的TCP/IP Cisco信息发布登记薄。

已知问题说明

并行GRE隧道处理的限制在ASR1K存在。这被跟踪在Cisco Bug ID CSCue00443下。此时，限制有一个被安排的修正在Cisco IOS XE软件版本3.12。

请监控此bug，如果希望通知修正一次变得可用。