

# ASA 9.x EIGRP配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[准则和限制](#)

[EIGRP和故障转移](#)

[配置](#)

[网络图](#)

[ASDM 配置](#)

[配置 EIGRP 身份验证](#)

[EIGRP路由过滤](#)

[验证](#)

[配置](#)

[Cisco ASA CLI 配置](#)

[Cisco IOS 路由器 \(R1\) CLI 配置](#)

[验证](#)

[数据包流](#)

[故障排除](#)

[故障排除命令](#)

[EIGRP邻居关系与系统日志ASA-5-336010断开](#)

## 简介

本文档介绍如何配置思科自适应安全设备(ASA)，以便通过ASA软件版本9.x及更高版本支持的增强型内部网关路由协议(EIGRP)学习路由并执行身份验证。

## 先决条件

### 要求

在尝试此配置之前，思科要求您满足以下条件：

- Cisco ASA必须运行9.x或更高版本。
- EIGRP必须处于单情景模式，因为多情景模式不支持它。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 软件版本 9.2.1
- Cisco 自适应安全设备管理器 (ASDM) 版本 7.2.1
- 运行版本 12.4 的 Cisco IOS® 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

### 准则和限制

- 单模式和多模式中每个情景支持一个EIGRP实例。
- 每个EIGRP实例在多模式下每个情景创建两个线程，并可通过show进程查看。
- 默认情况下禁用自动总结。
- 在单个接口模式下，集群设备之间未建立邻居关系。
- 使用[<acl>]中的默认信息过滤传入候选默认路由中的外部位。
- 使用Default-information out [<acl>]过滤传出候选默认路由中的外部位。

### EIGRP和故障转移

Cisco ASA代码版本8.4.4.1及更高版本将从主用设备到备用设备的动态路由同步。此外，删除路由也会同步到STANDBY设备。但是，对等邻接的状态不同步；只有活动设备会维护邻居状态并主动参与动态路由。请参阅[ASA常见问题：如果同步动态路由，故障切换后会发生什么情况？](#)。

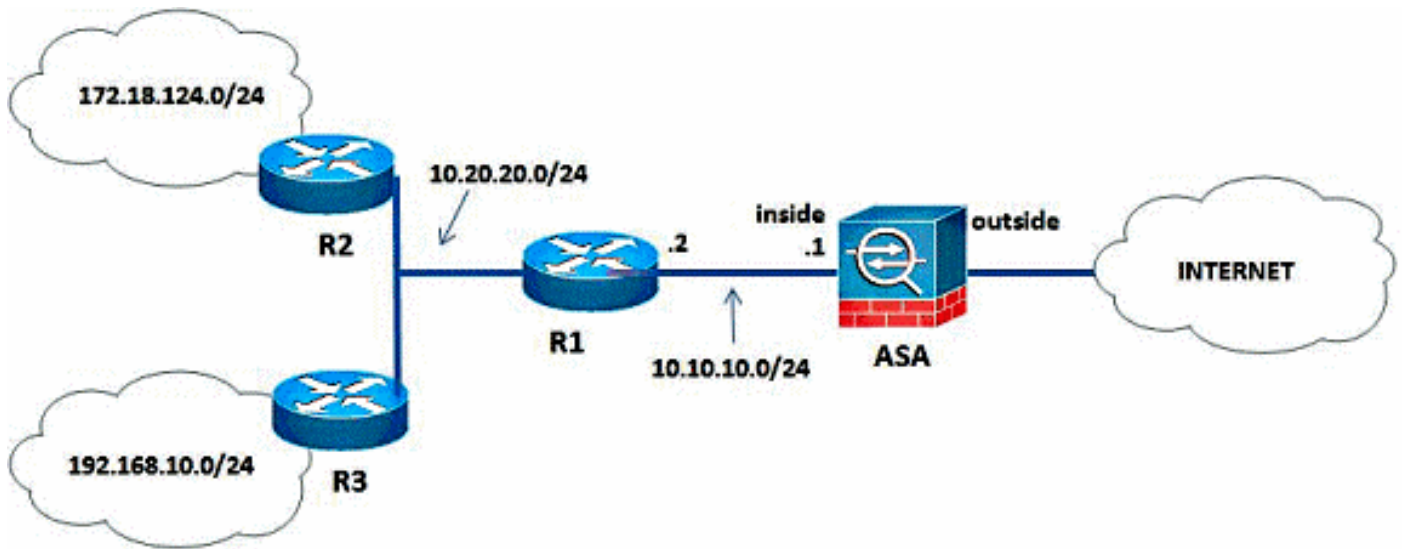
## 配置

本节介绍如何配置本文档中涵盖的功能。

**注意：**使用[命令查找工具（仅限注册用户）](#)可获取有关本部分所使用命令的详细信息。

## 网络图

本文档使用以下网络设置：



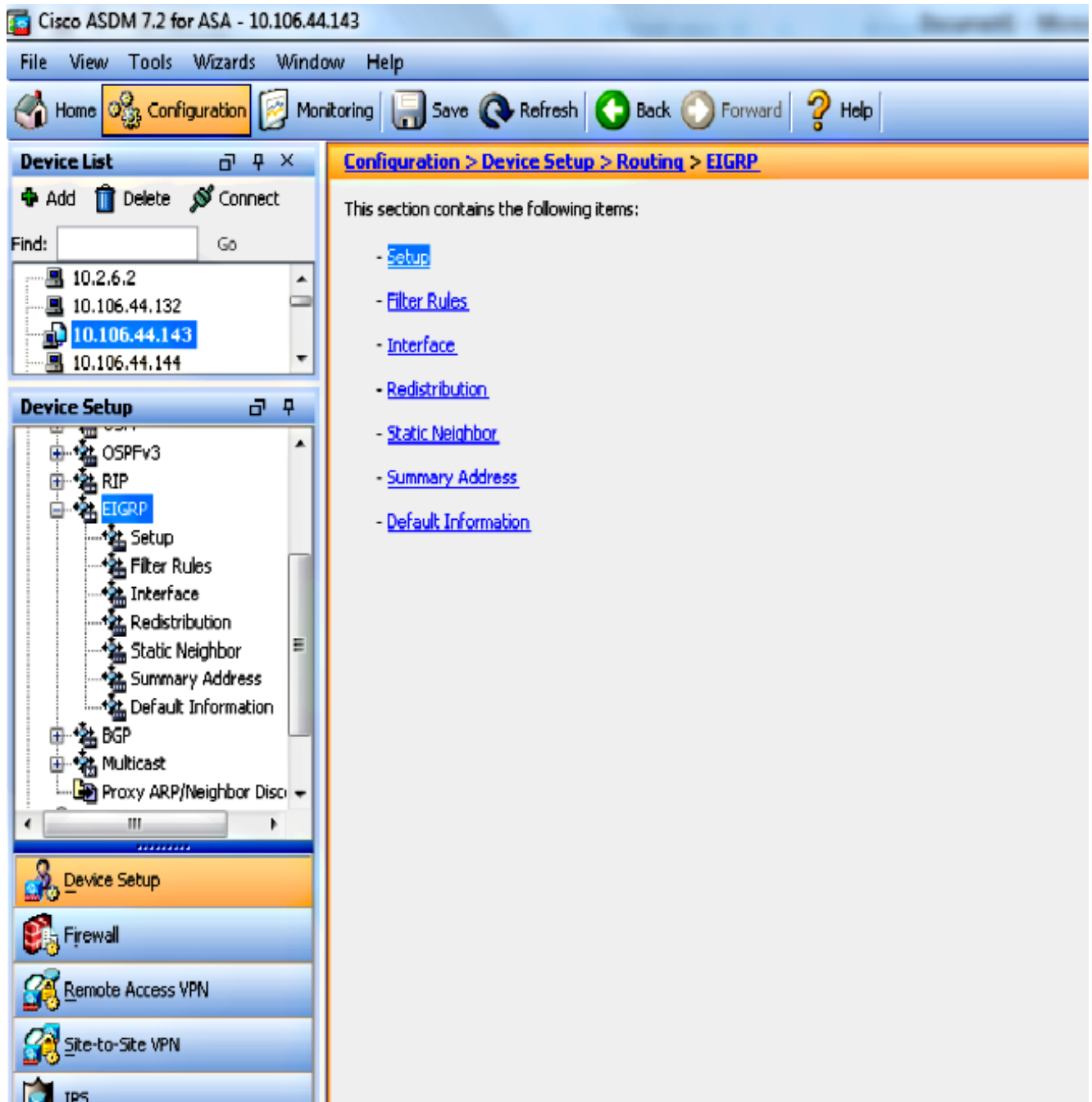
在图示的网络拓扑中，Cisco ASA内部接口IP地址为10.10.10.1/24。目标是在Cisco ASA上配置EIGRP，以便通过相邻路由器(R1)动态获取到内部网络(10.20.20.0/24、172.18.124.0/24和192.168.10.0/24)的路由。R1通过其他两个路由器(R2和R3)识别通往远程内部网络的路由。

## ASDM 配置

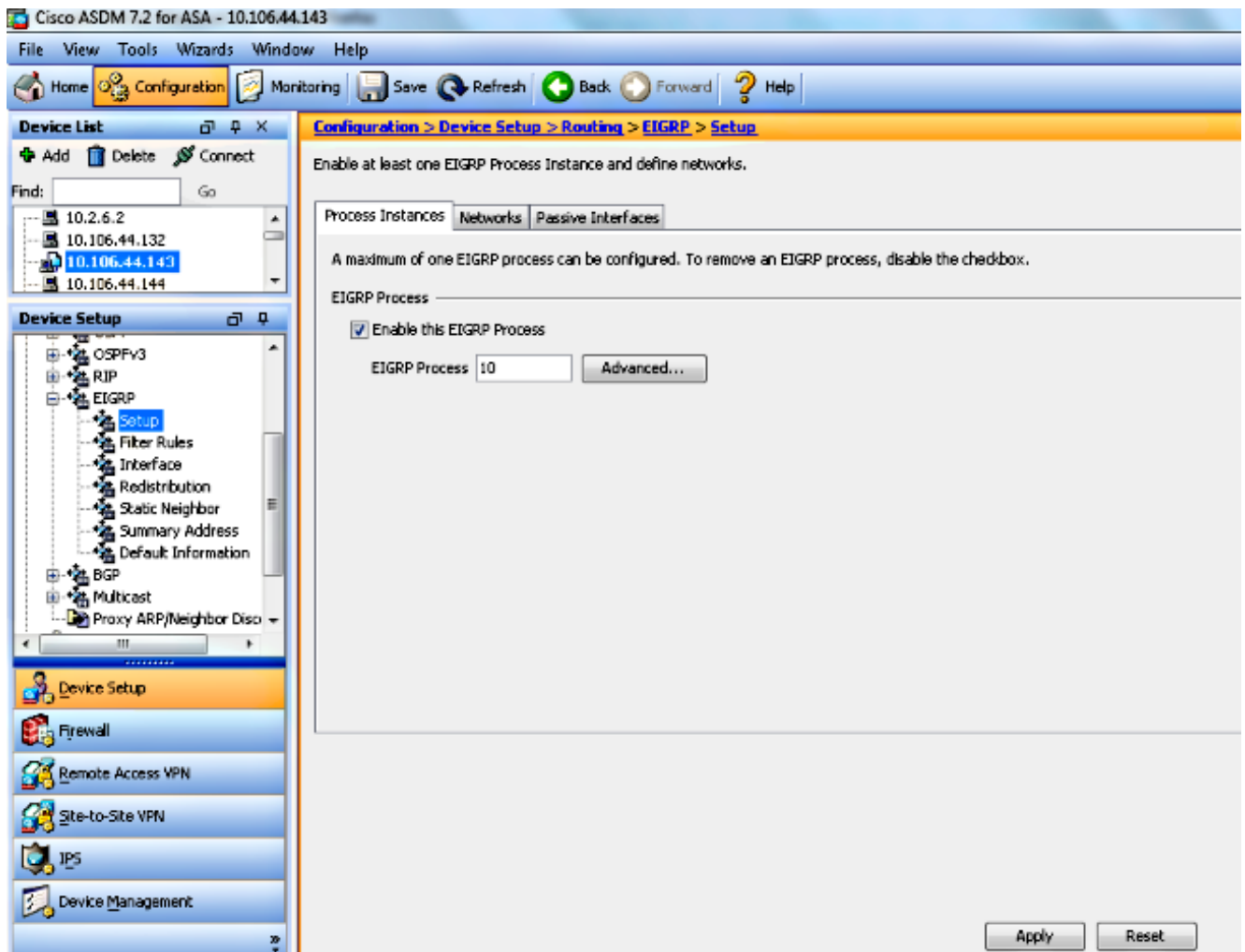
ASDM是基于浏览器的应用，用于配置和监控安全设备上的软件。ASDM从安全设备加载，然后用于配置、监控和管理设备。您还可以使用ASDM启动程序以比Java小程序更快地启动ASDM应用。本节介绍使用ASDM配置本文档中描述的功能所需的信息。

要在Cisco ASA中配置EIGRP，请完成以下步骤。

1. 使用ASDM登录Cisco ASA。
2. 导航到ASDM接口的Configuration > Device Setup > Routing > EIGRP区域，如此屏幕截图所示。



3. 如此屏幕截图所示，在“设置”>“进程实例”选项卡上启用EIGRP路由进程。在本示例中，EIGRP进程是 10。



4. 您可以配置可选的高级 EIGRP 路由进程参数。单击 **Setup > Process Instances** 选项卡上的 **Advanced**。您可以将 EIGRP 路由进程配置为残域路由进程，禁用自动路由汇总，定义重分配路由的默认度量值，更改内部和外部 EIGRP 路由的管理距离，配置静态路由器 ID，并且启用或禁用邻接更改的日志记录。在本示例中，使用内部接口的 IP 地址 (10.10.10.1) 静态配置 EIGRP 路由器 ID。另外，也禁用了 **Auto-summary**。所有其他选项都使用默认值配置。

**Edit EIGRP Process Advanced Properties**

EIGRP Process:

Router ID:

---

Summary

Auto-Summary

---

Default Metrics

Bandwidth:  (1 - 4294967295)    Delay:  (1 - 4294967295)

Loading:  (1 - 255)    MTU:  (1 - 65535)

Reliability:  (0 - 255)

---

Stub

Stub Receive only (If selected, no other stub options may be selected.)

Stub Connected     Stub Redistributed

Stub Static     Stub Summary

---

Adjacency Changes

Enable this for the firewall to send a syslog message when a neighbor goes up/down.

Log neighbor changes

Enable this for the firewall to send a syslog message for warnings at interval in seconds.

Log neighbor warnings

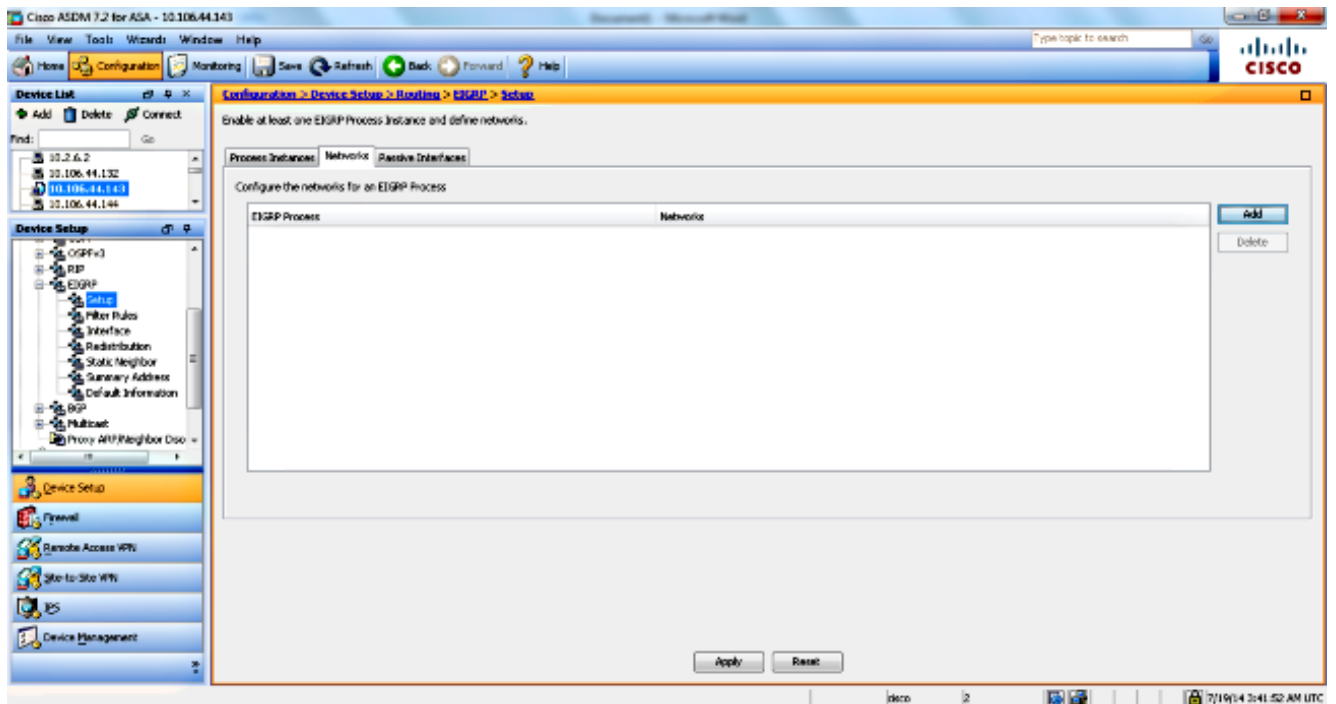
---

Administrative Distance

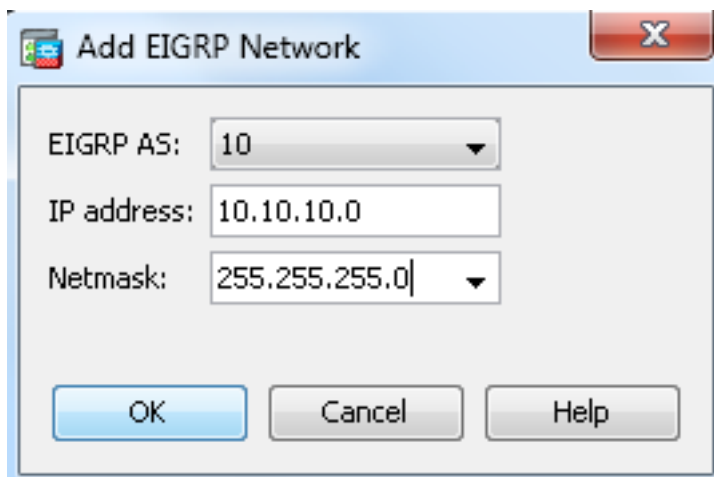
Internal distance:  (1 - 255 default 90)

External distance:  (1 - 255 default 170)

5. 完成前述步骤后，在 **Setup > Networks** 选项卡上定义 EIGRP 路由中涉及的网络和接口。单击 **Add**，如屏幕截图所示。



6. 将出现此屏幕。在本例中，您添加的唯一网络是内部网络(10.10.10.0/24)，因为EIGRP仅在内部接口上启用。



只有具有IP地址的接口属于已定义网络，才参与EIGRP路由过程。如果您有一个接口不想参与EIGRP路由，但该接口已连接到要通告的网络，请在**Setup > Networks**选项卡上配置一个网络条目，该条目覆盖该接口所连接的网络，然后将该接口配置为被动接口，以便该接口无法发送或接收EIGRP更新。

**注意：**配置为无源的接口不发送或接收 EIGRP 更新。

7. 还可以选择在 Filter Rules 窗格中定义路由过滤器。路由过滤可对允许在 EIGRP 更新中发送或接收的路由提供更多控制。
8. 您也可以选择配置路由重分配。Cisco ASA可以将路由信息协议(RIP)和开放最短路径优先(OSPF)发现的路由重新分发到EIGRP路由进程。您还可以将静态和连接的路由重分配到EIGRP 路由进程。如果静态或已连接路由在 **Setup > Networks** 选项卡上配置的网络范围内，则不需要对其重分配。请在 Redistribution 窗格中定义路由重分配。

9. EIGRP hello 数据包作为多播数据包发送。如果EIGRP邻居位于非广播网络中，则必须手动定义该邻居。手动定义 EIGRP 邻居时，hello 数据包作为单播消息发送到该邻居。为了定义静态 EIGRP 邻居，请转到 **Static Neighbor** 窗格。

10. 默认情况下，会发送并且接受默认路由。为了限制或禁用发送和接收默认路由信息，请打开 **Configuration > Device Setup > Routing > EIGRP > Default Information** 窗格。Default Information 窗格显示控制发送和接收 EIGRP 更新中的默认路由信息的规则表。

**注意：**每个EIGRP路由进程可以有一个“输入”和一个“输出”规则。（当前仅支持一个进程。）

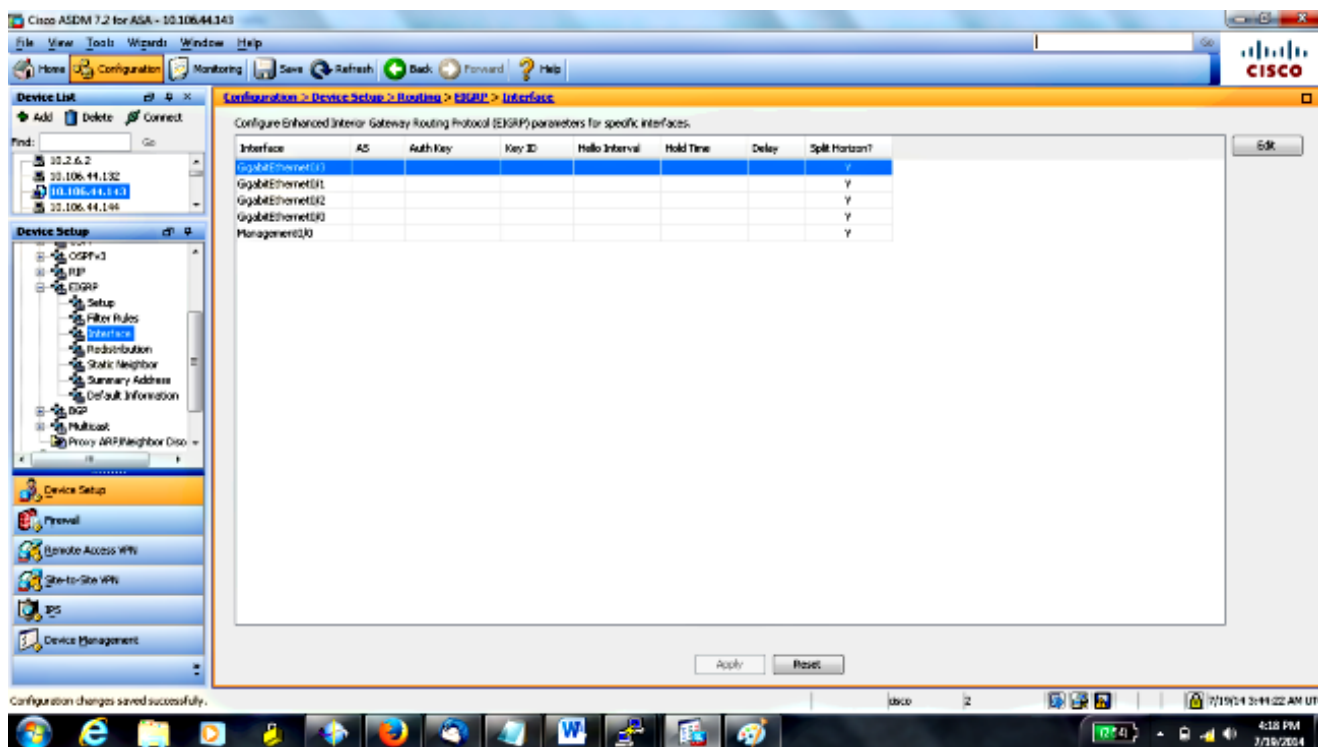
## 配置 EIGRP 身份验证

Cisco ASA 支持来自 EIGRP 路由协议的更新路由的 MD5 身份验证。每个EIGRP数据包中带有 MD5密钥的摘要可防止从未批准的源引入未授权或虚假路由消息。对 EIGRP 消息添加身份验证可确保您的路由器和 Cisco ASA 只接受来自配置了相同预共享密钥的其他路由设备的路由消息。如果未配置此身份验证，如果有人将具有不同或相反路由信息的其他路由设备引入网络，则路由器或 Cisco ASA 上的路由表可能会损坏，并且可能会发起拒绝服务攻击。当您向路由设备（包括 ASA）之间发送的EIGRP消息添加身份验证时，它会防止未经授权将EIGRP路由器添加到您的路由拓扑中。

EIGRP 路由身份验证基于每个接口进行配置。对于针对 EIGRP 消息身份验证配置的接口上的所有 EIGRP 邻居，必须为要建立的相邻关系配置相同的身份验证模式和密钥。

要在Cisco ASA上启用EIGRP MD5身份验证，请完成以下步骤。

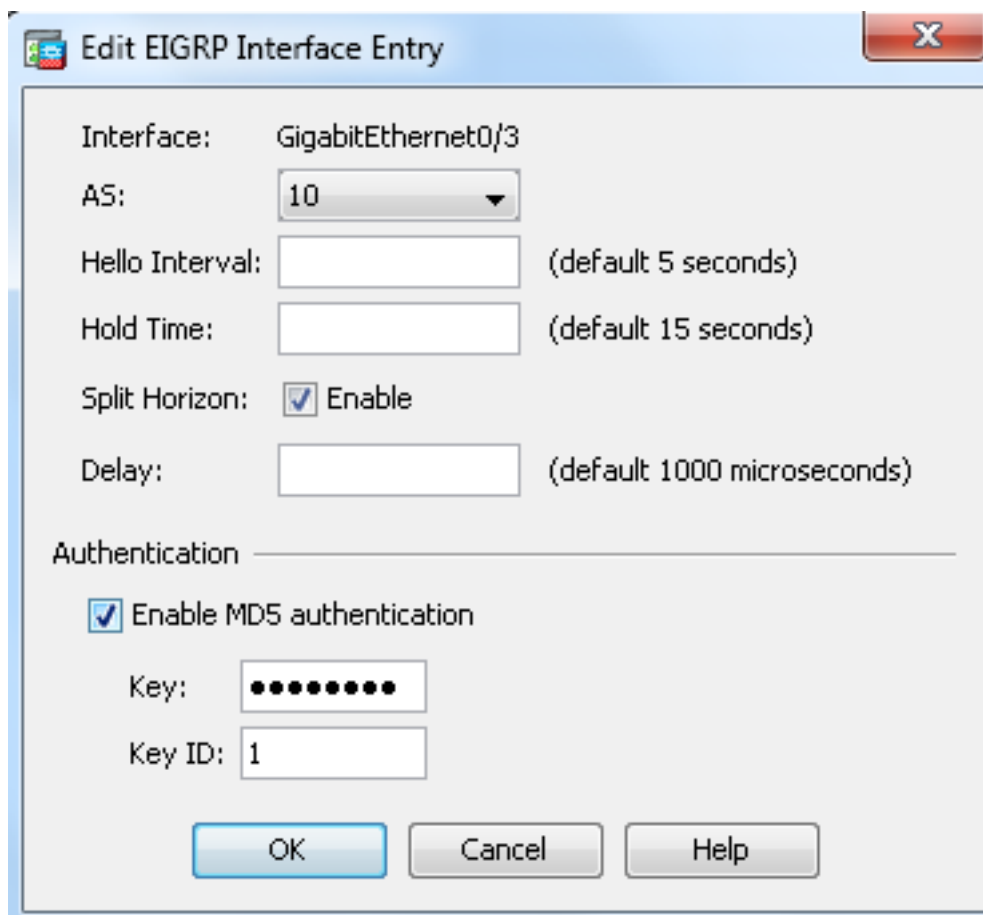
1. 在ASDM上，导航至**Configuration > Device Setup > Routing > EIGRP > Interface**，如图所示。



2. 在这种情况下，EIGRP 在内部接口 (GigabitEthernet 0/1) 上启用。选择 **GigabitEthernet 0/1** 接口，然后单击 **Edit**。



3. 在 Authentication 下，选择 **Enable MD5 authentication**。在此处添加有关身份验证参数的详细信息。在本示例中，预共享密钥是 **cisco123**，密钥 ID 是 1。



Interface: GigabitEthernet0/3

AS: 10

Hello Interval: (default 5 seconds)

Hold Time: (default 15 seconds)

Split Horizon:  Enable

Delay: (default 1000 microseconds)

Authentication

Enable MD5 authentication

Key: ●●●●●●●●

Key ID: 1

OK Cancel Help

## EIGRP路由过滤

使用EIGRP，您可以控制发送和接收的路由更新。在本示例中，您将阻止ASA上网络前缀 192.168.10.0/24的路由更新，该前缀位于R1后面。对于路由过滤，您只能使用**标准ACL**。

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any
```

```
router eigrp 10
distribute-list eigrp in
```

## 验证

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

## 配置

### Cisco ASA CLI 配置

这是Cisco ASA CLI配置。

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
nameif management
security-level 99
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

## Cisco IOS 路由器 (R1) CLI 配置

这是 R1 ( 内部路由器 ) 的 CLI 配置。

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
parameters.

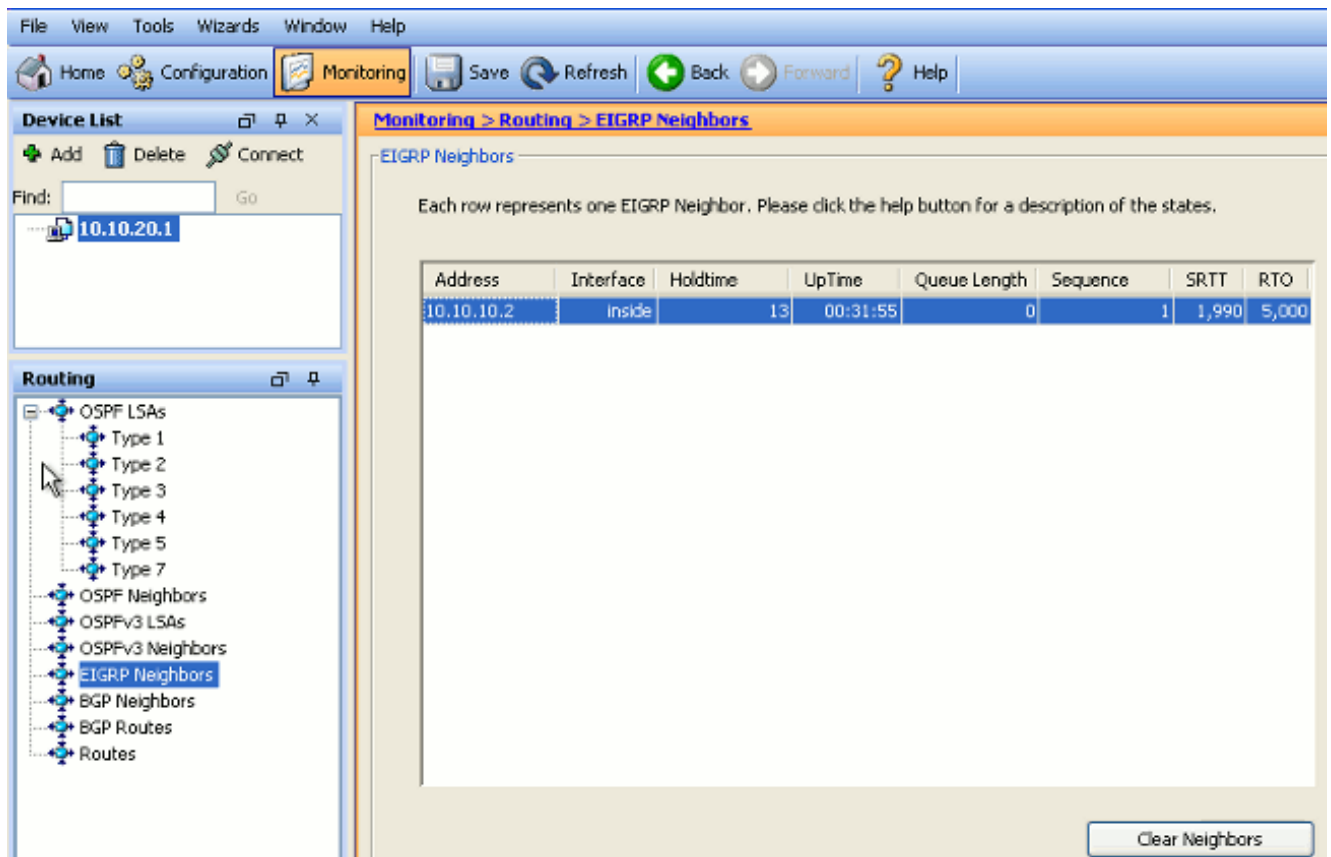
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
```

```
ip authentication key-chain eigrp 10 MYCHAIN
!  
!  
  
! EIGRP Configuration  
  
router eigrp 10  
network 10.10.10.0 0.0.0.255  
network 10.20.20.0 0.0.0.255  
network 172.18.124.0 0.0.0.255  
network 192.168.10.0  
no auto-summary
```

## 验证

完成以下步骤以验证您的配置。

1. 在ASDM上，您可以导航到**Monitoring > Routing > EIGRP Neighbor**，以查看每个EIGRP邻居。此屏幕截图显示了作为活动邻居的内部路由器 (R1)。您还可以看到此邻居驻留的接口、保持时间和邻接关系的正常运行时间 (UpTime)。



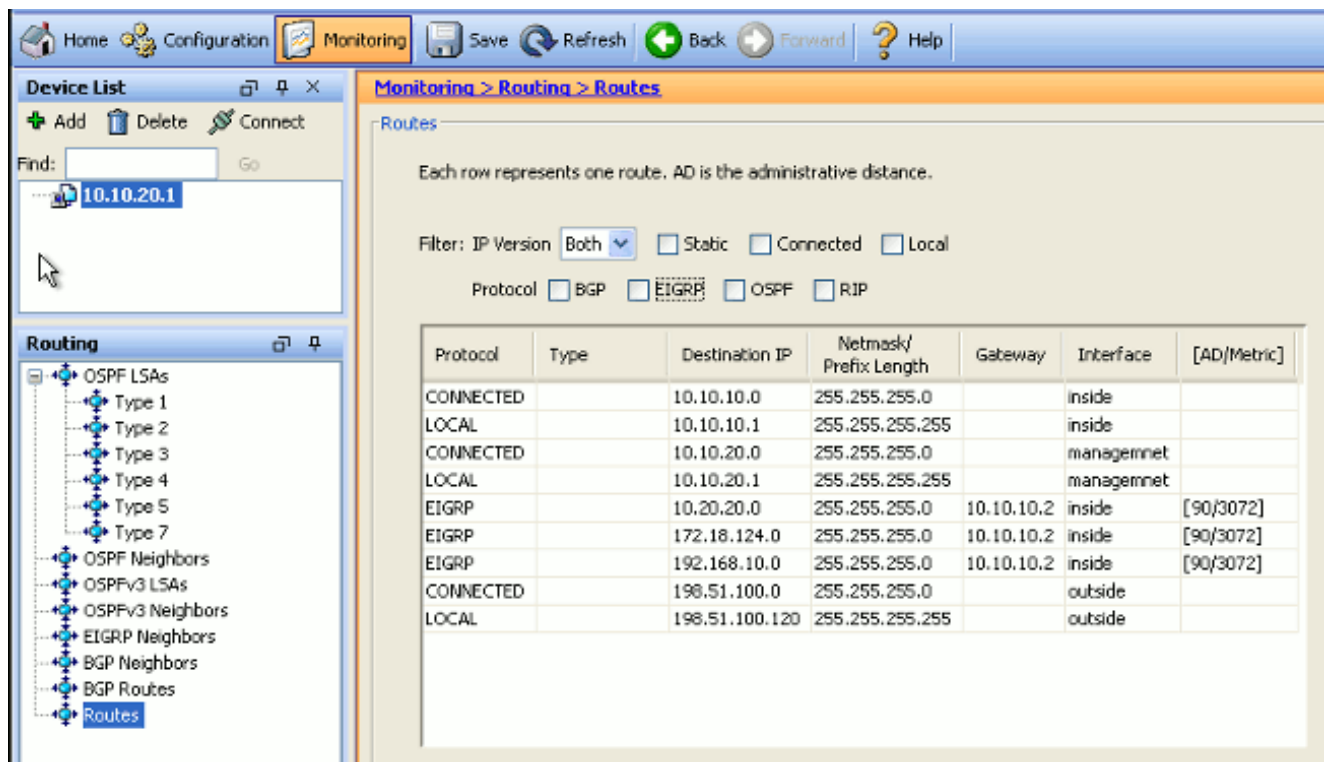
The screenshot shows the ASDM interface with the 'Monitoring > Routing > EIGRP Neighbors' page selected. The 'Device List' on the left shows '10.10.20.1' selected. The 'Routing' tree on the left has 'EIGRP Neighbors' highlighted. The main content area displays a table of EIGRP neighbors.

Address	Interface	Holdtime	UpTime	Queue Length	Sequence	SRTT	RTO
10.10.10.2	inside	13	00:31:55	0	1	1,990	5,000

Each row represents one EIGRP Neighbor. Please click the help button for a description of the states.

Clear Neighbors

2. 此外，如果导航到 **Monitoring > Routing > Routes**，还可以验证路由表。在此屏幕截图中，可以看到 **192.168.10.0/24**、**172.18.124.0/24** 和 **10.20.20.0/24** 网络是通过 R1 (10.10.10.2) 识别的。



从 CLI 中，可以使用 **show route** 命令获得相同的输出。

```
ciscoasa# show route
```

Codes: C - connected, S - static, I - IGRP, 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, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 100.10.10.2 to network 0.0.0.0

C 198.51.100.0 255.255.255.0 is directly connected, outside

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside

D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside

C 127.0.0.0 255.255.0.0 is directly connected, cplane

D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside

C 10.10.10.0 255.255.255.0 is directly connected, inside

C 10.10.20.0 255.255.255.0 is directly connected, management

S\* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside

对于ASA 9.2.1版及更高版本，您可以使用**show route eigrp**命令来仅显示EIGRP路由。

```
ciscoasa(config)# show route eigrp
```

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

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  
o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

```
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

### 3. 您还可以使用show eigrp topology命令来获取有关已获知网络和EIGRP拓扑的信息。

```
ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

### 4. show eigrp neighbors命令也可用于验证活动邻居和相应信息。此示例显示您在步骤1中从ASDM获取的相同信息。

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

## 数据包流

这是数据包流。

1. ASA在链路上启动，并通过其所有配置了EIGRP的接口发送mCast Hello数据包。
2. R1收到Hello数据包并发送mCast Hello数据包。

13	5.572557	10.10.10.1	10.10.10.1	224.0.0.10	EIGRP	86	0x3b1a (15130)	Hello
14	5.573335	10.10.10.2	10.10.10.2	224.0.0.10	EIGRP	86	0x2321 (8993)	Hello
15	5.575212	10.10.10.1	10.10.10.1	10.10.10.2	EIGRP	54	0x0589 (1417)	Update
16	5.581712	10.10.10.2	10.10.10.2	10.10.10.1	EIGRP	54	0x19d9 (6617)	Update
17	5.585145	10.10.10.1	10.10.10.1	10.10.10.2	EIGRP	54	0x755e (30046)	Hello (Ack)
18	5.585373	10.10.10.1	10.10.10.1	10.10.10.2	EIGRP	98	0x1c93 (7315)	Update
19	5.591919	10.10.10.2	10.10.10.2	10.10.10.1	EIGRP	54	0x6695 (26261)	Hello (Ack)
20	5.591950	10.10.10.2	10.10.10.2	10.10.10.1	EIGRP	180	0x7925 (31013)	Update
21	5.595200	10.10.10.1	10.10.10.1	10.10.10.2	EIGRP	98	0x62e8 (25320)	Update
22	5.601913	10.10.10.2	10.10.10.2	10.10.10.1	EIGRP	54	0x08a7 (2215)	Hello (Ack)
23	5.601944	10.10.10.2	10.10.10.2	10.10.10.1	EIGRP	98	0x31c5 (12741)	Update

3. ASA接收Hello数据包并发送包含初始位集的更新数据包，这表示这是初始化过程。

4. R1收到更新数据包并发送包含初始位集的更新数据包，这表示这是初始化过程。

```
Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
Cisco EIGRP
  version: 2
  opcode: Update (1)
  checksum: 0xfdc4 [correct]
  flags: 0x00000001, Init
    ..... 1 = Init: Set
    ..... 0. = Conditional Receive: Not set
    ..... 0. = Restart: Not set
    ..... 0... = End Of Table: Not set
  sequence: 47
  acknowledge: 0
  virtual router id: 0 (Address-Family)
  autonomous system: 10
```

5. 在ASA和R1都交换了hello消息并建立邻居邻接关系后，ASA和R1都使用ACK数据包进行应答，这表示已收到更新信息。

6. ASA在更新数据包中将其路由信息发送到R1。

7. R1在其拓扑表中插入更新数据包信息。拓扑表包含邻居通告的所有目标。按照组织方式列出每个目标，以及可以到达目的地的所有邻居及其关联的度量。

8. 然后R1向ASA发送更新数据包。

```
Frame 20: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits)
Ethernet II, Src: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3), Dst: Cisco_25:32:e2 (00:21:a0:25:32:e2)
Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
Cisco EIGRP
  version: 2
  opcode: Update (1)
  checksum: 0xd032 [correct]
  flags: 0x00000000
  sequence: 21
  acknowledge: 48
  virtual router id: 0 (Address-Family)
  autonomous system: 10
  Internal Route(MTR) = 10.20.20.0/24
  Internal Route(MTR) = 172.18.124.0/24
  Internal Route(MTR) = 192.168.10.0/24
```

Unicast

Routing update received

9. 收到更新数据包后，ASA向R1发送ACK数据包。在ASA和R1成功收到彼此发送的更新数据包后，它们准备好在拓扑表中选择后继路由（最佳）和可行后继路由（备份）路由，并将后继路由提供到路由表。

## 故障排除

本节包含有关debug和show命令的信息，这些命令对于排除EIGRP故障非常有用。

### 故障排除命令

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输

出的分析。

**注意：**使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。要显示扩散更新算法 (DUAL)有限状态机的调试信息，请在特权EXEC模式下使用**debug eigrp fsm**命令。此命令使您可以观察 EIGRP 可行后继路由活动并确定路由进程是否安装并删除了路由更新。

这是与R1成功对等中**debug**命令的输出。您可以看到系统上成功安装的每个不同路由。

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

您还可以使用 **debug eigrp neighbor** 命令。这是此 debug 命令在 Cisco ASA 成功创建具有 R1 的新邻居关系时的输出。

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

您还可以将 debug eigrp 数据包用于 Cisco ASA 和其对等体之间详细的 EIGRP 消息交换信息。在

本示例中，身份验证密钥在路由器 (R1) 上进行了更改，并且 debug 输出显示问题是身份验证不匹配。

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

## EIGRP邻居关系与系统日志ASA-5-336010断开

当对EIGRP分发列表进行任何更改时，ASA会丢弃EIGRP邻居关系。此系统日志消息已显示。

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

使用此配置时，每当在ACL中添加新的acl条目时，Eigrp-network-list EIGRP邻居关系就会重置。

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static
```

```
access-list Eigrp-network-list standard permit any
```

您可以观察到相邻设备的邻居关系已启用。

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5
```

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

现在可以添加access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0。

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

在debug eigrp fsm中可以看到这些日志。



```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

这是8.4和8.6到9.1版所有新ASA版本中的预期行为。运行12.4到15.1代码系列的路由器也观察到了同样的行为。但是，在ASA 8.2版和更早的ASA软件版本中，未观察到此行为，因为对ACL所做的更改不会重置EIGRP邻接关系。

由于EIGRP在邻居首次启动时向邻居发送完整拓扑表，然后只发送更改，因此配置具有EIGRP事件驱动性质的分发列表会使更改难以在不完全重置邻居关系的情况下应用。路由器需要跟踪每个发送到邻居和从邻居接收的路由，以便知道哪条路由已更改（即，将发送/接受或不会发送/接受），以便应用当前分发列表规定的更改。简单地拆除和重建邻居之间的邻接关系要容易得多。

当邻接关系被拆除并重新建立时，特定邻居之间的所有学习路由都会被忘记，并且邻居之间的整个同步将重新执行 — 新分发列表就位。

您用于排除Cisco IOS路由器故障的大多数EIGRP技术都可应用于Cisco ASA。要排除EIGRP故障，请使用主[故障排除流程图](#)；从标记 **Main** 的框处开始。