

RIP 的 ASA/PIX 配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[ASDM 配置](#)

[配置 RIP 身份验证](#)

[Cisco ASA CLI 配置](#)

[Cisco IOS 路由器 \(R2\) CLI 配置](#)

[Cisco IOS 路由器 \(R1\) CLI 配置](#)

[Cisco IOS 路由器 \(R3\) CLI 配置](#)

[使用 ASA 重分配到 RIP](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

[简介](#)

本文解释如何配置思科ASA为了学习路由通过路由信息协议(RIP)，进行验证和再分配。

有关 EIGRP 配置的详细信息，请参阅 [PIX/ASA 8.X：在 Cisco 自适应安全设备 \(ASA\) 上配置 EIGRP](#)。

注意： 本文档中的配置基于 RIP 版本 2。

注意： ASA/PIX 不支持非对称路由。

[先决条件](#)

[要求](#)

尝试进行此配置之前，请确保满足以下要求：

- Cisco ASA/PIX 必须运行版本 7.x 或更高版本。
- 在多上下文模式下不支持 RIP；仅在单一模式下支持 OSPF。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 8.0 及更高版本的 Cisco 5500 系列自适应安全设备 (ASA)。
- Cisco 自适应安全设备管理器 (ASDM) 软件版本 6.0 及更高版本。

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。

相关产品

本文档中的信息也适用于运行软件版本 8.0 及更高版本的 Cisco 500 系列 PIX 防火墙。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

背景信息

RIP 是一种距离矢量路由协议，使用跃点计数作为路径选择的度量。当 RIP 在某个接口上已启用时，该接口会与相邻的设备交换 RIP 广播，以便动态了解和通告路由。

安全设备同时支持 RIP 版本 1 和 RIP 版本 2。RIP 版本 1 不会发送包含路由更新的子网掩码。RIP 版本 2 会发送包含路由更新的子网掩码，并支持可变长度的子网掩码。此外，RIP 版本 2 支持在交换路由更新时进行邻居身份验证。该身份验证确保安全设备从受信任源接收可靠的路由信息。

限制：

1. 安全设备无法在接口之间传递 RIP 更新。
2. RIP 版本 1 不支持可变长度子网掩码 (VLSM)。
3. RIP 的最大跃点计数为 15。跃点计数超过 15 的路由被认为不可达。
4. 与其他路由协议相比，RIP 收敛相对较慢。
5. 在安全设备上只能启用单个 RIP 进程。

注意： 此信息仅适用于 RIP 版本 2：

1. 如果使用邻居身份验证，则向接口提供 RIP 版本 2 更新的所有邻居设备上的身份验证密钥和密钥 ID 必须相同。
2. 通过 RIP 版本 2，安全设备使用多播地址 224.0.0.9 传输和接收默认路由更新。在被动模式中，它在该地址接收路由更新。
3. 当某个接口上已配置 RIP 版本 2 时，多播地址 224.0.0.9 会在该接口进行注册。当 RIP 版本 2 配置从某个接口删除时，该多播地址未注册。

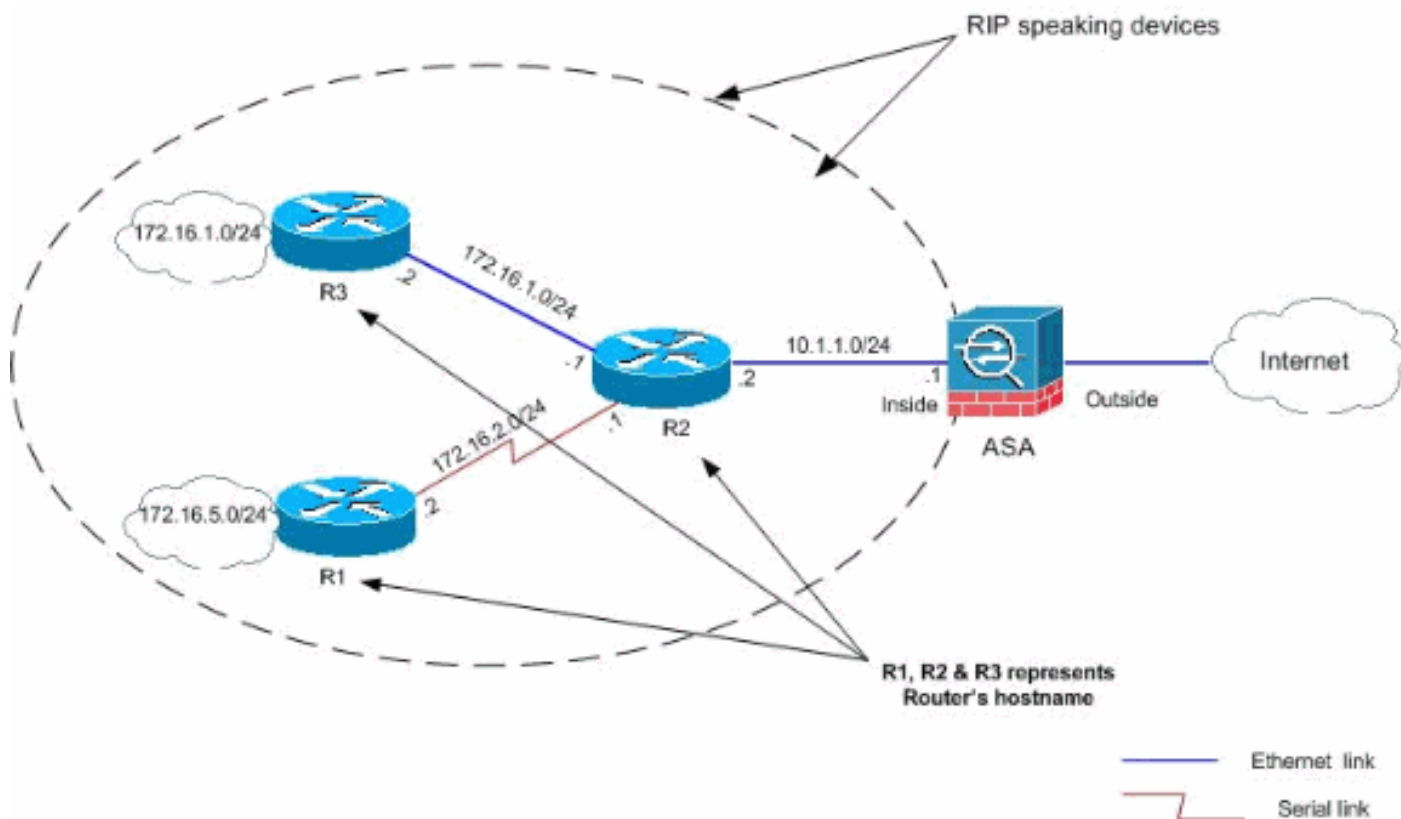
配置

本部分提供有关如何配置本文档所述功能的信息。

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：



配置

本文档使用以下配置：

- [ASDM 配置](#)
- [配置 RIP 身份验证](#)
- [Cisco ASA CLI 配置](#)
- [Cisco IOS 路由器 \(R2\) CLI 配置](#)
- [Cisco IOS 路由器 \(R1\) CLI 配置](#)
- [Cisco IOS 路由器 \(R3\) CLI 配置](#)

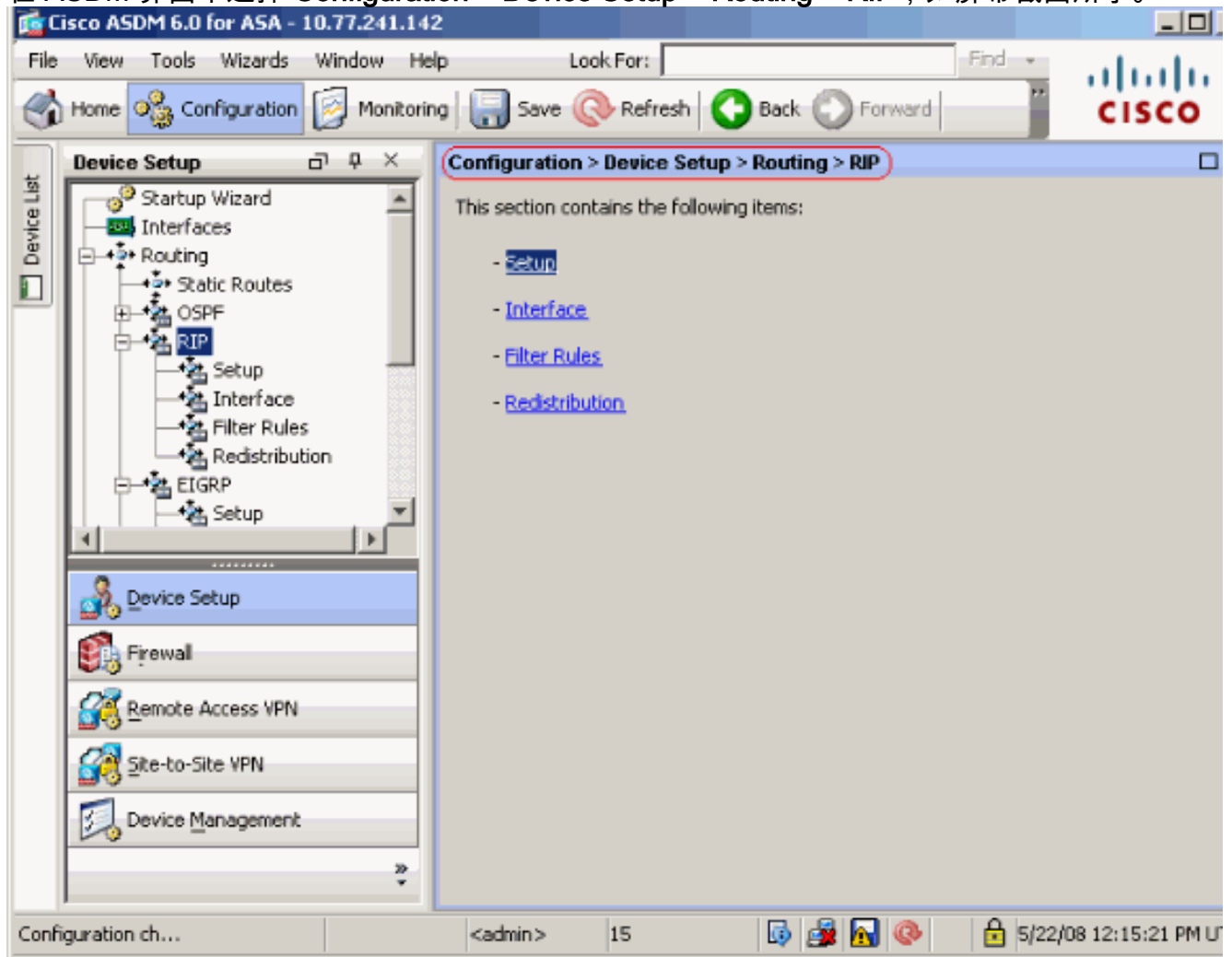
ASDM 配置

可适应安全设备管理器(ASDM)是用于的一基于浏览器的应用程序为了配置和监控在安全工具的软件。ASDM 从安全设备加载，然后用于配置、监控和管理设备。也可以使用 ASDM 启动程序 (仅适用于 Windows®) 启动 ASDM 应用程序，其速度比 Java 小程序更快。本部分介绍了使用 ASDM 配置本文档中所述功能所需的信息。

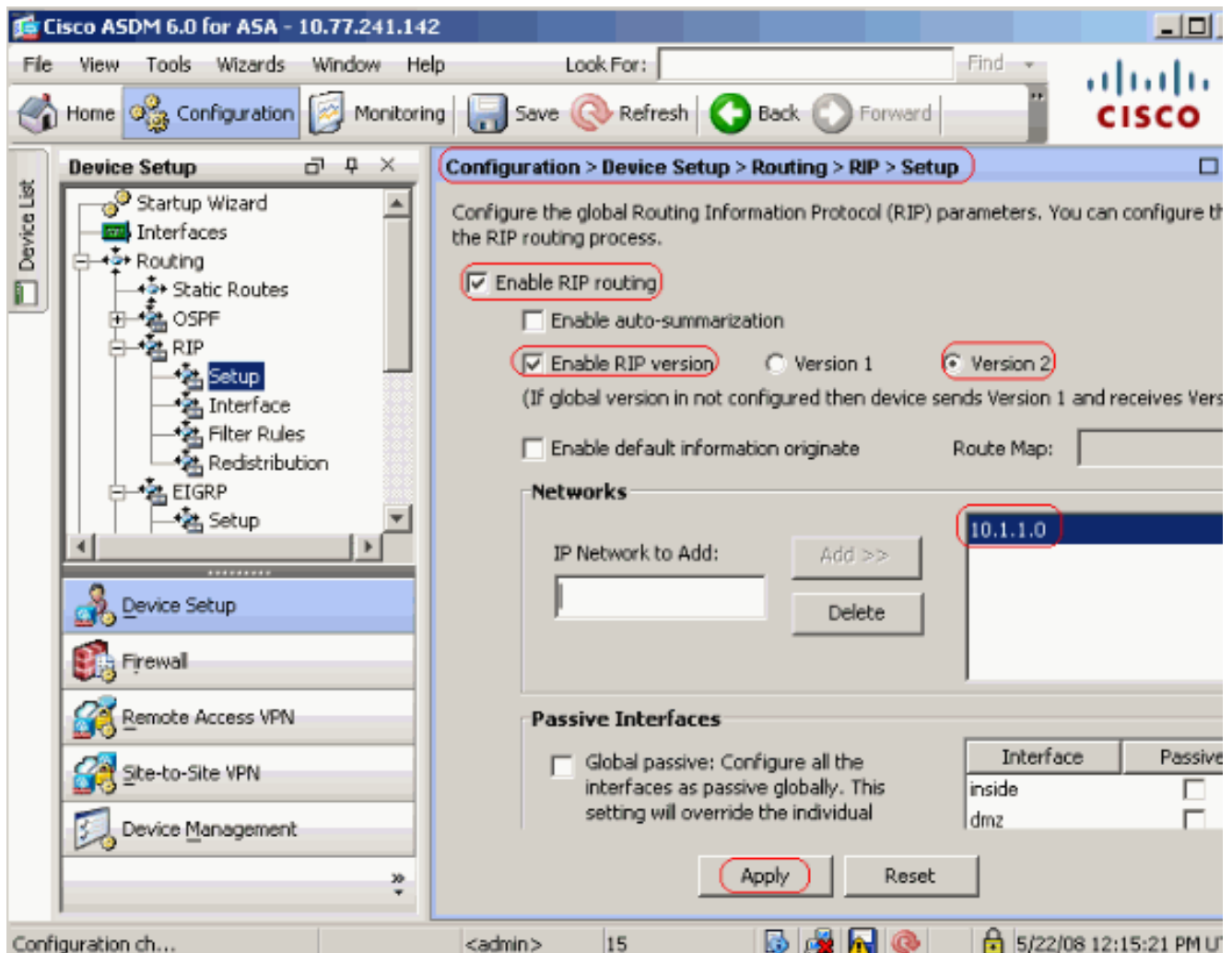
请通过完成以下步骤在 Cisco ASA 中配置 RIP：

1. 登录到使用 ASDM 的 Cisco ASA。

2. 在 ASDM 界面中选择 **Configuration > Device Setup > Routing > RIP**，如屏幕截图所示。



3. 选择 **Configuration > Device Setup > Routing > RIP > Setup**，以启用 RIP 路由（如图所示）。选中 **Enable RIP routing** 复选框。选中 **Enable RIP version** 复选框并选中 **Version 2** 单选按钮。在 **Networks** 选项卡下，添加网络 10.1.1.0。单击 **Apply**。



菲尔茨Enable RIP Routing - 选中该复选框以在安全设备上启用 RIP 路由。启用 RIP 时，即在所有接口上启用 RIP。如果选中该复选框，则也会启用该窗格内的其他字段。取消选中该复选框以在安全设备上禁用 RIP 路由。Enable Auto-summarization - 清除该复选框以禁用自动路由汇总。选中该复选框以重新启用自动路由汇总。RIP 版本 1 始终使用自动汇总。无法对 RIP 版本 1 禁用自动汇总。如果使用的是 RIP 版本 2，则取消选中该复选框可以关闭自动汇总。如果必须在已断开连接的子网之间执行路由，请禁用自动汇总。禁用自动汇总时，子网将得到通告。Enable RIP version - 选中该复选框以指定安全设备所使用的 RIP 版本。如果清除该复选框，则安全设备将发送 RIP 版本 1 更新并接受 RIP 版本 1 和版本 2 更新。该设置可在 Interface 窗格中按每个接口进行覆盖。Version 1 - 指定安全设备仅发送和接收 RIP 版本 1 更新。接收的所有版本 2 更新都将被丢弃。Version 2 - 指定安全设备仅发送和接收 RIP 版本 2 更新。接收的所有版本 1 更新都将被丢弃。Enable default information originate - 选中该复选框以向 RIP 路由进程中生成默认路由。可以配置生成默认路由所必须满足的路由映射。Route-map - 输入要应用的路由映射的名称。如果满足路由映射，则路由进程生成默认路由。IP Network to Add - 为 RIP 路由进程定义网络。指定的网络编号不得包含任何子网信息。可以向安全设备配置中添加的网络数没有限制。RIP 路由更新仅通过指定网络上的接口进行发送和接收。并且，如果某个接口的网络未指定，则该接口不会收到任何 RIP 更新通告。Add - 单击该按钮以将指定网络添加到网络列表中。Delete - 单击该按钮以将所选网络从网络列表中删除。Configure interfaces as passive globally - 选中此复选框以将安全设备上的所有接口设置为被动 RIP 模式。安全设备会监听所有接口上的 RIP 路由广播并使用该信息填充路由表，但不会广播路由更新。使用 Passive Interface 表以将特定接口设置为被动 RIP。Passive Interfaces 表 - 列出安全设备上已配置的接口。对于要在被动模式下操作的接口，选中 Passive 列中对应的复选框。其他接口仍将发送和接收 RIP 广播。

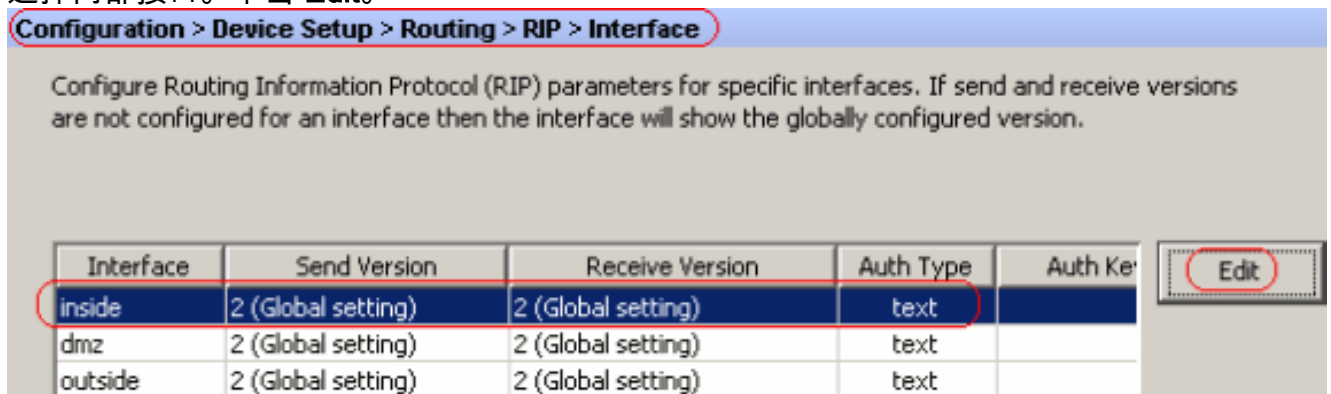
配置 RIP 身份验证

Cisco ASA 支持对来自 RIP v2 路由协议的路由更新进行 MD5 身份验证。每个 RIP 数据包中的 MD5 密钥保护摘要可防止从未经批准的源引入未经授权的或者错误的路由消息。对 RIP 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。在未配置此身份验证的情况下，如果将其他包含不同或相反路由信息的路由设备引入网络，则可能损坏路由器或 Cisco ASA 上的路由表，并可能随之拒绝服务攻击。向在路由设备（包括 ASA）之间发送的 RIP 消息中添加身份验证时，可避免发生故意或意外向网络中添加其他路由器等任何问题。

RIP 路由身份验证基于每个接口进行配置。为 RIP 消息身份验证配置的接口上的所有 RIP 邻居必须配置有相同的身份验证模式和密钥。

要在 Cisco ASA 上启用 RIP MD5 身份验证，请完成以下步骤。

1. 在 ASDM 上，选择 **Configuration > Device Setup > Routing > RIP > Interface**，然后使用鼠标选择内部接口。单击 **Edit**。



2. 选中 **Enable authentication key** 复选框，然后输入 Key 值和 Key ID 值。

Edit RIP Interface Entry

Interface: inside

Send Version

Override global send version

Version 1 Version 2 Version 1 & 2

Receive Version

Override global receive version

Version 1 Version 2 Version 1 & 2

Authentication

Enable authentication key

Key: key123

Key ID: 1

Authentication Mode: MD5 Clear text

OK Cancel Help

单击 OK，然后单击

Apply。

Cisco ASA CLI 配置

Cisco ASA

```

ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! !--- Inside interface
configuration interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !--
- RIP authentication is configured on the inside
interface. rip authentication mode md5 rip
authentication key <removed> key_id 1 ! !--- Output
Suppressed !--- Outside interface configuration
interface Ethernet0/2 nameif outside security-level 0 ip
address 192.168.1.2 255.255.255.0 !--- RIP Configuration
router rip network 10.0.0.0 version 2 !--- This is the
static default gateway configuration in !--- order to
reach the Internet. route outside 0.0.0.0 0.0.0.0
192.168.1.1 1
```

Cisco IOS 路由器 (R2) CLI 配置

Cisco IOS 路由器 (R2)

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5 ip rip authentication
key-chain 1 ! router rip version 2 network 10.0.0.0
network 172.16.0.0 no auto-summary
```

Cisco IOS 路由器 (R1) CLI 配置

Cisco IOS 路由器 (R1)

```
router rip version 2 network 172.16.0.0 no auto-summary
```

Cisco IOS 路由器 (R3) CLI 配置

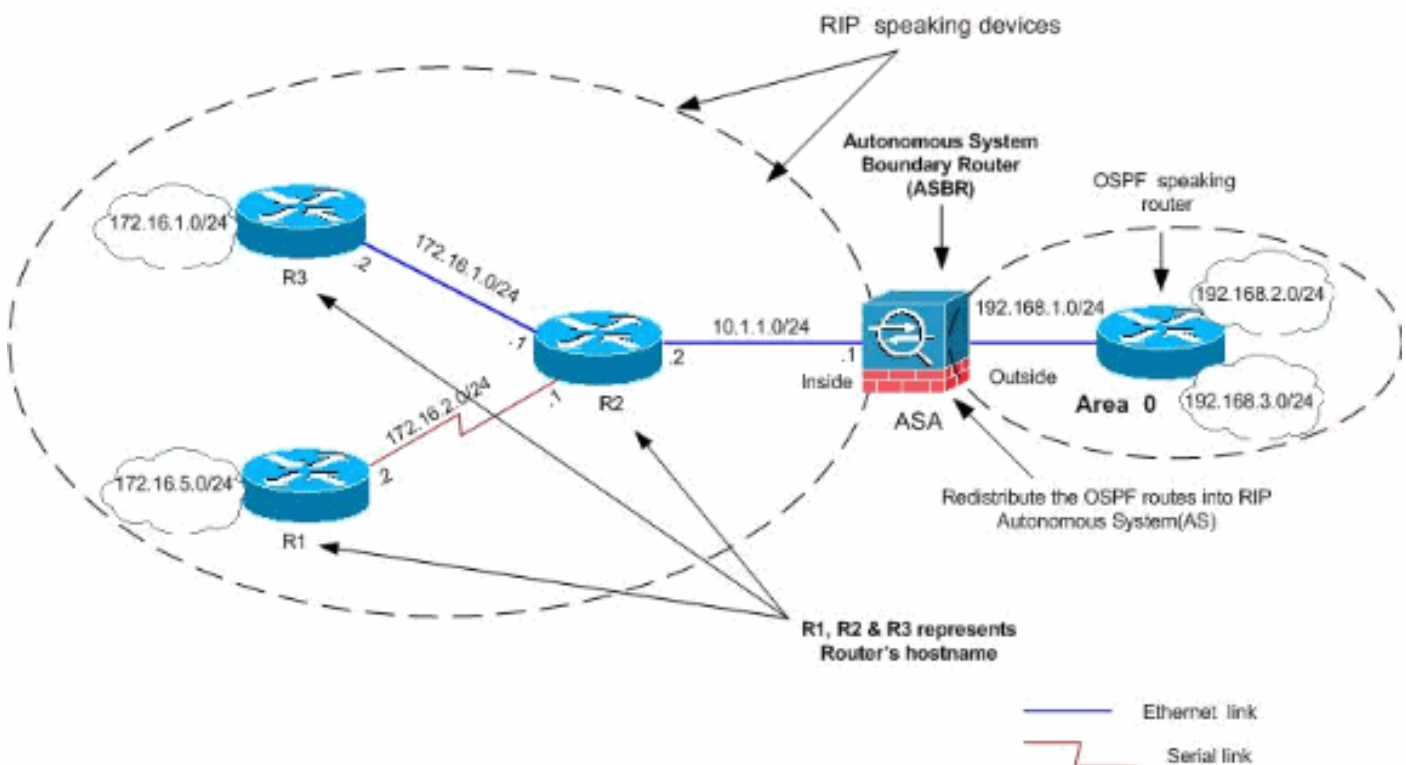
Cisco IOS 路由器 (R3)

```
router rip version 2 network 172.16.0.0 no auto-summary
```

使用 ASA 重分配到 RIP

可以将来自 OSPF、EIGRP、静态和已连接路由进程的路由重分配到 RIP 进程中。

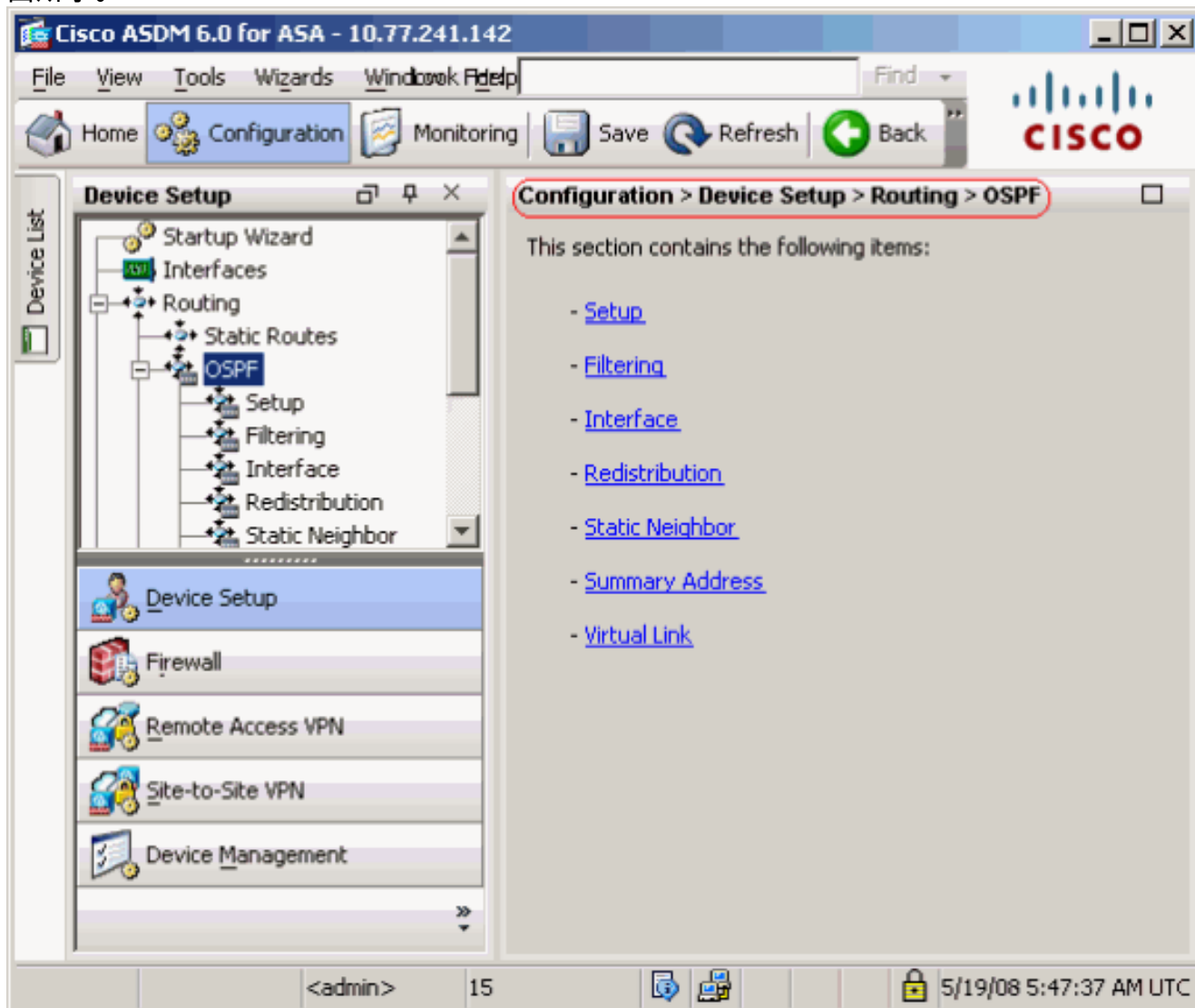
在本示例中，将 OSPF 路由重分配到 RIP 的网络图如下所示：



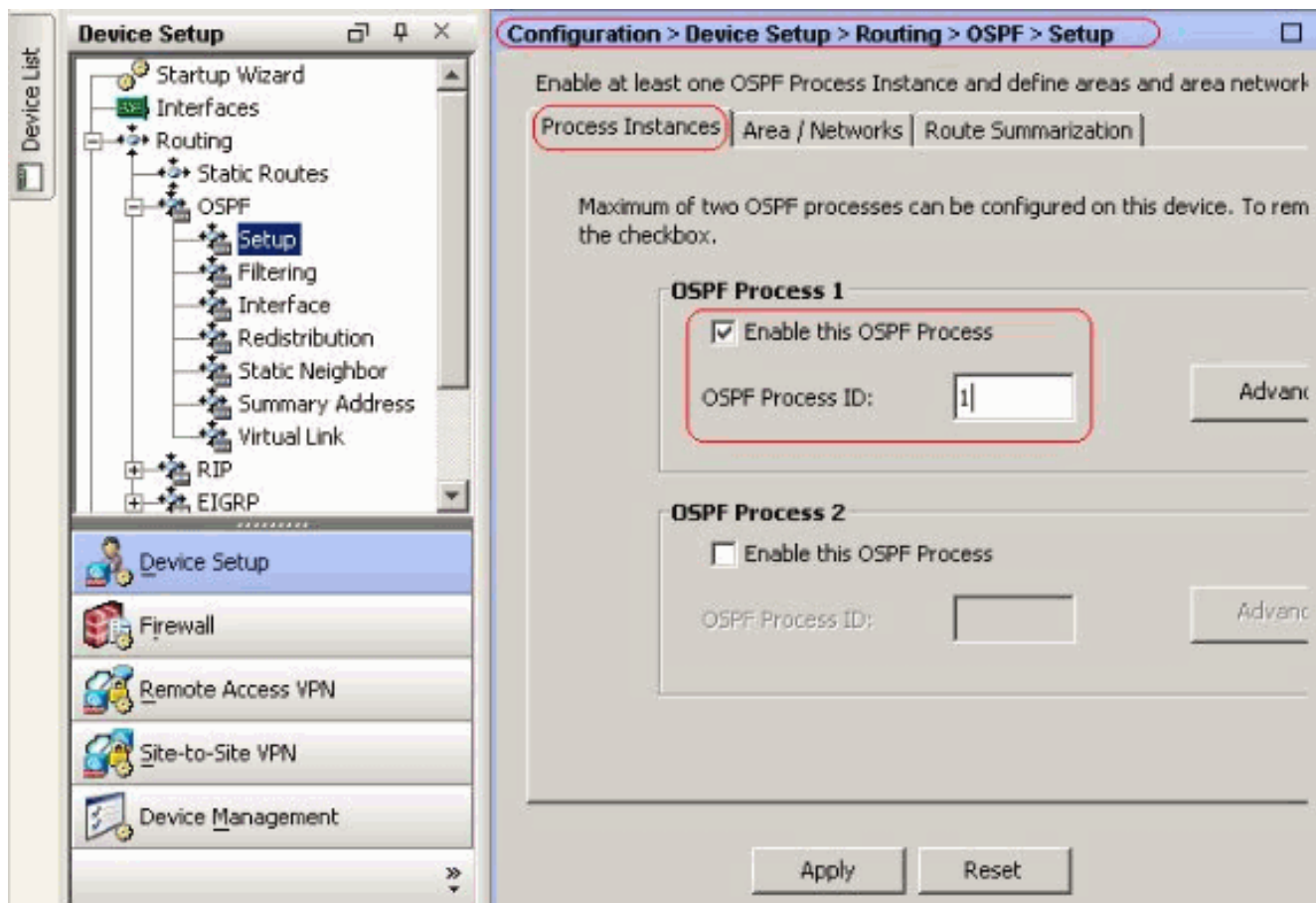
ASDM 配置

完成这些步骤：

1. OSPF 配置在 ASDM 界面中选择 Configuration > Device Setup > Routing > OSPF，如屏幕截图所示。



在 Setup > Process Instances 选项卡中，启用 OSPF 路由进程，如屏幕截图所示。在本示例中，OSPF 进程 ID 是 1。



单击 Setup > Process Instances 选项卡中的 **Advanced**，以配置可选的高级 OSPF 路由进程参数。您可以编辑特定于进程的设置，例如 Router ID、Adjacency Changes、Administrative Route Distances、Timers 和 Default Information Originate 设置。

Edit OSPF Process Advanced Properties

OSPF Process: Router ID:

Ignore LSA MOSPF (suppress the sending of syslog messages when router receives a LSA MOSPF packets) RFC1583 Compatible (calculate summary route costs per RFC 1583)

Adjacency Changes

Enable this for the firewall to send a syslog message when an OSPF neighbor goes up/down. Log Adjacency Changes

Enable this for the firewall to send a syslog for each state change. Log Adjacency Change Details

Administrative Route Distances

Inter Area (distance for all routes from one area to another area)

Intra Area (distance for all routes within an area)

External (distance for all routes from other routing domains, learned by redistribution)

Timers (in seconds)

SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)

SPF Hold Time (between two consecutive SPF calculations)

LSA Group Pacing (interval at which OSPF LSAs are collected into a group and refreshed)

Default Information Originate

Configure this to generate default external route into an OSPF routing domain.

Enable Default Information Originate Always advertise the default route

Metric Value: Metric Type: Route Map:

单击 **Ok**。完成前述步骤后，在 **Setup > Area/Networks** 选项卡中定义 OSPF 路由中涉及的网络和接口。单击 **Add**，如屏幕截图所示。

Configuration > Device Setup > Routing > OSPF > Setup

Enable at least one OSPF Process Instance and define areas and area networks.

Process Instances **Area / Networks** | Route Summarization

Configure the area properties and area networks for OSPF Process

Networks	Authentication	Options	Cost	Add
				Edit
				Delete

将出现此屏幕。在本示例中，添加的唯一网络是外部网络 (192.168.1.0/24)，因为 OSPF 仅在外部接口上启用。**注意**：只有具有定义网络范围内的 IP 地址的接口参与 OSPF 路由进程。

Add OSPF Area

OSPF Process: Area ID:

Area Type

Normal

Stub Summary (allows sending LSAs into the stub area)

NSSA Redistribute (imports routes to normal and NSSA areas)

Summary (allows sending LSAs into the NSSA area)

Default Information Originate (generate a Type 7 default)

Metric Value: Metric Type:

Area Networks

Enter IP Address and Mask

IP Address:

Netmask:

Add >>

Delete

IP Address	Netmask
192.168.1.0	255.255.255.0

Authentication

None Password MD5

Default Cost:

OK Cancel Help

单击 Ok。单击 Apply。

Configuration > Device Setup > Routing > OSPF > Setup

Enable at least one OSPF Process Instance and define areas and area networks.

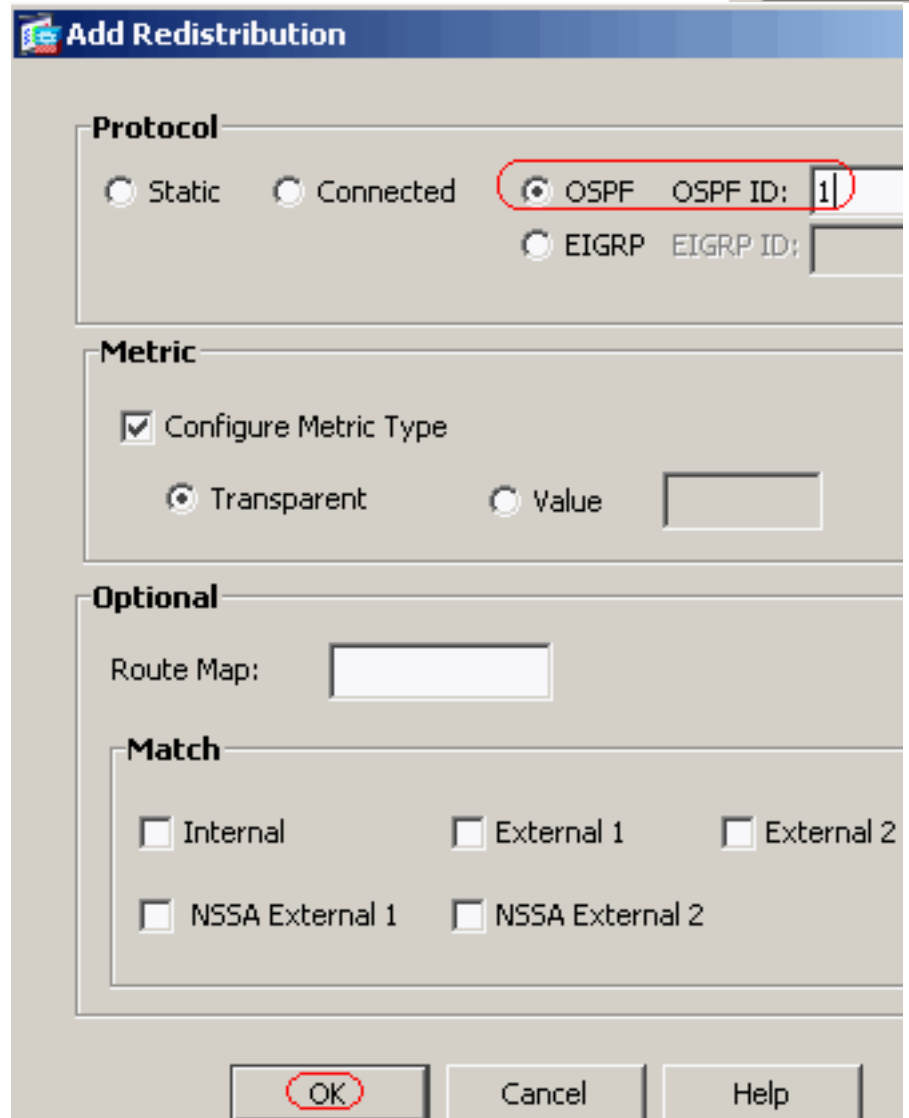
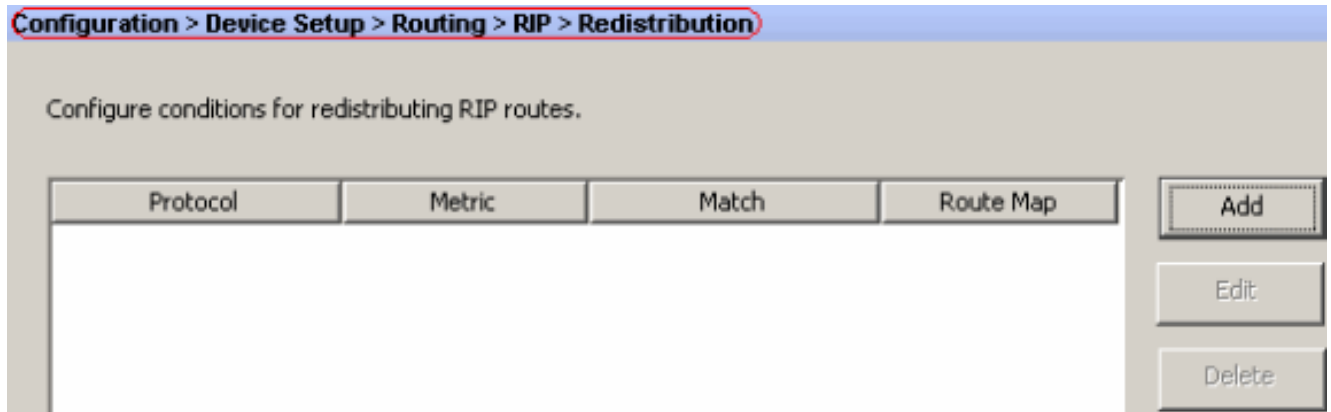
Process Instances **Area / Networks** Route Summarization

Configure the area properties and area networks for OSPF Process

OSPF Process	Area ID	Area Type	Networks	Authe
1	0	Normal	192.168.1.0 / 255.255.255.0	None

Add Edit Delete

2. 选择 Configuration > Device Setup > Routing > RIP > Redistribution > Add，以将 OSPF 路由重分配到 RIP。



3. 单击 OK，然后单击 Apply。

等效 CLI 配置

将 OSPF 重分配到 RIP AS 的 ASA CLI 配置

```
router rip
 network 10.0.0.0
 redistribute ospf 1 metric transparent version 2 !
router ospf 1 router-id 192.168.1.1 network 192.168.1.0
255.255.255.0 area 0 area 0 log-adj-changes
```

将 OSPF 路由重分配到 RIP AS 后，可以看到相邻 Cisco IOS 路由器 (R2) 的路由表。

R2#show ip 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, 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 Gateway of last resort is not set 172.16.0.0/24 is subnetted, 4 subnets R 172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1 R 172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1 C 172.16.1.0 is directly connected, Ethernet1 C 172.16.2.0 is directly connected, Serial1 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.1.1.0/24 is directly connected, Ethernet0 R 10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0 R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0 192.168.2.0/32 is subnetted, 1 subnets R 192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0 192.168.3.0/32 is subnetted, 1 subnets R 192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0 !--- Redistributed route advertised by Cisco ASA

验证

要验证配置，请完成以下步骤：

1. 导航到 **Monitoring > Routing > Routes**，可验证路由表。在此屏幕截图中，可以看到 172.16.1.0/24、172.16.2.0/24、172.16.5.0/24 和 172.16.10.0/24 网络是通过 R2 (10.1.1.2) 使用 RIP 进行识别的。

Monitoring > Routing > Routes

Routes

Each row represents one route. AD is the administrative distance.

Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

2. 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 not set R 172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside R 172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside C 10.1.1.0 255.255.255.0 is directly connected, inside C 10.77.241.128 255.255.255.192 is directly connected, dmz S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz C 192.168.1.0 255.255.255.0 is directly connected, outside O 192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside O 192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside ciscoasa#

故障排除

此部分包括有关对于排除 OSPF 故障可能有用的 debug 命令的信息。

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](#)。

- **debug rip events - 启用 RIP 事件的调试**

```
ciscoasa#debug rip events rip_route_adjust for inside
coming up RIP: sending request on inside to 224.0.0.9 RIP: received v2 update from 10.1.1.2
on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0
in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0
in 2 hops RIP: Update contains 4 routes RIP: received v2 update from 10.1.1.2 on inside
172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes RIP: sending v2 flash update to 224.0.0.9 via dmz
(10.77.241.142) RIP: build flash update entries 10.1.1.0 255.255.255.0 via 0.0.0.0, metric
1, tag 0 172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.2.0 255.255.255.0 via
0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 172.16.10.0
255.255.255.0 via 0.0.0.0, metric 3, tag 0 RIP: Update contains 5 routes RIP: Update queued
RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1) RIP: build flash update
entries - suppressing null update RIP: Update sent via dmz rip-len:112 RIP: sending v2
update to 224.0.0.9 via dmz (10.77.241.142) RIP: build update entries 10.1.1.0 255.255.255.0
via 0.0.0.0, metric 1, tag 0 172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0,
metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 192.168.1.0
255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric
12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 8
routes RIP: Update queued RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1) RIP:
build update entries 10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0 192.168.1.0
255.255.255.0 via 0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric
12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 4
routes RIP: Update queued RIP: Update sent via dmz rip-len:172 RIP: Update sent via inside
rip-len:92 RIP: received v2 update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via
0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via
0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP: Update contains 4
routes
```

相关信息

- [Cisco 5500 系列自适应安全设备支持页](#)
- [Cisco 500 系列 PIX 支持页](#)
- [PIX/ASA 8.X：在 Cisco 自适应安全设备 \(ASA\) 上配置 EIGRP](#)
- [技术支持和文档 - Cisco Systems](#)