

# 使用OSPF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 OSPF 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 OSPF](#)

[验证](#)

[故障排除](#)

[点对点网络的静态邻居配置](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文档介绍如何配置 Cisco ASA 以通过开放最短路径优先 (OSPF) 识别路由、执行身份验证和重分配。

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：**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 OSPF；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

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

## 背景信息

OSPF 使用链路状态算法来生成和计算指向所有已知目标的最短路径。OSPF 区域的每个路由器包含一个相同的链路状态数据库，该数据库是包含每个路由器可用接口和可到达邻居的列表。

OSPF 优于 RIP 之处包括：

- OSPF 链路状态数据库更新的发送不及 RIP 更新频繁，并且当过期信息超时，立刻（而不是逐步）更新链路状态数据库。
- 路由决策基于成本，而成本指示通过某接口发送数据包所需的开销。安全设备根据链路带宽而不是到目标的跳数计算接口的成本。可以配置成本来指定首选路径。

最短路径优先算法的缺点是需要大量的 CPU 周期和内存。

安全设备可以在不同的接口组上同时运行 OSPF 协议的两个进程。如果有使用相同 IP 地址的接口（NAT 允许这些接口共存，但 OSPF 不允许地址重叠），您最好运行两个进程。或者您最好在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重分配路由的子集。同样，您最好将专用地址与公用地址隔离开来。

您可以将路由从另一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口配置的静态和连接的路由重分配到一个 OSPF 路由进程。

安全设备支持以下 OSPF 功能：

- 支持域内、域间和外部（类型 I 和类型 II）路由。
- 支持虚拟链路。
- OSPF LSA 泛洪。
- 对 OSPF 数据包的验证（口令和 MD5 身份验证）。
- 支持将安全设备配置为指定路由器或指定的备用路由器。还可以将安全设备设置为 ABR。然而

- ，将安全设备配置为 ASBR 的功能仅限于默认信息（例如，注入默认路由）。
- 支持残域和非完全残域。
- 区域边界路由器类型 3 LSA 过滤。

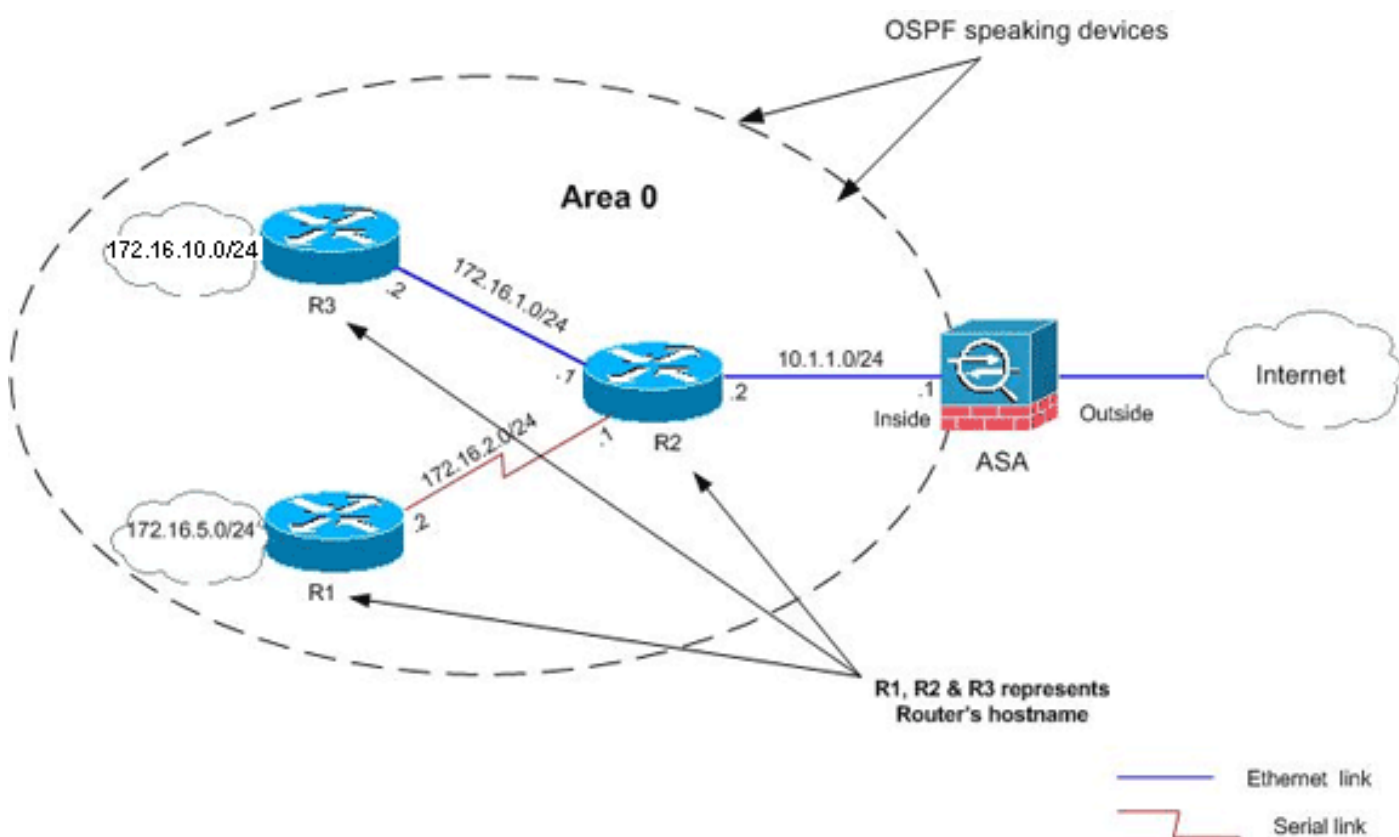
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要获取有关本部分中所使用命令的更多信息，可使用[命令查找工具](#)（仅限[已注册](#)客户）。

## 网络图

本文档使用以下网络设置：



在此网络拓扑中，Cisco ASA内部接口IP地址为10.1.1.1/24。目标是在Cisco ASA上配置OSPF，以便通过相邻路由器(R2)动态获取到内部网络(172.16.1.0/24、172.16.2.0/24、172.16.5.0/24和172.16.10.0/24)的路由。R2 通过其他两个路由器（R1 和 R3）识别通往远程内部网络的路由。

## 配置

本文档使用以下配置：

- [ASDM 配置](#)
- [配置 OSPF 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](#)

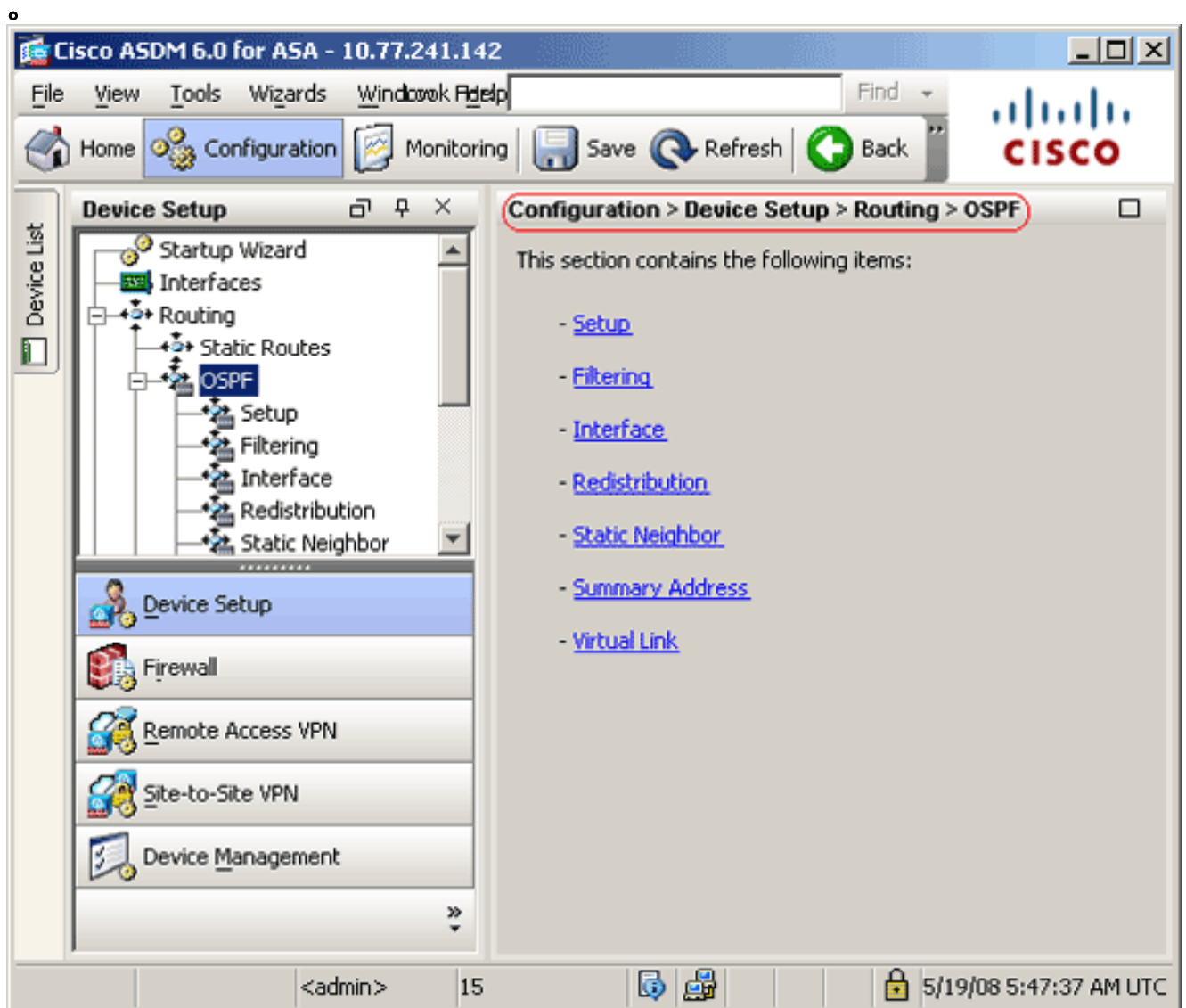
- [使用 ASA 重分配到 OSPF](#)

## ASDM 配置

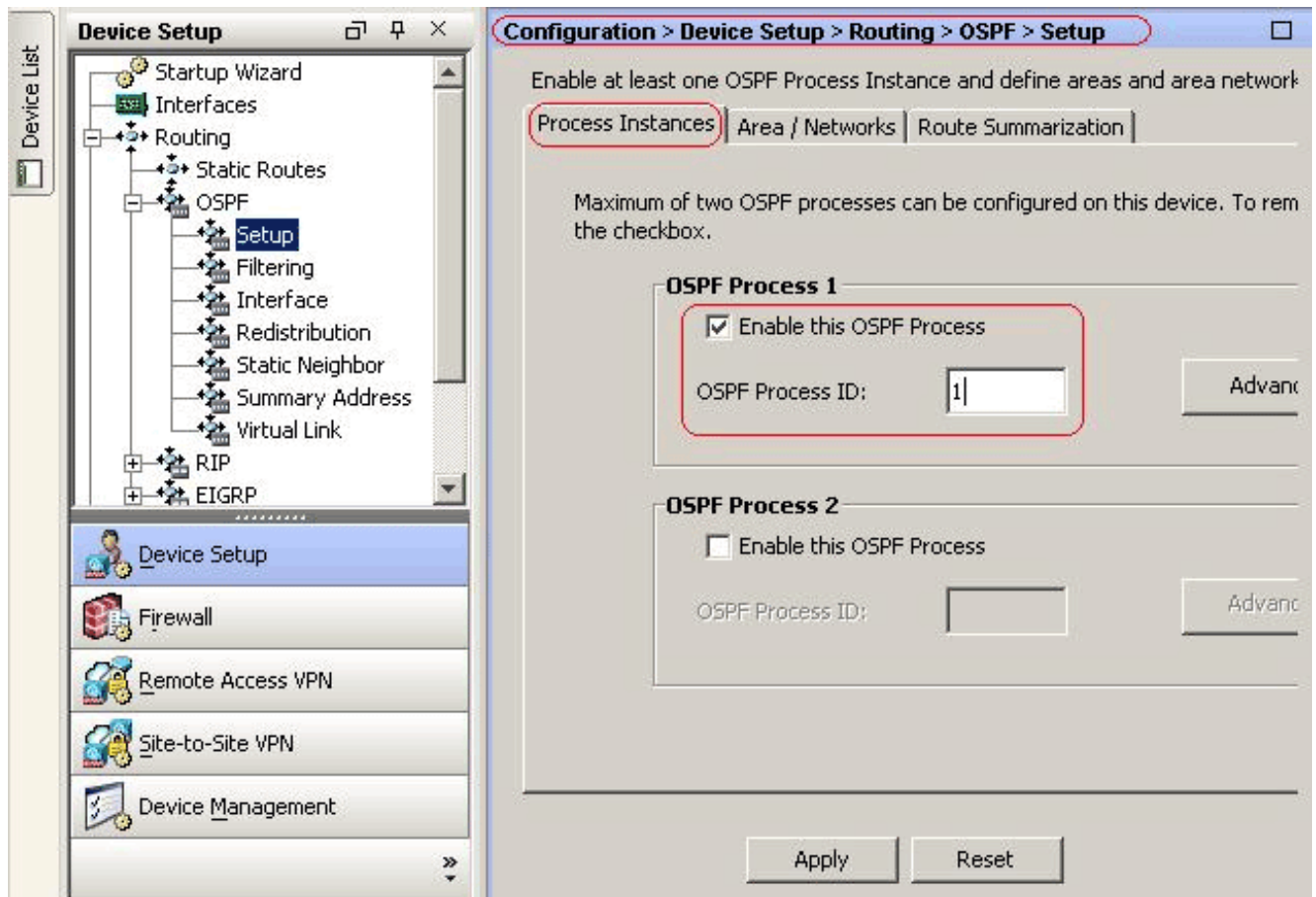
自适应安全设备管理器 (ASDM) 是一个基于浏览器的应用程序，用于配置和监控安全设备上的软件。ASDM 从安全设备加载，然后用于配置、监控和管理设备。还可以使用 ASDM 启动程序（仅适用于 Windows）以比 Java 小程序更快速地启动 ASDM 应用程序。本部分介绍了使用 ASDM 配置本文档中所述功能所需的信息。

请通过完成以下步骤在 Cisco ASA 中配置 OSPF：

1. 登录到使用 ASDM 的 Cisco ASA。
2. 导航到 ASDM 界面的 **Configuration > Device Setup > Routing > OSPF** 区域，如此图中所示



3. 启用 **Setup > Process Instances** 选项卡上的 OSPF 路由进程，如此图中所示。在本示例中，OSPF 进程 ID 是 1。



4. 您可以单击 Setup > Process Instances 选项卡上的 **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)
<input type="text" value="110"/>	<input type="text" value="110"/>	<input type="text" value="110"/>

**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)
<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="text" value="240"/>

**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:

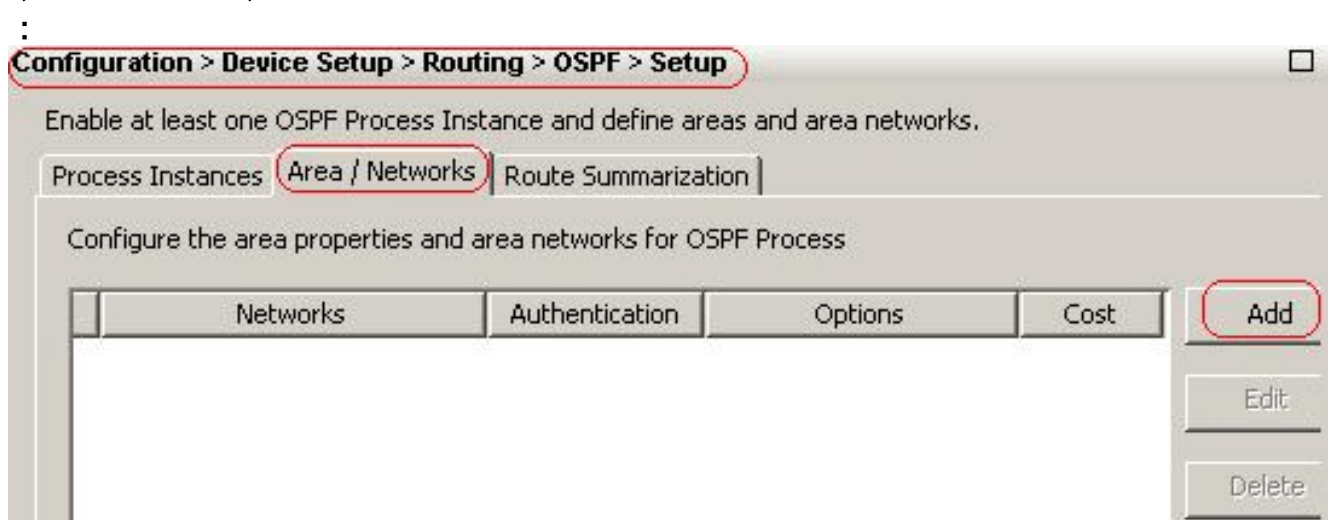
OK Cancel Help

此列表介绍了每个字段：OSPF Process - 显示您正在配置的 OSPF 进程。不能更改此值。Router ID - 为使用固定的路由器 ID，在 Router ID 字段中以 IP 地址格式输入路由器 ID。如果将此值留空，将使用安全设备上最高级别的 IP 地址作为路由器 ID。在本示例中，使用内部接口的 IP 地址 (10.1.1.1) 静态配置 Router ID。Ignore LSA MOSPF - 选中此复选框可在安全设备接收类型 6 (MOSPF) LSA 数据包时禁止发送系统日志消息。默认情况下取消选中此设置。RFC 1583兼容 — 选中此复选框以计算每个 RFC 1583 的汇总路由开销。取消选中此复选框可计算每个 RFC 2328 的汇总路由成本。为了使路由环路的可能性降至最低，OSPF 路由域中的所有 OSPF 设备应设置相同的 RFC 兼容性。默认情况下选中此设置。Adjacency Changes - 包含如此定义的设置，即在发生邻接更改时发送系统日志消息。Log Adjacency Changes - 选中此复选框可在 OSPF 邻居接通或断开时导致安全设备发送系统日志消息。默认情况下选中此设置。Log Adjacency Changes Detail - 选中此复选框可在发生任何状态更改时（不仅是邻居接通或断开时）导致安全设备发送系统日志消息。默认情况下取消选中此设置。Administrative Route Distances - 包含基于路由类型的路由管理距离的设置。Inter Area - 设置一个区域到另一个区域的所有路由的管理距离。有效值范围为1到255。默认值为100。Intra Area - 设置区域内所有路由的管理距离。有效值范围为1到255。默认值为100。



External - 设置通过重分配识别的其他路由域中所有路由的管理距离。有效值范围为1到255。默认值为100。Timers - 包含用于配置 LSA 步调和 SPF 计算计时器的设置。SPF Delay Time - 指定在 OSPF 接收拓扑更改和 SPF 计算开始之间的时间差。有效值范围为0到65535。默认值为5。SPF Hold Time — 指定连续SPF计算之间的保持时间。有效值范围为1到65534。默认值为10。LSA Group Pacing - 指定将 LSA 收集到组并刷新、进行校验和计算或使之老化的时间间隔。有效值范围为从 10 到 1800。默认值为 240。Default Information Originate - 包含 ASBR 用于将默认外部路由生成到 OSPF 路由域的设置。Enable Default Information Originate - 选中此复选框可使默认路由生成到 OSPF 路由域。Always advertise the default route - 选中此复选框可始终通告默认路由。默认情况下取消选中此选项。Metric Value - 指定 OSPF 默认度量值。有效值范围为0到16777214。默认值为1。Metric Type - 指定与通告到 OSPF 路由域的默认路由关联的外部链路类型。有效值是 1 或 2，指示类型 1 或类型 2 外部路由。默认值为 2。Route Map - ( 可选 ) 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。

5. 完成前面的步骤后，请在 **Setup > Area/Networks** 选项卡上定义参与 OSPF 路由的网络和接口，然后单击 **Add**，如此图中所示



此时将会显示 Add OSPF Area 对话框。

OSPF Process: 1 Area ID: 0

**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: 1 Metric Type: 2

**Area Networks**

Enter IP Address and Mask

IP Address:

Netmask: 255.255.255.0

Add >>

Delete

IP Address	Netmask
10.1.1.0	255.255.255.0

**Authentication**

None  Password  MD5

Default Cost: 1

OK Cancel Help

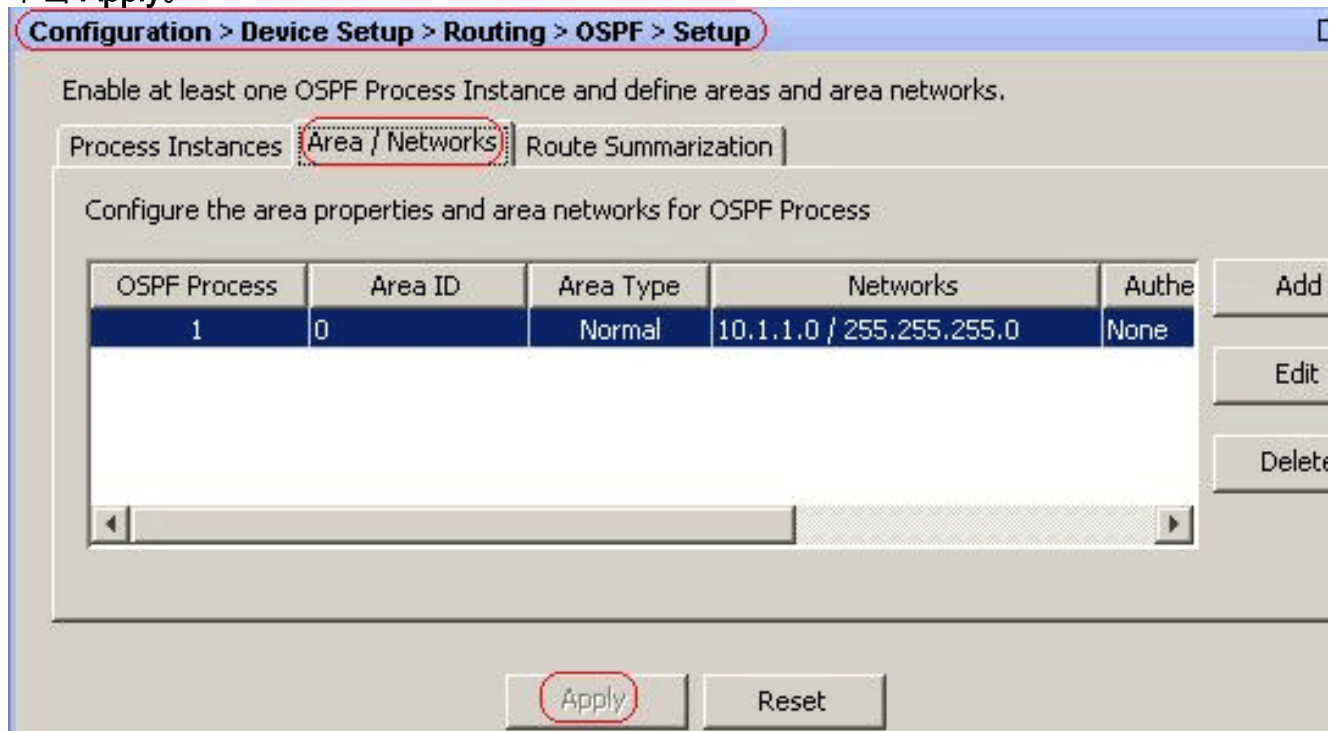
在本示例中，由于只在内部接口上启用 OSPF，因此所添加的唯一网络是内部网络 (10.1.1.0/24)。注意：只有 IP 地址在已定义网络内的接口才参与 OSPF 路由进程。

6. Click **OK**. 此列表介绍了以下每个字段：OSPF Process - 添加新区域时，选择 OSPF 进程的 ID。如果在安全设备上只启用了—个 OSPF 进程，则默认情况下选中该进程。编辑现有区域时，不能更改 OSPF 进程 ID。Area ID - 添加新区域时，输入区域 ID。可以将区域 ID 指定为十进制数字或 IP 地址。有效的十进制值范围为 0 到 4294967295。编辑现有区域时无法更改区域 ID。在本示例中，Area ID 是 0。Area Type - 包含所配置区域的类型的设置。Normal - 选择此选项可使该区域成为标准的 OSPF 区域。默认情况下，在您最初创建区域时选中此选项。Stub - 选择此选项可使该区域成为残域。残域不具有任何存在于其自身区域之外的路由器或区域。设置残域，可防止 AS 外部 LSA (类型 5 LSA) 泛洪至残域。创建残域时，可以取消选中 Summary 复选框以防止汇总 LSA (类型 3 和 4) 泛洪至该区域。Summary - 当所定义的区域是残域时，取消选中此复选框可防止 LSA 发送到残域。默认情况下为残域选中此复选框。NSSA - 选择此选项可使该区域成为非完全残域。NSSA 接受类型 7 LSA。创建 NSSA 时，可以取消选中 Summary 复选框以防止汇总 LSA 泛洪至该区域。此外，还可以取消选中 Redistribute 复选框并启用 Default Information Originate 以禁用路由重分配。



Redistribute - 取消选中此复选框可防止路由导入到 NSSA。默认情况下选中此复选框。  
 Summary - 当所定义的区域是 NSSA 时，取消选中此复选框可防止 LSA 发送到残域。默认情况下为 NSSA 选中此复选框。  
 Default Information Originate - 选中此复选框可将类型 7 默认值生成到 NSSA 中。默认情况下取消选中此复选框。  
 Metric Value - 输入一个值以为默认路由指定 OSPF 度量值。有效值范围为 0 到 16777214。默认值为 1。  
 Metric Type - 选择一个值以为默认路由指定 OSPF 度量类型。选项为 1 (类型 1) 或 2 (类型 2)。默认值为 2。  
 Area Networks - 包含定义 OSPF 区域的设置。  
 Enter IP Address and Mask - 包含用于定义区域中网络的设置。  
 IP Address - 输入要添加到区域的网络的 IP 地址，或者主机。将 0.0.0.0 与网络掩码 0.0.0.0 一起使用可创建默认区域。只能在一个区域中使用 0.0.0.0。  
 Netmask - 选择要添加到区域的 IP 地址或主机的网络掩码。如果添加主机，则选择 255.255.255.255 掩码。在本示例中，10.1.1.0/24 是要配置的网络。  
 Add - 将在 Enter IP Address and Mask 区域定义的网络添加到区域。添加的网络显示在 Area Networks 表中。  
 Delete - 从 Area Networks 表删除所选网络。  
 Area Networks - 显示为区域定义的网络。  
 IP Address - 显示网络的 IP 地址。  
 Netmask - 显示网络的网络掩码。  
 Authentication - 包含用于 OSPF 区域身份验证的设置。  
 None - 选择此选项可禁用 OSPF 区域身份验证。这是默认设置。  
 Password - 选择此选项可将明文口令用于区域身份验证。如果重视网络安全的话，不建议使用此选项。  
 MD5 - 选择此选项以使用 MD5 身份验证。  
 Default Cost - 指定区域的默认成本。有效值范围为 0 到 65535。默认值为 1。

7. 单击 **Apply**。



8. 还可以在 Filter Rules 窗格中定义路由过滤器。路由过滤可对允许在 OSPF 更新中发送或接收的路由提供更多控制。
9. 您也可以选择配置路由重分配。Cisco ASA 可以将 RIP 和 EIGRP 发现的路由重分配到 OSPF 路由进程。您还可以将静态和连接的路由重分配到 OSPF 路由进程。请在 Redistribution 窗格中定义路由重分配。
10. OSPF hello 数据包作为多播数据包发送。如果 OSPF 邻居位于非广播网络，则必须手动定义该邻居。手动定义 OSPF 邻居时，hello 数据包作为单播报文发送到该邻居。为了定义静态 OSPF 邻居，请转到 Static Neighbor 窗格。
11. 可以汇总从其他路由协议识别的路由。用于通告汇总的度量值是所有更为具体路由的最小度量值。汇总路由有助于减小路由表的大小。使用 OSPF 的汇总路由可导致 OSPF ASBR 将一个外部路由通告为相应地址包括的所有重分配路由的聚合。只能汇总重分配到 OSPF 的其他

路由协议中的路由。

- 在 Virtual link 窗格中，可以向 OSPF 网络添加区域，并且无法将该区域直接连接到主干区域；您必须创建虚拟链路。虚拟链路可连接具有公用区域（称为中转区域）的两个 OSPF 设备。其中一个 OSPF 设备必须连接到主干区域。

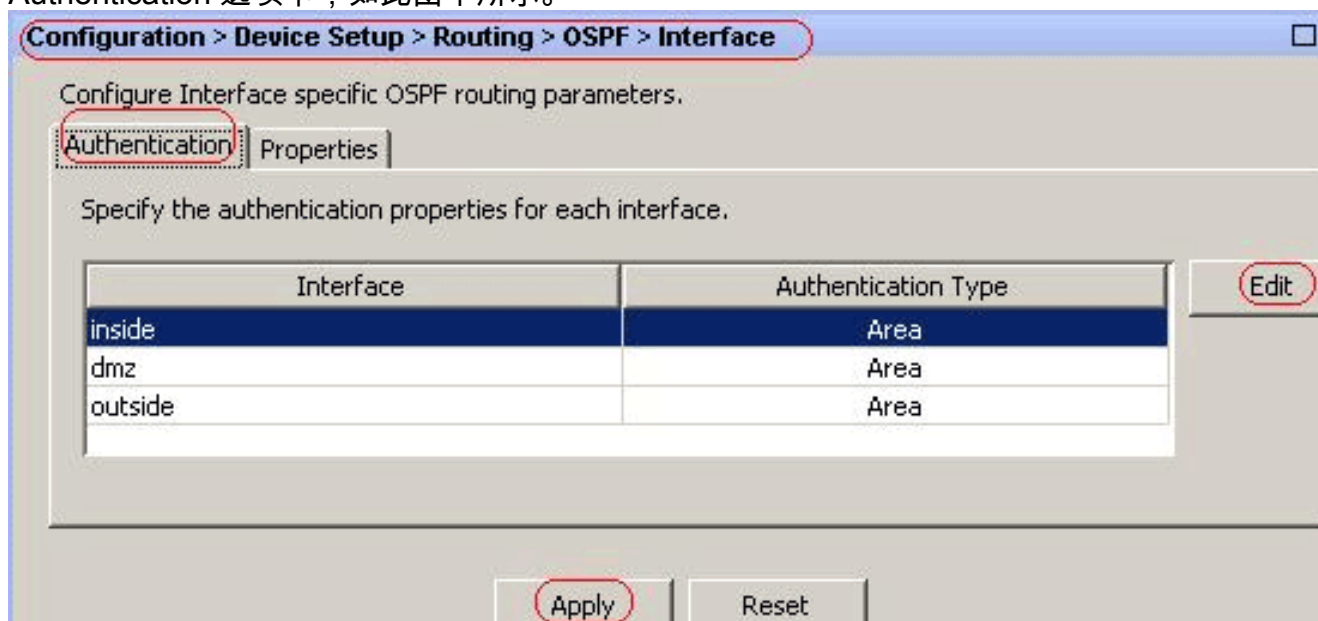
## 配置 OSPF 身份验证

Cisco ASA 支持从 OSPF 路由协议更新路由的 MD5 身份验证。每个 OSPF 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 OSPF 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，如果某人将具有不同或相反路由信息的另一个路由设备引入到网络，则您路由器上的路由表或 Cisco ASA 可能会发生损坏，并且可能随之发生拒绝服务攻击。向在路由设备（包括 ASA）之间发送的 EIGRP 消息添加身份验证后，可防止向网络故意或意外添加其他路由器以及任何其他问题。

OSPF 路由身份验证基于每个接口进行配置。对于针对 OSPF 消息身份验证配置的接口上的所有 OSPF 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。

完成以下步骤以在 Cisco ASA 启用 OSPF MD5 身份验证：

- 在 ASDM 上，导航到 **Configuration > Device Setup > Routing > OSPF > Interface**，然后单击 Authentication 选项卡，如此图中所示。



在本示例中，OSPF 已在内部接口上启用。

- 选择 **inside** 接口，然后单击 **Edit**。
- 在 Authentication 下，选择 **MD5 authentication**，并在此处添加有关身份验证参数的更多信息。在本示例中，预共享密钥是 **cisco123**，密钥 ID 是 **1**。

**Edit OSPF Interface Authentication**

Interface:

**Authentication**

No authentication
  Area authentication, if defined
  **MD5 authentication**

**Authentication Password**

Enter Password:  Re-enter Password:

**MD5 IDs and Keys**

MD5 Key ID:

MD5 Key:

MD5 Key ID	MD5 Key
1	cisco123

4. 单击 OK，然后单击 Apply。

**Configuration > Device Setup > Routing > OSPF > Interface**

Configure Interface specific OSPF routing parameters.

Specify the authentication properties for each interface.

Interface	Authentication Type
inside	MD5
dmz	Area
outside	Area

[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 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
  network 10.1.1.0 255.255.255.0 area 0
  log-adj-changes
!

!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

## Cisco IOS 路由器 (R2) CLI 配置

### Cisco IOS 路由器 (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0
ip address 10.1.1.2 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco123

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.1.0 0.0.0.255 area 0
  network 172.16.2.0 0.0.0.255 area 0
```

## Cisco IOS 路由器 (R1) CLI 配置

### Cisco IOS 路由器 (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 172.16.5.0 0.0.0.255 area 0
```

```
network 172.16.2.0 0.0.0.255 area 0
```

## Cisco IOS 路由器 (R3) CLI 配置

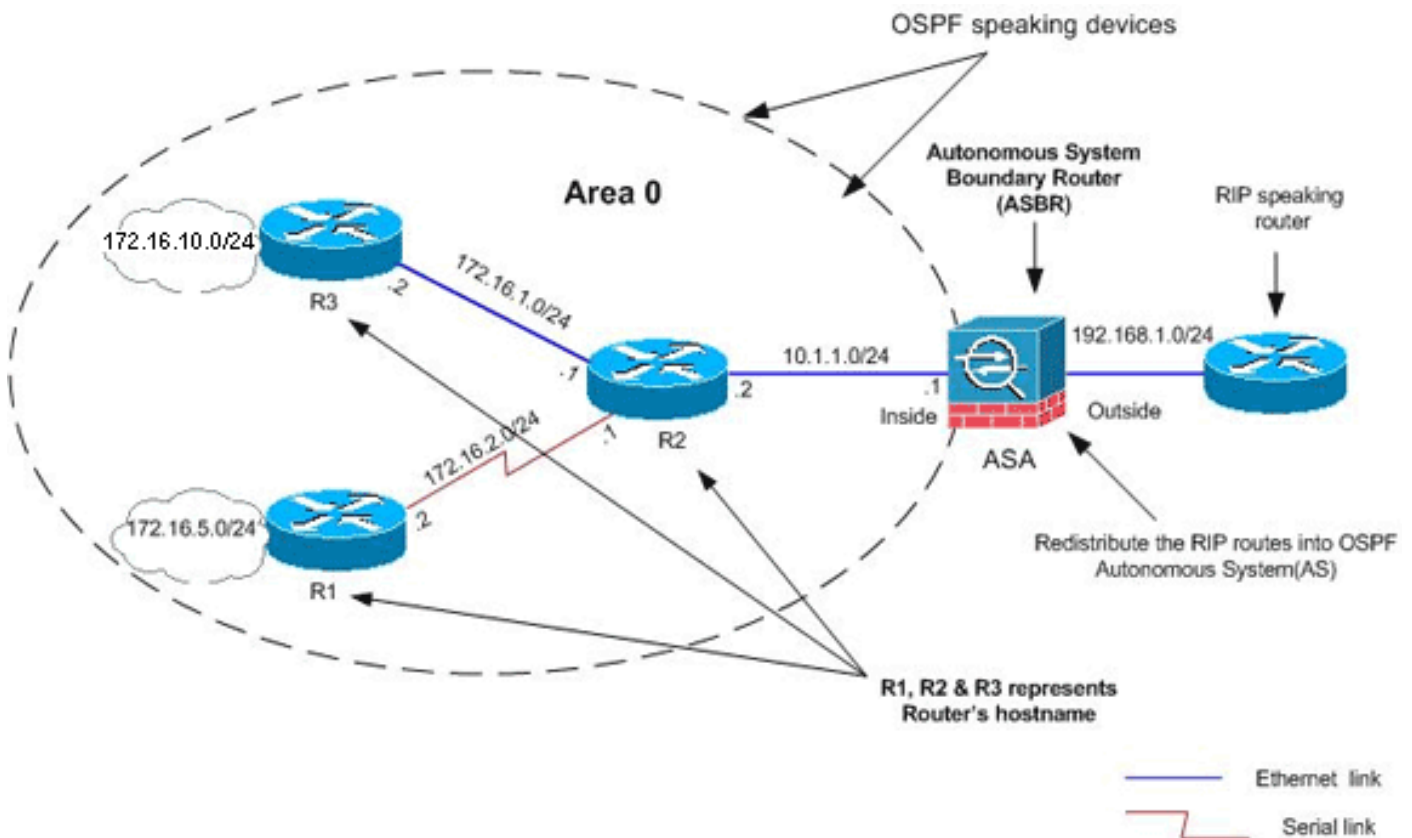
### Cisco IOS 路由器 (R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0
network 172.16.10.0 0.0.0.255 area 0
```

## 使用 ASA 重分配到 OSPF

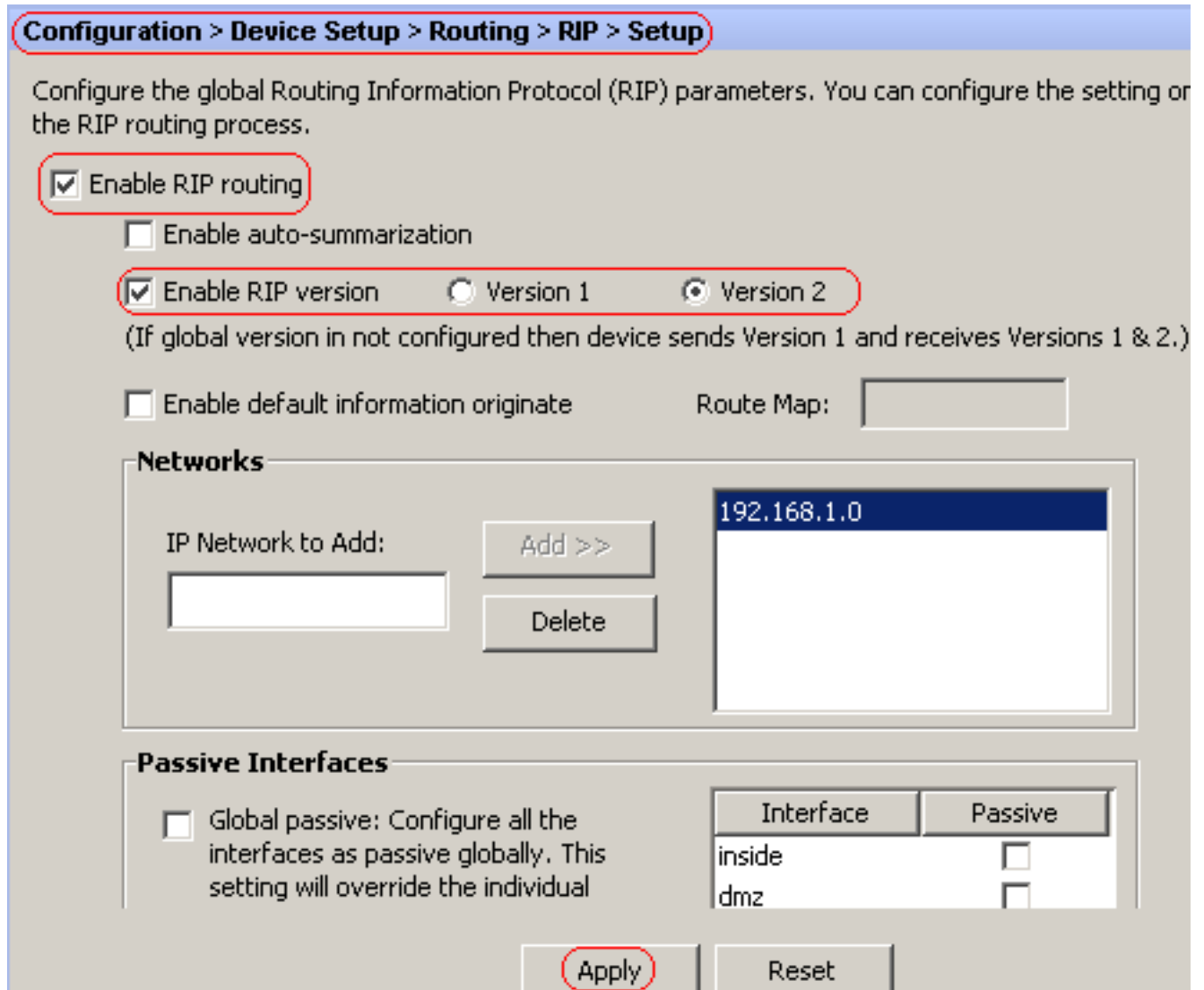
如前所述，您可以将路由从另一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口上配置的静态和连接的路由，重分配到一个 OSPF 路由进程。

在本示例中，使用如下所示的网络图将 RIP 路由重分配到 OSPF：

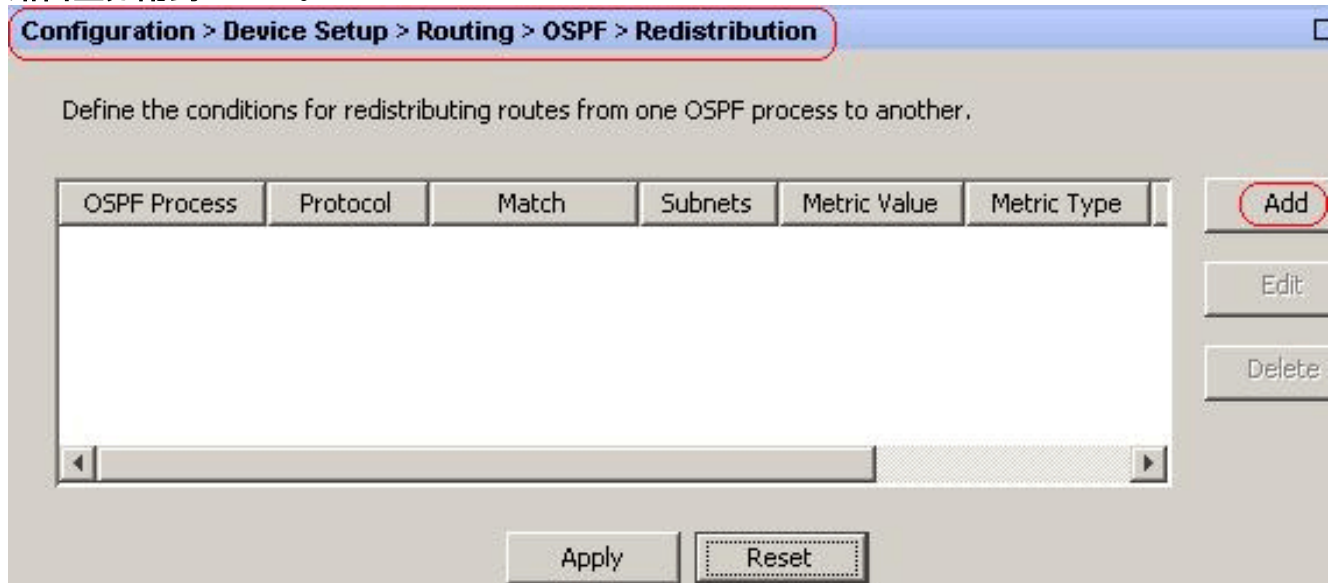


## ASDM 配置

1. 依次选择 Configuration > Device Setup > Routing > RIP > Setup 以启用 RIP，并添加网络 192.168.1.0，如此图中所示。



2. 单击 **Apply**。
3. 依次选择 **Configuration > Device Setup > Routing > OSPF > Redistribution > Add** 以将 RIP 路由重分配到 OSPF。



4. 单击 **OK**，然后单击 **Apply**。



**Add OSPF Redistribution Entry**

OSPF Process: 1

**Protocol**

Static  Connected  OSPF

**RIP**  EIGRP

**Optional**

**Match**

Internal  External 1  External 2  NSSA External 1  NSSA External 2

Metric Value:  Metric Type: 2 Tag Value:   Use subnets

Route Map:

### 等效 CLI 配置

#### 用于将 RIP 重分配到 OSPF AS 的 ASA 之 CLI 配置

```

router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 log-adj-changes
 redistribute rip subnets

router rip
 network 192.168.1.0

```

将 RIP 路由重分配到 OSPF AS 之后，可以看到邻居 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

```

       172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
O       172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C       172.16.1.0/24 is directly connected, Ethernet1
C       172.16.2.0/24 is directly connected, Serial1
       10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Ethernet0
O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0
!--- Redistributed route adversted by Cisco ASA

```

## 验证

完成以下步骤以验证您的配置：

1. 在 ASDM 上，可以导航到 **Monitoring > Routing > OSPF Neighbors** 查看每一个 OSPF 邻居。此图将内部路由器 (R2) 显示为活动邻居。还可以查看此邻居驻留的接口、邻居路由器 ID、状态和 dead 时间。

**Monitoring > Routing > OSPF Neighbors**

OSPF Neighbors

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

Neighbor	Priority	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:34	10.1.1.2	inside

Last Updated: 5/19/08 3:55:10 PM

2. 此外，如果导航到 **Monitoring > Routing > Routes**，还可以验证路由表。在此图中，通过 R2 (10.1.1.2) 识别了 172.16.1.0/24、172.16.2.0/24、172.16.5.0/24 和 172.16.10.0/24 网络。

**Monitoring > Routing > Routes**

Routes

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

Protocol	Type	Destination IP	Netmask	Gateway	Int
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
OSPF	-	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
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	outside

3. 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 192.168.1.1 to network 0.0.0.0
```

```
O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, 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
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside

```

#### 4. 也可以使用 `show ospf database` 命令获得关于识别的网络和 ospf 拓扑的信息。

```
ciscoasa#show ospf database
```

```
OSPF Router with ID (192.168.1.2) (Process ID 1)
```

##### Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.16.1.2	172.16.1.2	123	0x80000039	0xfd1d	2
172.16.2.1	172.16.2.1	775	0x8000003c	0x9b42	4
172.16.5.1	172.16.5.1	308	0x80000038	0xb91b	3
192.168.1.2	192.168.1.2	1038	0x80000037	0x29d7	1

##### Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	192.168.1.2	1038	0x80000034	0x72ee
172.16.1.1	172.16.2.1	282	0x80000036	0x9e68

#### 5. `show ospf neighbors` 命令在验证活动邻居和对应的信息方面也很有用。此示例显示的信息与您在步骤 1 中从 ASDM 获得的信息相同。

```
ciscoasa#show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:36	10.1.1.2	inside

## 故障排除

本节提供有助于排除 OSPF 故障的信息。

### 点对点网络的静态邻居配置

如果已在 ASA 上配置了 OSPF 网络点对点非广播，则必须定义静态 OSPF 邻居以在点对点非广播网络上通告 OSPF 路由。有关详细信息，[请参阅定义静态 OSPF 邻居](#)。

### 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：**在使用 debug 命令之前，[请参阅](#)有关 Debug 命令的重要信息。

- **debug ospf events** - 启用对 OSPF 事件的调试。

```

ciscoasa(config)#debug ospf events
OSPF events debugging is on
ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu
ciscoasa(config-if)#
OSPF: Interface inside going Up
OSPF: Send with youngest Key 1

```

```
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
OSPF: Backup seen Event before WAIT timer on inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 172.16.2.1
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 172.16.2.1 (Id)
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32
OSPF: Send with youngest Key 1
OSPF: End of hello processing
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32  mtu
 1500 state EXSTART
OSPF: First DBD and we are not SLAVE
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152  mt
u 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the MASTER
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Database request to 172.16.2.1
OSPF: sent LS REQ packet to 10.1.1.2, length 12
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Exchange Done with 172.16.2.1 on inside
OSPF: Synchronized with 172.16.2.1 on inside, state FULL
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: Neighbor change Event on interface inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 192.168.1.2 (Id)
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

**注意：**有关各种命令的详细信息，请参阅[Cisco安全设备命令参考8.0版](#)中的debug ospf部分，这些命令对故障排除很有帮助。

## [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](#)