



OSPF

本章介绍如何将 ASA 配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

- [关于 OSPF，第 1 页](#)
- [OSPF 准则，第 4 页](#)
- [配置 OSPFv2，第 6 页](#)
- [配置 OSPFv2 路由器 ID，第 9 页](#)
- [自定义 OSPFv2，第 10 页](#)
- [配置 OSPFv3，第 26 页](#)
- [配置无中断重启，第 36 页](#)
- [OSPFv2 示例，第 40 页](#)
- [OSPFv3 示例，第 42 页](#)
- [监控 OSPF，第 44 页](#)
- [OSPF 历史记录，第 45 页](#)

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

相比 RIP，OSPF 具有以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于开销，它表明通过特定接口发送数据包所需的开销。ASA 根据链路带宽而非到目标的跃点数计算接口的开销。可以配置开销来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

ASA 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠地址），则可能要运行两个进程。或者，可能要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新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

您可以将路由从一个 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路由和已连接路由重新分发到另一个 OSPF 路由进程中。

ASA 支持以下 OSPF 功能：

- 区域内、区域间和外部（I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证（密码和 MD5 身份验证）。
- 将 ASA 配置为指定路由器或指定备用路由器。ASA 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议（如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 筛选，您可以具有单独的以 ASA 作为 ABR 的专用和公共区域。3 类 LSA（区域间路由）可以从一个区域筛选到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。



注释 只能筛选 3 类 LSA。如果在专用网络中将 ASA 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将到公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 ASA 保护的专用网络配置静态路由。此外，不应在同一 ASA 接口上混用公用和专用网络。

您可以同时在 ASA 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

OSPF 快速呼叫数据包支持功能提供了一种以短于一秒的间隔发送呼叫数据包的配置方式。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

OSPF 支持快速呼叫数据包的前提条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

关于快速呼叫数据包의 OSPF 支持

与快速呼叫数据包의 OSPF 支持相关的主要概念，以及 OSPF 快速呼叫数据包的优势如下所述：

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔（以秒为单位）进行发送。对于以太网链路，默认值为 10 秒；对于非广播链路，默认值为 30 秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔（以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF 快速呼叫数据包是指按照小于 1 秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 [OSPF 呼叫间隔和停顿间隔，第 3 页](#)。

通过使用 `ospf dead-interval` 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 `hello-multiplier` 值设置为在该 1 秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为 1 秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF 快速呼叫数据包功能的优势是 OSPF 网络将比没有快速呼叫数据包的情况更快收敛。通过此功能，您可以在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 按链路进行协议处理。
- 删除寻址语义。
- 添加泛洪范围。

- 支持每条链路多个实例。
- 使用 IPv6 链路本地地址执行网络发现和其他功能。
- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 准则

情景模式准则

OSPFv2 支持单情景模式和多情景模式。

- 由于默认情况下不支持跨共享接口的情景间组播流量交换，因此 OSPFv2 实例不能跨共享接口相互建立邻接关系。但是，您可以使用 OSPFv2 进程下 OSPFv2 进程配置中的静态邻居配置，在共享接口上建立 OSPFv2 邻居关系。
- 支持单独的接口上的情景间 OSPFv2。

OSPFv3 仅支持单情景模式。

密钥链身份验证准则

OSPFv2 同时在物理和虚拟模式下支持单一和多模式下的密钥链身份验证。但是，在多模式下，仅可在情景模式下配置密钥链。

- 轮换密钥仅适用于 OSPFv2 协议。不支持密钥链的 OSPF 区域身份验证。
- 但仍支持 OSPFv2 中无时间范围的现有 MD5 身份验证以及新的轮换密钥。
- 尽管平台支持 SHA1 和 MD5 加密算法，但只有 MD5 加密算法会用于身份验证。

防火墙模式准则

OSPF 仅支持路由防火墙模式。OSPF 不支持透明防火墙模式。

故障转移 准则

OSPFv2 和 OSPFv3 支持状态 故障转移。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。

- OSPFv3 使用 IPv6 进行身份验证。
- ASA 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。
- 可以在 `capture` 命令中使用 IPv6 ACL 滤除 OSPFv3 数据包。

OSPFv3 Hello 数据包和 GRE

通常，OSPF 流量不会通过 GRE 隧道。当 IPv6 上的 OSPFv3 封装在 GRE 内时，安全检查（例如组播目标）的 IPv6 报头验证失败。由于隐式安全检查验证，数据包被丢弃，因为此数据包具有目标 IPv6 组播。

您可以定义预过滤器规则来绕过 GRE 流量。但是，使用预过滤器规则，检测引擎不会询问内部数据包。

集群准则

- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式下，仅管理接口上不支持动态路由。
- 在单个接口模式下，确保已作为 OSPFv2 或 OSPFv3 邻居建立控制和数据单元。
- 在单个接口模式下，只能在控制单元共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 当集群中的控制角色发生变化时，会发生以下行为：
 - 在跨接口模式中，路由器进程仅在控制单元上处于活动状态，在数据单元上处于暂停状态。各集群设备具有同一路由器 ID，因为已从控制单元对配置进行同步。因此，在角色更改过程中，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
 - 在单个接口模式中，路由器进程在所有单个集群设备上都处于活动状态。各集群设备从已配置的集群池中选择其自己独特的路由器 ID。集群中的控制角色更改不会以任何方式更改路由拓扑。

多协议标签交换 (MPLS) 和 OSPF 准则

如果 MPLS 配置的路由器发送的链路状态 (LS) 更新数据包包含不透明 Type-10 链路状态通告 (LSA)，而且其中包括 MPLS 报头，则身份验证会失败且设备会自动丢弃更新数据包，而不是确认它们。最终，对等路由器将终止邻居关系，因为它没有收到任何确认。

禁用 ASA 上的不透明功能，以确保邻居关系保持稳定：

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

路由重分布准则

- 不支持在 OSPFv2 或 OSPFv3 上重新分发具有 IPv4 或 IPv6 前缀列表的路由映射。使用 OSPF 上的连接路由进行重新分发。

- 在属于 EIGRP 网络的设备上配置 OSPF 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 尚不支持路由标记）。

将 OSPF 重新分发到 EIGRP 并将 EIGRP 重新分发到 OSPF 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。
- 可分发的区域内（类型 1）路由数具有限制。对于这些路由，单一 1 类 LSA 包含所有前缀。由于系统的数据包大小限制为 35 KB，所以 3000 个路由会导致数据包超出该限制。考虑设置 2900 个 1 类路由作为支持的最大数量。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 由于 Azure 云路由的性质，ASA Virtual 无法使用 EIGRP、OSPF 等动态内部路由协议。无论虚拟客户端是否配置了任何静态/动态路由，有效路由表都会确定下一跳。

目前，您无法查看有效路由表或系统路由表。

配置 OSPFv2

此部分介绍如何在 ASA 上启用 OSPFv2 进程。

启用 OSPFv2 后，您需要定义路由映射。有关详细信息，请参阅[定义路由映射](#)。然后，生成默认路由。有关详细信息，请参阅[配置静态路由](#)。

为 OSPFv2 进程定义路由映射后，您可以根据特定需要对其进行自定义。要了解任何在 ASA 上自定义 OSPFv2 进程，请参阅[自定义 OSPFv2](#)，第 10 页。

要启用 OSPFv2，您需要创建 OSPFv2 路由进程，指定与该路由进程关联的 IP 地址的范围，然后指定与 IP 地址范围关联的区域 ID。

您最多可以启用两个 OSPFv2 进程实例。每个 OSPFv2 进程具有其自己的关联区域和网络。

要启用 OSPFv2，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

在 OSPF Setup 窗格中，您可以启用 OSPF 进程，配置 OSPF 区域和网络，以及定义 OSPF 路由汇总。

步骤 2 ASDM 中用于启用 OSPF 的三个选项卡如下：

- 通过 Process Instances 选项卡，您最多可以为每个情景启用两个 OSPF 进程实例。单情景模式和多情景模式均受支持。选中 **Enable Each OSPF Process** 复选框后，可以为该 OSPF 进程输入唯一数字标识符。此进程 ID 在内部使用，并且无需与任何其他 OSPF 设备上的 OSPF 进程 ID 匹配；有效值范围为 1 至 65535。每个 OSPF 进程具有其自己的关联区域和网络。

如果点击“高级”，系统将显示“编辑 OSPF 进程高级属性”对话框。从此处，您可以配置每个 OSPF 进程的 Router ID、Spanned EtherChannel 或 Individual Interface 集群中的集群 IP 地址池、Adjacency Changes、Administrative Route Distances、Timers 和 Default Information Originate 设置。。

- 通过 Area/Networks 选项卡，您可以显示其为 ASA 上的各 OSPF 进程包含的区域和网络。从此选项卡可以显示区域 ID、区域类型和为区域设置的身份验证类型。要添加或编辑 OSPF 区域或网络，请参阅[配置 OSPFv2 区域参数](#)，第 16 页以获取详细信息。
- 通过 Route Summarization 选项卡，您可以配置 ABR。在 OSPF 中，ABR 会将一个区域中的网络通告到另一个区域中。如果您以某种方式分配区域中的网络号来使其连续，则可以将 ABR 配置为通告汇总路由，包括该区域内属于指定范围的所有单独网络。有关详细信息，请参阅[配置 OSPFv2 区域之间的路由汇总](#)，第 13 页。

配置身份验证所用的密钥链

为了增强设备的数据安全和防护，你可以启用 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

本节介绍如何为 OSPF 对等体身份验证创建密钥链。本节还介绍添加或编辑密钥链属性的步骤。配置密钥链对象后，您可以将其用于定义接口和虚拟链路的 OSPFv2 身份验证。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID，以建立成功的邻接关系。要了解如何为接口定义身份验证，请参阅[配置 OSPFv2 接口参数](#)，第 14 页；有关虚拟链路的信息，请参阅[在 OSPF 中配置虚拟链路](#)，第 25 页。

要配置密钥链，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 密钥链。

步骤 2 在配置部分，点击添加。

步骤 3 在添加密钥链对话框中输入密钥链名称，然后点击 Ok。

创建的密钥链名称在 **Configure Key Chain** 中列出。

步骤 4 从 **Configure Key Chain** 部分中选择密钥链名称，然后在 **Configure Key** 部分中，点击 **Add**。要编辑现有密钥，请选择密钥名称并点击 **Edit**。

系统将显示 **Add Key** 或 **Edit Key** 对话框，具体取决于您选择执行哪一项操作。

步骤 5 在密钥 ID 字段中指定密钥标识符。

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

注释 无法编辑已保存的密钥 ID。

步骤 6 从“加密算法”下拉列表中，选择 **MD5**。MD5 是唯一支持对密钥链进行身份验证的算法。

步骤 7 通过点击 **Plain Text** 或 **Encrypted** 单选按钮选择加密类型，然后在 **Authentication Key** 字段中输入密码。

- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

步骤 8 在 **Accept Lifetime** 和 **Send Lifetime** 字段中提供生命周期值：

您可以指定设备在与其他设备交换密钥期间接受/发送密钥的时间间隔。结束时间可为持续时间，即接受/发送生命周期结束时的绝对时间，也可以是永不到期。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于结束生存期。

步骤 9 要保存密钥链样式，请点击 **Ok**。在 **Key Chain** 页面中，点击 **Apply**。

下一步做什么

现在，您可以应用配置的密钥链来定义接口和虚拟链路的 OSPFv2 身份验证。

- [配置 OSPFv2 接口参数，第 14 页](#)
- [在 OSPF 中配置虚拟链路，第 25 页](#)

配置 OSPFv2 路由器 ID

OSPF Router-ID 用于标识 OSPF 数据库中的特定设备。在 OSPF 系统中，任何两个路由器都不能具有相同的 `router-id`。

如果未在 OSPF 路由进程中手动配置 `router-id`，路由器将自动配置从主用接口中的最高 IP 地址确定的 `router-id`。在配置 `router-id` 时，将不会自动更新邻居，直至路由器出现故障或 OSPF 进程已被清除并且已重新建立邻居关系。

手动配置 OSPF 路由器 ID

本节介绍如何在 ASA 上手动配置 OSPFv2 进程中的 `router-id`。

过程

步骤 1 要使用固定路由器 ID，请使用 `router-id` 命令。

`router-id ip-address`

示例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

步骤 2 要恢复到以前的 OSPF 路由器 ID 行为，请使用 `no router-id` 命令。

`no router-id ip-address`

示例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

迁移时的路由器 ID 行为

在从一个 ASA（譬如 ASA 1）向另一个 ASA（譬如 ASA 2）迁移开放式最短路径优先配置（OSPF 配置）时，可以观察到以下路由器 id 选择行为：

1. 当所有接口都处于关闭模式时，ASA 2 不将任何 IP 地址用于 OSPF `router-id`。当所有接口都处于“管理关闭”状态或关闭模式时，配置 `router-id` 可能出现的情况如下：

- 如果 ASA 2 之前没有配置任何 `router-id`，您将看到以下消息：

```
%OSPF: 路由器进程 1 未在运行，请配置一个 router-id
```

在第一个接口启用后，ASA 2 会将此接口的 IP 地址作为路由器 id。

- 如果 ASA 2 之前已配置 `router-id`，并且所有接口在发出“no router-id”命令时都处于“管理关闭”状态，那么 ASA 2 将使用旧的路由器 id。即使启用的接口上的 IP 地址发生了更改，ASA 2 仍会使用旧的路由器 id，直至发出“clear ospf process”命令为止。
2. 如果 ASA 2 之前已配置 `router-id`，并且在发出“no router-id”命令时至少有一个接口未处于“管理关闭”状态或关闭模式，则 ASA 2 将使用新的路由器 id。即使接口处于“关闭/关闭”状态，ASA 2 也会使用这些接口的 IP 地址作为新的路由器 id。

自定义 OSPFv2

本节介绍如何自定义 OSPFv2 进程。

将路由重新分发到 OSPFv2 中

ASA 可以控制路由在 OSPFv2 路由进程之间的重新分发。



注释 如果要通过定义允许将来自指定路由协议的哪些路由重新分发到目标路由进程中来重新分发路由，必须先生成默认路由。请参阅[配置静态路由](#)，然后根据[定义路由映射](#)定义路由映射。

要将静态路由、已连接路由、RIP 路由或 OSPFv2 路由重新分发到 OSPFv2 进程中，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 重新分发。

Redistribution 窗格显示用于将路由从一个路由进程重新分发到 OSPF 路由进程中的规则。您可以将 RIP 和 OSPF 发现的路由重新分布到 EIGRP 路由过程中。您还可以将静态路由和已连接路由重新分布到 EIGRP 路由过程中。如果静态路由或已连接路由属于已通过 Setup > Networks 选项卡配置的网络范围，则无需重新分发这些路由。

步骤 2 点击 **Add** 或 **Edit**。

或者，双击 Redistribution 窗格中的表条目（如有）将为所选条目打开 Add/Edit OSPF Redistribution Entry 复选框。

注释 后面所有步骤都是可选的。

通过 Add/Edit OSPF Redistribution Entry 对话框，您可以在 Redistribution 表中添加新的重新分发规则或编辑现有重新分发规则。编辑现有重新分发规则时，无法更改某些重新分发规则信息。

步骤 3 选择与路由重新分发条目关联的 OSPF 进程。如果编辑的是现有重新分发规则，则无法更改此设置。

步骤 4 选择根据其重新分发路由的源协议。您可以选择以下其中一个选项：

- **Static** - 将静态路由重新分发到 OSPF 路由进程。
- **Connected** - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 OSPF 路由进程。已连接路由重新分发为 AS 的外部路由。
- **OSPF** - 从另一个 OSPF 路由进程重新分发路由。从列表中选择 OSPF 进程 ID。如果选择此协议，则此对话框中的 **Match** 选项变为可见。当重新分发静态、已连接、RIP 或 EIGRP 路由时，这些选项不可用。请跳至步骤 5。
- **RIP** - 从 RIP 路由进程重新分发路由。
- **BGP** - 从 BGP 路由进程重新分发路由。
- **EIGRP** - 从 EIGRP 路由进程重新分发路由。从列表中选择 EIGRP 路由进程的自治系统编号。

步骤 5 如果已为源协议选择 OSPF，请选择用于将路由从另一个 OSPF 路由进程重新分配到所选 OSPF 路由进程中的条件。当重新分发静态、已连接、RIP 或 EIGRP 路由时，这些选项不可用。路由必须与要重新分发的所选条件相匹配。您可以选择以下一个或多个匹配条件：

- **Internal** - 该路由必须是特定 AS 的内部路由。
- **External 1** - 对于自治系统而言属于外部的路由，但是会作为 1 类外部路由导入 OSPF。
- **External 2** - 对于自治系统而言属于外部的路由，但是会作为 2 类外部路由导入 OSPF。
- **NSSA External 1** - 对于自治系统而言属于外部的路由，但是会作为 2 类 NSSA 路由导入 OSPF。
- **NSSA External 2** - 对于自治系统而言属于外部的路由，但是会作为 2 类 NSSA 路由导入 OSPF。

步骤 6 在 **指标值** 字段中，输入进行重新分发的路由的指标值。有效值范围为 1 到 16777214。

在同一设备上从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定指标值，则默认指标为 20。

步骤 7 为 **Metric Type** 选择以下其中一个选项。

- 如果指标是 1 类外部路由，请选择 **1**。
- 如果指标是 2 类外部路由，请选择 **2**。

步骤 8 在 **Tag Value** 字段中输入标签值。

标签值是附加到 OSPF 本身未使用但可用于在 ASBR 之间传达信息的各外部路由的 32 位十进制值。有效值范围为 0 到 4294967295。

步骤 9 选中 **Use Subnets** 复选框以启用于子网路由的重新分发。取消选中此复选框会导致仅重新分发未划分子网的路由。

步骤 10 从 **Route Map** 下拉列表中选择要应用于重新分发条目的路由映射的名称。

步骤 11 如果需要添加或配置路由映射，请点击 **Manage**。

系统将显示 **Configure Route Map** 对话框。

步骤 12 点击 **Add** 或 **Edit** 以定义允许将来自指定路由协议的哪些路由重新分发到目标路由进程中。有关详细信息，请参阅[定义路由映射](#)。

步骤 13 点击确定 (**OK**)。

配置将路由重新分发到 OSPFv2 时的路由汇总

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。不过，可以将 ASA 配置为对于指定网络地址和掩码包含的所有重新分发路由通告单一路由。此配置可减小 OSPF 链路状态数据库的大小。

可以抑制与指定 IP 地址/掩码相匹配的路由。标签值可用于作用于通过路由映射控制重新分发的值。

添加路由汇总地址

“汇总地址”窗格显示有关为每个 OSPF 路由进程配置的汇总地址的信息。

可以汇总从其他路由协议获知的路由。用于通告汇总的指标是所有较为具体路由的最小指标。汇总路由帮助减小路由表的大小。

对 OSPF 使用汇总路由会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。只能汇总重新分发到 OSPF 中的来自其他路由协议的路由。



注释 OSPF 不支持汇总地址 0.0.0.0 0.0.0.0。

要在一个汇总路由上配置适用于为网络地址和掩码包含的所有重新分发的路由的软件通告，请执行以下步骤：

过程

步骤 1 在主 ASDM 主页中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 汇总地址。

步骤 2 点击添加 (**Add**)。

系统将显示 Add OSPF Summary Address Entry 对话框。您可以向 Summary Address 表中的现有条目添加新条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3 从 OSPF Process 下拉列表中选择与汇总地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4 在 IP 地址字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5 从 Netmask 下拉列表中选择汇总地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6 选中 **Advertise** 复选框以通告汇总路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

标签值显示附加到各外部路由的 32 位十进制值。OSPF 本身未使用此值，但是其可能用于在 ASBR 之间传达信息。

步骤 7 点击确定 (OK)。

添加或编辑 OSPF 汇总地址

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Route Summarization** 选项卡。

系统将显示 Add/Edit a Route Summarization Entry 对话框。

通过 Add/Edit a Route Summarization Entry 对话框，您可以在 Summary Address 表中添加新条目或修改现有条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3 从 **OSPF Process** 下拉列表中选择与汇总地址关联的指定 OSPF 进程 ID。编辑现有条目时，无法更改此信息。

步骤 4 在 **IP 地址** 字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

步骤 5 从 **Netmask** 下拉列表中输入汇总地址的网络掩码。编辑现有条目时，无法更改此信息。

步骤 6 选中 **Advertise** 复选框以通告汇总路由。取消选中此复选框以抑制属于汇总地址的路由。默认情况下，此复选框为选中状态。

配置 OSPFv2 区域之间的路由汇总

路由汇总是通告地址的整合。此功能导致通过区域边界路由器向其他区域通告单个汇总路由。在 OSPF 中，区域边界路由器将一个区域中的网络通告到另一个区域中。如果以某种方式分配区域中的网络号来使其连续，则可以将区域边界配置为通告汇总路由，包括该区域内属于指定范围的所有单独网络。

要定义汇总路由的地址范围，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Route Summarization** 选项卡。

系统将显示 Add/Edit a Route Summarization Entry 对话框。

通过 Add/Edit a Route Summarization Entry 对话框，您可以在 Summary Address 表中添加新条目或修改现有条目。编辑现有条目时，无法更改某些汇总地址信息。

步骤 3 在 **Area ID** 字段中输入 OSPF 区域 ID。编辑现有条目时，无法更改此信息。

步骤 4 在 IP 地址字段中输入汇总地址的 IP 地址。编辑现有条目时，无法更改此信息。

配置 OSPFv2 接口参数

如有必要，您可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：呼叫间隔、停顿间隔和身份验证密钥。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

在 ASDM 中，通过 **Interface** 窗格可以配置特定于接口的 OSPF 路由属性，例如 OSPF 消息验证和属性。有两个选项卡可帮助配置 OSPF 中的接口：

- “Authentication” 选项卡显示 ASA 接口的 OSPF 身份验证信息。
- Properties 选项卡以表格式显示为每个接口定义的 OSPF 属性。

要配置 OSPFv2 接口参数，请执行以下步骤：

过程

步骤 1 点击 **Authentication** 选项卡以显示 ASA 接口的身份验证信息。双击表中的行以打开所选接口的 Edit OSPF Authentication Interface 对话框。

步骤 2 点击 **Edit**。

系统将显示“编辑 OSPF 身份验证接口”对话框。通过 Edit OSPF Authentication Interface 对话框，您可以配置所选接口的 OSPF 身份验证类型和参数。

步骤 3 通过点击相关单选按钮选择身份验证类型：

- **No authentication**，表示禁用 OSPF 身份验证。
- **Area authentication, if defined**（默认），表示使用为区域指定的身份验证类型。有关配置区域身份验证的信息，请参阅[配置 OSPFv2 区域参数](#)，第 16 页。默认情况下，区域身份验证已禁用。因此，除非先前已指定区域身份验证类型，否则设置为使用区域身份验证的接口会禁用身份验证，直到配置此设置为止。
- **Password authentication**，表示使用明文密码身份验证（在有安全问题的情况下不建议使用）。
- **MD5 身份验证**以使用 MD5 身份验证。
- **密钥链身份验证**以使用密钥链身份验证（推荐）。请参阅[配置身份验证所用的密钥链](#)，第 7 页，了解有关配置用于进行身份验证的密钥链的信息。

步骤 4 如果选择的是密码身份验证，在 **Authentication Password** 区域中输入密码：

- a) 在 Enter Password 字段中，键入最多八个字符的文本字符串。
- b) 在 Re-enter Password 字段中，再次键入密码。

步骤 5 如果已选择密钥链身份验证，请在输入密钥链名称字段中输入密钥链名称。

步骤 6 在 ID 字段中输入 MD5 ID 和密钥的设置，其中包括对于在启用 MD5 身份验证时输入 MD5 密钥和参数的设置。接口上所有使用 OSPF 身份验证的设备都必须使用同一 MD5 密钥和 ID。

- a) 在 Key ID 字段中，输入数字密钥标识符。有效值范围为 1 到 255。系统将显示所选接口的密钥 ID。
- b) 在 Key 字段中，输入最多 16 字节的字母数字字符串。系统将显示所选接口的密钥。
- c) 点击 **Add** 或 **Delete** 以在 MD5 ID 和 Key 表中添加或删除指定的 MD5 密钥。

步骤 7 点击 **OK**。

步骤 8 点击 **Properties** 选项卡。

步骤 9 选择要编辑的接口。双击表中的行以打开所选接口的“Properties”选项卡对话框。

步骤 10 点击 **Edit**。

系统将显示“编辑 OSPF 接口属性”对话框。接口字段显示正在为其配置 OSPF 属性的接口的名称。您无法编辑此字段。

步骤 11 选中或取消选中“广播”复选框以指定接口是广播接口。

默认情况下，对于以太网接口会选中此复选框。取消选中此复选框以将接口指定为点对点非广播接口。将接口指定为点对点非广播可以通过 VPN 隧道传输 OSPF 路由。

当接口配置为点对点非广播时，以下限制适用：

- 只能为接口定义一个邻居。
- 需要手动配置邻居。有关详情，请参见[定义静态 OSPFv2 邻居](#)，第 21 页。
- 您无需定义指向加密终端的静态路由。有关详情，请参见[配置静态路由](#)。
- 如果通过隧道执行的 OSPF 是在接口上运行，则上游路由器的常规 OSPF 不能在同一接口上运行。
- 在指定 OSPF 邻居之前应将加密映射绑定到接口，以确保通过 VPN 隧道传递 OSPF 更新。如果在指定 OSPF 邻居之后将加密映射绑定到接口，请使用 **clear local-host all** 命令清除 OSPF 连接，以便可以通过 VPN 隧道建立 OSPF 邻接。

步骤 12 配置以下选项：

- 在 Cost 字段中输入值，该值确定通过接口发送数据包的开销。默认值为 10。
- 在 Priority 字段中，输入 OSPF 路由器优先级值。

当两个路由器连接到网络时，两者均尝试成为指定路由器。具有更高路由器优先级的设备成为指定路由器。如果有绑定，则具有更高路由器 ID 的路由器成为指定路由器。

此设置的有效值范围为 0 至 255。默认值为 1。为此设置输入 0 将使路由器不符合成为指定路由器或备用指定路由器的条件。此设置不适用于配置为点对点非广播接口的接口。

在多情景模式下，对于共享接口，请指定 0 以确保设备不会成为指定路由器。OSPFv2 实例无法跨共享接口相互建立邻接关系。

- 选中或取消选中 **MTU Ignore** 复选框。

OSPF 检查邻居在公用接口上是否使用的是同一 MTU。在邻居交换 DBD 数据包时会执行此检查。如果 DBD 数据包中的接收 MTU 高于传入接口上配置的 IP MTU，将不建立 OSPF 邻接。

- 选中或取消选中 **Database filter** 复选框。

使用此设置在同步和泛洪过程中筛选传出 LSA 接口。默认情况下，OSPF 会在同一区域中的所有接口上泛洪新 LSA，但 LSA 到达的接口除外。在全网拓扑中，此泛洪可能会浪费带宽并产生过多的链路和 CPU 使用情况。选中此复选框可防止 OSPF 在所选接口上进行 LSA 泛洪。

步骤 13 （可选）点击“高级”以显示“编辑 OSPF 高级接口属性”对话框，通过其可以更改 OSPF 呼叫间隔、重新传输间隔、传输延迟和停顿间隔的值。

通常，仅在网络上遇到 OSPF 问题的情况下才需要根据默认值更改这些值。

步骤 14 在 Intervals 部分中，输入以下各项的值：

- “呼叫间隔”，它指定在接口上发送的呼叫数据包之间的间隔（以秒为单位）。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。有效值的范围为 1 到 8192 秒。默认值为 10 秒。
- “重传间隔”，它指定属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。当路由器向其邻居发送 LSA 时，它会保留 LSA，直到其接收到确认消息为止。如果路由器没有接收到确认，则将重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。有效值的范围为 1 到 8192 秒。默认值为 5 秒。
- “传输延迟”，它指定在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。有效值的范围为 1 到 8192 秒。默认值为 1 秒。

步骤 15 在 Detecting Lost Neighbors 部分中，执行以下其中一项操作：

- 点击“Configure interval within which hello packets are not received before the router declares the neighbor to be down”。在 Dead Interval 字段中，指定在其期间未接收到呼叫数据包而导致邻居声明路由器关闭的时间间隔（以秒为单位）。有效值的范围为 1 到 8192 秒。此设置的默认值是 Hello Interval 字段中设置的间隔的四倍。
- 点击“Send fast hello packets within 1 seconds dead interval”。在 Hello multiplier 字段中，指定每秒要发送的呼叫数据包的数量。有效值介于 3 和 20 之间。

配置 OSPFv2 区域参数

您可以配置多个 OSPF 区域参数。这些区域参数（显示在以下任务列表中）包括设置身份验证、定义末节区域以及向默认汇总路由分配特定开销。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Area/Networks** 选项卡。

系统将显示 Add OSPF Area 对话框。

步骤 3 选择以下其中一个“区域类型”选项：

- **Normal**，用于使该区域成为标准 OSPF 区域。首次创建区域时，默认情况下会选择此选项。
- **Stub**，用于使该区域成为末节区域。末节区域外没有任何路由器或区域。末节区域防止 AS 外部 LSA（5 类 LSA）泛洪至末节区域中。创建末节区域时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA（3 类和 4 类）泛洪至该区域中。
- **Summary**，用于防止将 LSA 发送到末节区域中，当所定义的区域是末节区域时，请取消选中此复选框。默认情况下，对于末节区域会选中此复选框。
- **NSSA**，用于使区域成为次末节区域。NSSA 接受 7 类 LSA。创建 NSSA 时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA 泛洪至该区域中。您也可以通过取消选中 Redistribute 复选框并选中 Default Information Originate 复选框来禁用路由重新分发。

步骤 4 在 IP Address 字段中输入要添加到区域中的网络或主机的 IP 地址。将 **0.0.0.0** 与子网掩码 **0.0.0.0** 配合使用以创建默认区域。您只能在一个区域中输入 **0.0.0.0**。

步骤 5 在 Network Mask 字段中输入要添加到区域中的 IP 地址或主机的网络掩码。如果添加的是主机，请选择 **255.255.255.255** 掩码。

步骤 6 从以下选项中选择 OSPF 身份验证类型：

- **None**，表示禁用 OSPF 区域身份验证。这是默认设置。
- **Password**，表示提供明文密码进行区域身份验证，在有安全问题的情况下不建议使用。
- **MD5**，表示允许 MD5 身份验证。

步骤 7 在 Default Cost 字段中输入值以指定 OSPF 区域的默认开销。

有效值范围为 0 到 65535。默认值为 1。

步骤 8 点击**确定 (OK)**。

配置 OSPFv2 过滤器规则

使用以下程序可过滤 OSPF 更新中接收或传输的路由或网络。

过程

-
- 步骤 1** 依次选择配置 > 设备设置 > 路由 > OSPF > 筛选器规则。
- 步骤 2** 点击添加。
- 步骤 3** 在 **OSPF AS** 中选择 OSPF 进程 ID。
- 步骤 4** 从 Access List 下拉列表选择一个标准访问列表。点击 **Manage** 以添加新的 ACL。
- 步骤 5** 从 Direction 下拉列表中选择方向。此方向将指定过滤器应用于入站更新还是出站更新。
- 步骤 6** 对于入站过滤器，可以选择性地指定某个接口来限制用于该接口上收到的更新的过滤器。
- 步骤 7** 对于出站过滤器，您可以选择性地指定分发的路由类型。
- a) 从 Protocol 下拉列表选择一个选项。

您可以选择路由协议，例如 **BGP**、**EIGRP**、**OSPF** 或 **RIP**。

选择 **Connected** 可对通过已连接路由获知的对等体和网络进行过滤。

选择 **Static** 可对通过静态路由获知的对等体和网络进行过滤。
 - b) 如果选择 BGP、EIGRP 或 OSPF，请选择该协议的 **Process ID**。
- 步骤 8** 点击确定。
- 步骤 9** 点击应用。
-

配置 OSPFv2 NSSA

NSSA 的 OSPFv2 实施类似于 OSPFv2 末节区域。NSSA 不会将 5 类外部 LSA 从核心泛洪至该区域中，但是可在区域内以有限的方法导入自治系统外部路由。

NSSA 通过重新分发在 NSSA 区域内导入 7 类自治系统外部路由。这些 7 类 LSA 由 NSSA ABR 转换为在整个路由域中泛洪的 5 类 LSA。在转换过程中支持汇总和筛选。

如果您是必须将使用 OSPFv2 的中心站点连接到对 NSSA 使用其他路由协议的远程站点的 ISP 或网络管理员，则可以简化管理。

在 NSSA 实施前，企业站点边界路由器和远程路由器之间的连接不能作为 OSPFv2 末节区域运行，因为远程站点的路由无法重新分发到末节区域中，并且需要保持两种路由协议。通常会运行简单协议（例如 RIP）并使用其处理重新分发。在使用 NSSA 的情况下，您可以通过将企业路由器和远程路由器之间的区域定义为 NSSA 来将 OSPFv2 扩展至覆盖远程连接。

使用此功能之前，请遵循以下准则：

- 您可以设置用于到达外部目标的 7 类默认路由。配置时，路由器会生成到 NSSA 或 NSSA 区域边界路由器中的 7 类默认路由。
- 同一区域内的每个路由器都必须同意区域为 NSSA；否则，路由器无法相互通信。

过程

步骤 1 在主 ASDM 主页中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Area/Networks** 选项卡。

步骤 3 点击 **Add**。

系统将显示 Add OSPF Area 对话框。

步骤 4 点击 Area Type 区域中的 **NSSA** 单选按钮。

选择此选项以使该区域成为次末节区域。NSSA 接受 7 类 LSA。创建 NSSA 时，可以通过取消选中 Summary 复选框来选择防止汇总 LSA 泛洪至该区域中。您也可以通过取消选中 Redistribute 复选框并选中 Default Information Originate 复选框来禁用路由重新分发。

步骤 5 在 IP Address 字段中输入要添加到区域中的网络或主机的 IP 地址。将 **0.0.0.0** 与子网掩码 **0.0.0.0** 配合使用以创建默认区域。您只能在一个区域中输入 **0.0.0.0**。

步骤 6 在 Network Mask 字段中输入要添加到区域中的 IP 地址或主机的网络掩码。如果添加的是主机，请选择 **255.255.255.255** 掩码。

步骤 7 在 Authentication 区域中，点击 **None** 单选按钮以禁用 OSPF 区域身份验证。

步骤 8 在 Default Cost 字段中输入值以指定 OSPF 区域的默认开销。

有效值范围为 0 到 65535。默认值为 1。

步骤 9 点击 **确定 (OK)**。

为集群配置 IP 地址池（OSPFv2 和 OSPFv3）

如果使用的是单个接口集群，则可以为路由器 ID 集群池分配 IPv4 地址范围。

要为 OSPFv2 的单个接口中的路由器 ID 集群池分配 IPv4 地址范围，请执行以下步骤：

过程

步骤 1 在主 ASDM 主页中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4 点击 **Cluster Pool** 单选按钮。如果使用的是集群，则无需指定路由器 ID 的 IP 地址池（即，将字段留空）。如果不输入 IP 地址池，则 ASA 使用自动生成的路由器 ID。

步骤 5 输入 IP 地址池的名称，或者点击省略号以显示 Select IP Address Pool 对话框。

步骤 6 双击现有 IP 地址池名称以将其添加到 Assign 字段中。或者，点击 **Add** 以创建新 IP 地址池。

系统将显示 Add IPv4 Pool 对话框。

步骤 7 在 **Name** 字段中输入新 IP 地址池名称。

步骤 8 输入开始 IP 地址，或者点击或省略号以显示 **Browse Starting IP Address** 对话框。

步骤 9 双击某个条目以将其添加到 **Starting IP Address** 字段中，然后点击 **OK**。

步骤 10 输入结束 IP 地址，或者点击或省略号以显示“**Browse Ending IP Address**”对话框

步骤 11 双击某个条目以将其添加到 **Ending IP Address** 字段中，然后点击 **OK**

步骤 12 从下拉列表中选择子网掩码，然后点击 **OK**。

在 **Select IP Address Pool** 列表中将显示新 IP 地址池。

步骤 13 双击新 IP 地址池名称以将其添加到 **Assign** 字段中，然后点击 **OK**。

在 **Edit OSPF Process Advanced Properties** 对话框的 **Cluster Pool** 字段中将显示新 IP 地址池名称。

步骤 14 点击 **OK**。

步骤 15 如果要更改新添加的 IP 地址池设置，请点击 **Edit**。

系统将显示 **Edit IPv4 Pool** 对话框。

步骤 16 重复步骤 4 至步骤 14。

注释 无法编辑或删除已分配和已经在由一个或多个连接配置文件使用的现有 IP 地址池。

步骤 17 点击 **OK**。

步骤 18 要为 OSPFv3 的单个接口集群中的路由器 ID 集群池分配 IPv4 地址范围，请执行以下步骤：

a) 在主 ASDM 主页中，依次选择 **配置 > 设备设置 > 路由 > OSPFv3 > 设置**。

b) 点击 **Process Instances** 选项卡。

c) 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 **Edit OSPFv3 Process Advanced Properties** 对话框。

d) 从“**路由器 ID**”下拉列表选择“**集群池**”选项。如果无需指定路由器 ID 的 IP 地址池，请选择 **Automatic** 选项。如果不配置 IP 地址池，则 ASA 使用自动生成的路由器 ID。

e) 输入 IP 地址池名称。或者，点击省略号以显示 **Select IP Address Pool** 对话框。

f) 双击现有 IP 地址池名称以将其添加到 **Assign** 字段中。或者，点击 **Add** 以创建新 IP 地址池。

系统将显示 **Add IPv4 Pool** 对话框。

g) 在 **Name** 字段中输入新 IP 地址池名称。

h) 输入开始 IP 地址，或者点击或省略号以显示 **Browse Starting IP Address** 对话框。

i) 双击某个条目以将其添加到 **Starting IP Address** 字段中，然后点击 **OK**。

j) 输入结束 IP 地址，或者点击或省略号以显示 **Browse Ending IP Address** 对话框。

k) 双击某个条目以将其添加到 **Ending IP Address** 字段中，然后点击 **OK**。

l) 从下拉列表中选择子网掩码，然后点击 **OK**。

在 **Select IP Address Pool** 列表中将显示新 IP 地址池。

m) 双击新 IP 地址池名称以将其添加到 **Assign** 字段中，然后点击 **OK**。

在 **Edit OSPF Process Advanced Properties** 对话框的 **Cluster Pool** 字段中将显示新 IP 地址池名称。

- n) 点击 **OK**。
- o) 如果要更改新添加的集群池设置，请点击 **Edit**。
系统将显示 Edit IPv4 Pool 对话框。
- p) 重复步骤 4 至步骤 14。
注释 无法编辑或删除已分配和已经在由其他 OSPFv3 进程使用的现有 IP 地址池。
- q) 点击**确定 (OK)**。

定义静态 OSPFv2 邻居

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv2 邻居的静态路由。有关创建静态路由的详细信息，请参阅[配置静态路由](#)。

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 静态邻居。

步骤 2 点击添加 (**Add**)或编辑 (**Edit**)。

系统将显示“添加/编辑 OSPF 邻居条目”对话框。通过此对话框，您可以定义新静态邻居或更改现有静态邻居的信息。您必须为每个点对点非广播接口定义静态邻居。请注意以下限制：

- 不能为两个不同的 OSPF 进程定义相同的静态邻居。
- 需要为每个静态邻居定义静态路由。

步骤 3 从 OSPF Process 下拉列表中，选择与静态邻居关联的 OSPF 进程。如果编辑的是现有静态邻居，则无法更改该值。

步骤 4 在 **Neighbor** 字段中，输入静态邻居的 IP 地址。

步骤 5 在 **Interface** 字段中，选择与静态邻居关联的接口。如果编辑的是现有静态邻居，则无法更改该值。

步骤 6 点击**确定 (OK)**。

配置路由计算计时器

您可以配置 OSPFv2 接收拓扑更改时与其启动 SPF 计算时之间的延迟时间。您还可以配置两次连续 SPF 计算之间的保持时间。

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4 通过 Timers 区域，您可以修改用于配置 LSA 步调计时器和 SPF 计算计时器的设置。在 Timers 区域中，输入以下值：

- **Initial SPF Delay**，指定 OSPF 接收拓扑更改时和 SPF 计算启动时间间隔的时间（以毫秒为单位）。有效值的范围为 0 到 600000 秒。
- **Minimum SPF Hold Time**，指定连续 SPF 计算之间的保持时间（以毫秒为单位）。有效值范围为 0 至 600000 毫秒。
- **Maximum SPF Wait Time**，指定两次连续 SPF 计算间隔的最长等待时间。有效值的范围为 0 到 600000 秒。

步骤 5 点击确定 (OK)。

记录邻居启动或关闭

默认情况下，在 OSPFv2 邻居启动或关闭时会生成系统日志消息。

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > OSPF > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 点击 **Advanced**。

系统将显示 Edit OSPF Process Advanced Properties 对话框。

步骤 4 Adjacency Changes 区域包含用于定义导致发送系统日志消息的邻接更改的设置。在 Adjacency Changes 区域中，输入以下值：

- 选中 **记录邻接更改** 复选框，以使 ASA 只要 OSPFv2 邻居启动或关闭便发送系统日志消息。默认情况下，此设置处于选中状态。
- 选中 **记录邻接更改详细信息** 复选框，以使 ASA 只要发生任何状态更改便发送系统日志消息，而不只是在邻居启动或关闭时发送系统日志消息。默认情况下，此设置处于未选中状态。

步骤 5 点击 **OK**。

注释 必须启用日志记录才能发送邻居启动或关闭消息。

配置身份验证所用的密钥链

为了增强设备的数据安全和防护，你可以启用 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

本节介绍如何为 OSPF 对等体身份验证创建密钥链。本节还介绍添加或编辑密钥链属性的步骤。配置密钥链对象后，您可以将其用于定义接口和虚拟链路的 OSPFv2 身份验证。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID，以建立成功的邻接关系。要了解如何为接口定义身份验证，请参阅 [配置 OSPFv2 接口参数，第 14 页](#)；有关虚拟链路的信息，请参阅 [在 OSPF 中配置虚拟链路，第 25 页](#)。

要配置密钥链，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 密钥链。

步骤 2 在配置部分，点击添加。

步骤 3 在添加密钥链对话框中输入密钥链名称，然后点击 Ok。

创建的密钥链名称在 **Configure Key Chain** 中列出。

步骤 4 从 **Configure Key Chain** 部分中选择密钥链名称，然后在 **Configure Key** 部分中，点击 **Add**。要编辑现有密钥，请选择密钥名称并点击 **Edit**。

系统将显示 **Add Key** 或 **Edit Key** 对话框，具体取决于您选择执行哪一项操作。

步骤 5 在密钥 ID 字段中指定密钥标识符。

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

注释 无法编辑已保存的密钥 ID。

步骤 6 从“加密算法”下拉列表中，选择 **MD5**。MD5 是唯一支持对密钥链进行身份验证的算法。

步骤 7 通过点击 **Plain Text** 或 **Encrypted** 单选按钮选择加密类型，然后在 **Authentication Key** 字段中输入密码。

- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

步骤 8 在 **Accept Lifetime** 和 **Send Lifetime** 字段中提供生命周期值：

您可以指定设备在与其他设备交换密钥期间接受/发送密钥的时间间隔。结束时间可为持续时间，即接受/发送生命周期结束时的绝对时间，也可以是永不到期。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于结束生存期。

步骤 9 要保存密钥链样式，请点击 **Ok**。在 **Key Chain** 页面中，点击 **Apply**。

下一步做什么

现在，您可以应用配置的密钥链来定义接口和虚拟链路的 OSPFv2 身份验证。

- [配置 OSPFv2 接口参数，第 14 页](#)
- [在 OSPF 中配置虚拟链路，第 25 页](#)

在 OSPF 中配置过滤

“筛选”窗格显示已为每个 OSPF 进程配置的 ABR 3 类 LSA 筛选器。

ABR 3 类 LSA 过滤器仅允许将指定的前缀从一个区域发送到另一个区域，并会限制其他所有前缀。此类型的区域筛选可以应用在特定 OSPF 区域外、应用到特定 OSPF 区域中，或者同时在相同 OSPF 区域的内外进行应用。

OSPF ABR 3 类 LSA 筛选可提高对 OSPF 区域之间路由重新分发的控制。



注释 系统仅筛选源于 ABR 的 3 类 LSA。

要在 OSPF 中配置筛选，请执行以下步骤：

过程

步骤 1 在主 ASDM 窗口中，依次选择 **配置 > 设备设置 > 路由 > OSPF > 筛选**。

步骤 2 点击 **Add** 或 **Edit**。

通过 **Add/Edit OSPF Filtering Entry** 对话框，您可以向过滤器表中添加新过滤器或修改现有过滤器。编辑现有过滤器时，某些筛选信息无法更改。

步骤 3 从 **OSPF Process** 下拉列表中选择与过滤器条目相关联的 OSPF 进程。

步骤 4 从 **Area ID** 下拉列表中选择与过滤器条目关联的区域 ID。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 5 从 Prefix List 下拉列表中选择前缀列表。

步骤 6 从 Traffic Direction 下拉列表中选择筛选的流量方向。

选择 Inbound 以筛选传入 OSPF 区域的 LSA，或者选择 Outbound 以筛选传出 OSPF 区域的 LSA。如果编辑的是现有过滤器条目，则无法修改此设置。

步骤 7 点击 **Manage** 以显示 Configure Prefix Lists 对话框，您可以从中添加、编辑或删除前缀列表和规则前缀。有关详细信息，请参阅[配置前缀列表](#)和[为路由操作配置度量值](#)。

步骤 8 点击**确定 (OK)**。

在 OSPF 中配置虚拟链路

如果将区域添加到 OSPF 网络，并且无法将该区域直接连接到主干区域，则需要创建虚拟链路。虚拟链路连接具有公共区域（称为中转区域）的两台 OSPF 设备。其中一台 OSPF 设备必须连接到主干区域。

如要定义新虚拟链路或更改现有虚拟链路的属性，请执行以下步骤：

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 虚拟链路。

步骤 2 点击 **Add** 或 **Edit**。

系统将显示 Add/Edit OSPF Virtual Link 对话框，通过其可以定义新虚拟链路或更改现有虚拟链路的属性。

步骤 3 从 OSPF Process 下拉列表中选择与虚拟链路关联的 OSPF 进程 ID。如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 4 从 Area ID 下拉列表中选择与虚拟链路关联的区域 ID。

选择 OSPF 邻居设备共享的区域。所选区域不能是 NSSA 区域或末节区域。如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 5 在 **Peer Router ID** 字段中，输入虚拟链路邻居的路由器 ID。

如果编辑的是现有虚拟链路条目，则无法修改此设置。

步骤 6 点击 **Advanced** 以编辑高级虚拟链路属性。

系统将显示 Advanced OSPF Virtual Link Properties 对话框。您可以在此区域中配置虚拟链路的 OSPF 属性。这些属性包括身份验证和数据包间隔设置。

步骤 7 在 Authentication 区域中，通过点击以下其中一个选项旁边的单选按钮来选择身份验证类型：

- **No authentication**，表示禁用 OSPF 身份验证。
- **Password authentication**，表示使用明文密码身份验证（在有安全问题的情况下不建议使用）。

- **MD5 身份验证**以使用 MD5 身份验证。
- **密钥链身份验证**以使用密钥链身份验证（推荐）。请参阅 [配置身份验证所用的密钥链](#)，第 7 页，了解有关配置用于进行身份验证的密钥链的信息。

步骤 8 在 Authentication Password 区域中，启用密码身份验证后输入并重新输入密码。密码必须是最多 8 个字符的文本字符串。

步骤 9 在 MD5 IDs and Key 区域中，启用 MD5 身份验证后输入 MD5 密钥和参数。接口上所有使用 OSPF 身份验证的设备都必须使用同一 MD5 密钥和 ID。指定以下设置：

- a) 在 **Key ID** 字段中，输入数字密钥标识符。有效值范围为 1 到 255。系统将显示所选接口的密钥 ID。
- b) 在 **Key** 字段中，输入最多 16 字节的字母数字字符串。系统将显示所选接口的密钥 ID。
- c) 点击 **Add** 或 **Delete** 以在 MD5 ID 和 Key 表中添加或删除指定的 MD5 密钥。

步骤 10 在 Interval 区域中，通过从以下选项中选择来指定数据包的间隔时间：

- **Hello Interval**，用于指定在接口上发送的呼叫数据包之间的间隔（以秒为单位）。呼叫间隔越小，检测到拓扑更改的速度越快，但会在接口上发送更多流量。此值对于特定接口上的所有路由器和接入服务器都必须相同。有效值的范围为 1 到 65535 秒。默认值为 10 秒。
- **Retransmit Interval**，用于指定属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。当路由器向其邻居发送 LSA 时，它会保留 LSA，直到其接收到确认消息为止。如果路由器没有接收到确认，则将重新发送 LSA。请保守地设置此值，否则可能会产生不必要的重新传输。串行线路和虚拟链路的值应较大。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- **Transmit Delay**，用于指定在接口上发送 LSA 数据包所需的估计时间（以秒为单位）。更新数据包中的 LSA 在传输之前会按此字段指定的量增大其年龄。如果在通过链路进行传输之前未添加延迟，则不考虑 LSA 通过该链路进行传播的时间。分配的值应将接口的传输和传播延迟考虑在内。此设置对于超低速链路意义更大。有效值的范围为 1 到 65535 秒。默认值为 1 秒。
- **Dead Interval**，用于指定在其期间未接收到呼叫数据包而导致邻居声明路由器关闭的间隔（以秒为单位）。有效值范围为 1 到 65535。此字段的默认值是 Hello Interval 字段设置的间隔的四倍。

步骤 11 点击确定 (OK)。

配置 OSPFv3

本节介绍配置 OSPFv3 路由进程所涉及的任务。

启用 OSPFv3

要启用 OSPFv3，您需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

过程

- 步骤 1** 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > OSPFv3 > 设置。
- 步骤 2** 在 Process Instances 选项卡上，选中 **Enable OSPFv3 Process** 复选框。您最多可以启用两个 OSPF 进程实例。仅支持单情景模式。
- 步骤 3** 在 Process ID 字段中输入进程 ID。ID 可以是任何正整数。
- 步骤 4** 点击 **Apply** 保存更改。
- 步骤 5** 要继续，请参阅配置 OSPFv3 区域参数，第 28 页。

配置 OSPFv3 接口参数

如有必要，您可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：**hello-interval** 和 **dead-interval**。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

过程

- 步骤 1** 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > OSPFv3 > 接口。
- 步骤 2** 点击 **Authentication** 选项卡。
- 步骤 3** 要指定接口的身份验证参数，请选择该接口并点击“编辑”。系统将显示编辑 OSPFv3 接口身份验证对话框。
- 步骤 4** 从身份验证类型下拉列表中选择身份验证类型。可用选项为 Area、Interface 和 None。None 选项表示未使用身份验证。
- 步骤 5** 从 **Authentication Algorithm** 下拉列表中选择身份验证算法。支持的值为 SHA-1 和 MD5。
- 步骤 6** 在 **Authentication Key** 字段中输入身份验证密钥。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
- 步骤 7** 从 **Encryption Algorithm** 下拉列表中选择加密算法。支持的值为 AES-CDC、3DES 和 DES。NULL 条目表示不加密。
- 步骤 8** 在 **Encryption Key** 字段中输入加密密钥。
- 步骤 9** 点击 **OK**。
- 步骤 10** 点击 **Properties** 选项卡。
- 步骤 11** 选择要修改其属性的接口，然后点击 **Edit**。系统将显示 Edit OSPFv3 Interface Properties 对话框。
- 步骤 12** 选中 **Enable OSPFv3 on this interface** 复选框。
- 步骤 13** 从下拉列表中选择进程 ID。
- 步骤 14** 从下拉列表中选择区域 ID。

- 步骤 15** (可选) 指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。您可以在多个接口上使用同一区域, 并且每个接口可以使用不同的区域实例 ID。
- 步骤 16** 从下拉列表中选择网络类型。支持的选项为 Default、Broadcast 和 Point-to-Point。
- 步骤 17** 在 Cost 字段中输入在接口上发送数据包的开销。
- 步骤 18** 在 Priority 字段中输入用于帮助确定网络的指定路由器的路由器优先级。有效值范围为 0 到 255。
- 步骤 19** 收到 DBD 数据包后, 选中 **Disable MTU mismatch detection** 复选框以禁用 OSPF MTU 不匹配检测。默认情况下, OSPF MTU 不匹配检测已启用。
- 步骤 20** 选中 **Filter outgoing link state advertisements** 复选框以筛选到 OSPFv3 接口的传出 LSA。默认情况下, 所有传出 LSA 都泛洪至该接口。
- 步骤 21** 选中 **OSPF 泛洪减少** 复选框, 以减少不必要的 LSA 泛洪和刷新接口。
- 步骤 22** 在 Timers 区域中的 **Dead Interval** 字段内, 输入在邻居表明路由器关闭之前不得查看呼叫数据包的时间段 (以秒为单位)。该值必须对于同一网络上的所有节点都相同, 并且范围可以是 1 至 65535。
- 步骤 23** 在呼叫间隔字段中, 输入接口上发送的呼叫数据包之间的间隔 (以秒为单位)。该值必须对于特定网络上的所有节点都相同, 并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒, 对于非广播接口为 30 秒。
- 步骤 24** 在 **重新传输间隔** 字段中, 输入属于接口的邻接的 LSA 重新传输的间隔时间 (以秒为单位)。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
- 步骤 25** 在 **传输延迟** 字段中, 输入在接口上发送链路状态更新数据包所需的估计时间 (以秒为单位)。有效值的范围为 1 到 65535 秒。默认值为 1 秒。
- 步骤 26** 点击 **OK**。
- 步骤 27** 点击 **Apply** 保存更改。

配置 OSPFv3 区域参数

过程

- 步骤 1** 在 ASDM 主窗口中, 依次选择配置 > 设备设置 > 路由 > OSPFv3 > 设置。
- 步骤 2** 点击区域 (Areas) 选项卡。
- 步骤 3** 要添加新区域, 请点击添加 (Add)。要修改现有区域, 请点击编辑 (Edit)。要删除所选区域, 请点击删除 (Delete)。
- 系统将显示“添加 OSPFv3 区域”对话框或“编辑 OSPFv3 区域”对话框。
- 步骤 4** 从 OSPFv3 Process ID 下拉列表中, 选择进程 ID。
- 步骤 5** 在 Area ID 字段中输入区域 ID, 它指定要为其汇总路由的区域。
- 步骤 6** 从 Area Type 下拉列表中选择区域类型。可用选项为 Normal、NSSA 和 Stub。
- 步骤 7** 要允许将汇总 LSA 发送到区域中, 请选中 **Allow sending of summary LSAs into the area** 复选框。

- 步骤 8** 要允许重新分发以将路由导入到普通区域和次末节区域，请选中 **Redistribution imports routes to normal and NSSA areas** 复选框。
- 步骤 9** 要生成到 OSPFv3 路由域中的默认外部路由，请选中 **Default information originate** 复选框。
- 步骤 10** 在 Metric 字段中输入用于生成默认路由的指标。默认值为 10。有效十进制值范围为 0 到 16777214。
- 步骤 11** 从 Metric Type 下拉列表中选择指标类型。指标类型是与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。可用选项为 1（表示 1 类外部路由）或 2（表示 2 类外部路由）。
- 步骤 12** 在 Default Cost 字段中输入开销。
- 步骤 13** 点击**确定 (OK)**。
- 步骤 14** 点击路由汇总 (**Route Summarization**) 选项卡。
- 步骤 15** 要指定整合与汇总路由的新范围，请点击**添加 (Add)**。要修改整合与汇总路由的现有范围，请点击**编辑 (Edit)**。
系统将显示“添加路由汇总”对话框或“编辑路由汇总”对话框。
- 步骤 16** 从 Process ID 下拉列表中选择进程 ID。
- 步骤 17** 从 Area ID 下拉列表中选择区域 ID。
- 步骤 18** 在 IPv6 Prefix/Prefix Length 字段中输入 IPv6 前缀和前缀长度。
- 步骤 19** （可选）输入汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。有效值范围为 0 到 16777215。
- 步骤 20** 选中 **Advertised** 复选框以将地址范围状态设置为已通告并生成 3 类汇总 LSA。
- 步骤 21** 点击**确定 (OK)**。
- 步骤 22** 要继续，请参阅[配置虚拟链路邻居，第 29 页](#)。

配置虚拟链路邻居

要配置虚拟链路邻居，请执行以下步骤：

过程

- 步骤 1** 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 虚拟链路。
- 步骤 2** 要添加新虚拟链路邻居，请点击**添加 (Add)**。要修改现有虚拟链路邻居，请点击**编辑 (Edit)**。要删除所选虚拟链路邻居，请点击**删除 (Delete)**。
系统将显示“添加虚拟链路”对话框或“编辑虚拟链路”对话框。
- 步骤 3** 从 Process ID 下拉列表中选择进程 ID。
- 步骤 4** 从 Area ID 下拉列表中选择区域 ID。
- 步骤 5** 在 Peer Router ID 字段中输入对等路由器 ID（即 IP 地址）。
- 步骤 6** （可选）在 TTL Security 字段中输入虚拟链路上的生存时间 (TTL) 安全跃点计数。跃点计数值范围可以为 1 至 254。

- 步骤 7** 在 Timers 区域中的 **Dead Interval** 字段内输入在邻居表明路由器关闭之前看不到呼叫数据包的时间（以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍（或 40 秒）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 8192。
- 步骤 8** 在 **Hello Interval** 字段中输入接口上发送的呼叫数据包的间隔时间（以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 8192。默认值为 10。
- 步骤 9** 在 **Retransmit Interval** 字段中输入属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 8192。默认值为 5。
- 步骤 10** 在 **Transmit Delay** 字段中输入在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。整数必须大于零。更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。值的范围可以从 1 至 8192。默认值为 1。
- 步骤 11** 在 **Authentication** 区域中，选中 **Enable Authentication** 复选框以启用身份验证。
- 步骤 12** 在 **Security Policy Index** 字段中输入安全策略索引，它必须是从 256 至 4294967295 的数字。
- 步骤 13** 从 **Authentication Algorithm** 下拉列表中选择身份验证算法。支持的值为 SHA-1 和 MD5。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
- 步骤 14** 在 **Authentication Key** 字段中输入身份验证密钥。密钥必须包含 32 个十六进制字符。
- 步骤 15** 从 **Encryption Algorithm** 下拉列表中选择加密算法。支持的值为 AES-CDC、3DES 和 DES。NULL 条目表示不加密。
- 步骤 16** 在 **Encryption Key** 字段中输入加密密钥。
- 步骤 17** 点击 **OK**。
- 步骤 18** 点击 **Apply** 保存更改。

配置 OSPFv3 被动接口

过程

- 步骤 1** 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > OSPFv3 > 设置。
- 步骤 2** 点击 **Process Instances** 选项卡。
- 步骤 3** 选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。
- 系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。
- 步骤 4** 通过 **Passive Interfaces** 区域，您可以在接口上启用备用 OSPFv3 路由。备用路由帮助控制 OSPFv3 路由信息的通告并禁用接口上发送和接收 OSPFv3 路由更新。在 **Passive Interfaces** 区域中，选择以下设置：
- 选中 **Global passive** 复选框以使表中列出的所有接口都成为被动接口。取消选中单个接口以使其成为非被动接口。

- 取消选中 **Global passive** 复选框以使所有接口都成为非被动接口。选中单个接口以使其成为被动接口。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply** 保存更改。

配置 OSPFv3 管理距离

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

通过 Administrative Route Distances 区域，您可以修改用于配置管理路由距离的设置。管理路由距离是从 10 至 254 的整数。在 Administrative Route Distances 区域中，输入以下值：

- Inter Area，用于指定 OSPF 的区域间路由作为 IPv6 路由。
- Intra Area，用于指定 OSPF 的区域内路由作为 IPv6 路由。
- External，用于指定 OSPF 的外部 5 类和 7 类路由作为 IPv6 路由。

步骤 4 点击 **OK**。

步骤 5 点击 **Apply** 保存更改。

配置 OSPFv3 计时器

您可以为 OSPFv3 设置 LSA 到达计时器、LSA 步调设置计时器和调速计时器。

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4 通过 Timers 区域，您可以修改用于配置 LSA 到达时间、LSA 步调设置时间、LSA 重新传输时间、LSA 调速时间和 SPF 调速时间的设置。在 Timers 区域中，输入以下值：

- **LSA Arrival**，用于指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围是从 0 到 6000,000 毫秒。默认值为 1000 毫秒。
- **LSA Flood Pacing**，用于指定在前后两次更新之间泛洪队列中的 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。
- **LSA Group Pacing**，用于指定将 LSA 收集到组中并刷新、校验和或老化的间隔（以秒为单位）。有效值范围为 10 到 1800。默认值为 240。
- **LSA Retransmission Pacing**，用于指定重新传输队列中 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。
- **LSA Throttle Initial**，用于指定生成 LSA 的第一次出现所需的延迟（以毫秒为单位）。默认值为 0 毫秒。
- **LSA Throttle Min Hold**，用于指定发起同一 LSA 所需的最小延迟（以毫秒为单位）。默认值为 5000 毫秒。
- **LSA Throttle Max Wait**，用于指定发起同一 LSA 所需的最大延迟（以毫秒为单位）。默认值为 5000 毫秒。

注释 对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

- **SPF Throttle Initial**，用于指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。默认值为 5000 毫秒。
- **SPF Throttle Min Hold**，用于指定第一次和第二次 SPF 计算之间的延迟（以毫秒为单位）。默认值为 10000 毫秒。
- **SPF Throttle Max Wait**，用于指定 SPF 计算最长等待时间（以毫秒为单位）。默认值为 10000 毫秒。

注释 对于 SPF 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply** 保存更改。

定义静态 OSPFv3 邻居

您需要定义静态 OSPFv3 邻居来通过点对点非广播网络通告 OSPF 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv3 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv3 邻居的静态路由。有关创建静态路由的详细信息，请参阅[配置静态路由](#)。

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > OSPFv3 > 静态邻居。

步骤 2 点击添加 (**Add**)或编辑 (**Edit**)。

系统将显示“添加/编辑静态邻居”对话框。通过此对话框，您可以定义新静态邻居或更改现有静态邻居的信息。您必须为每个点对点非广播接口定义静态邻居。请注意以下限制：

- 不能为两个不同的 OSPFv3 进程定义相同的静态邻居。
- 需要为每个静态邻居定义静态路由。

步骤 3 从 Interface 下拉列表中，选择与静态邻居关联的接口。如果要编辑的是现有静态邻居，则无法更改该值。

步骤 4 在 Link-local Address 字段中，输入静态邻居的 IPv6 地址。

步骤 5 （可选）在 Priority 字段中，输入优先级。

步骤 6 （可选）在 Poll Interval 字段中，输入轮询间隔（以秒为单位）。

步骤 7 点击确定 (**OK**)。

发送系统日志消息

将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息。

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > OSPFv3 > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

通过 Adjacency Changes 区域，您可以修改在 OSPFv3 邻居启动或关闭时发送系统日志消息的设置。在 Adjacency Changes 区域中，执行以下操作：

- 要在 OSPFv3 邻居启动或关闭时发送系统日志消息，请选中 **Log Adjacency Changes** 复选框。
- 要为每个状态发送系统日志消息，而不只是在 OSPFv3 邻居启动或关闭时才发送系统日志消息，请选中 **Include Details** 复选框。

步骤 4 点击 **OK**。

步骤 5 点击 **Apply** 保存更改。

抑制系统日志消息

要在路由器接收不受支持的 LSA 6 类多播 OSPF (MOSPF) 数据包时抑制发送系统日志消息，请执行以下步骤：

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4 选中 **Ignore LSA MOSPF** 复选框，然后点击 **OK**。

计算汇总路由成本

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPF 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4 选中 **RFC1583 Compatible** 复选框，然后点击 **OK**。

生成到 OSPFv3 路由域中的默认外部路由

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 点击 **Process Instances** 选项卡。

步骤 3 选择要编辑的 OSPFv3 进程，然后点击 **Advanced**。

系统将显示 Edit OSPFv3 Process Advanced Properties 对话框。

步骤 4 在 Default Information Originate Area 中，执行以下操作：

a) 选中 **Enable** 复选框以启用 OSPFv3 路由进程。

- b) 选中 **Always advertise** 复选框以始终通告默认路由（无论其是否存在）。
- c) 在 **Metric** 字段中输入用于生成默认路由的指标。有效十进制值范围为 0 到 16777214。默认值为 10。
- d) 从 **Metric Type** 下拉列表中，选择与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值包括以下值：
 - 1 - 1 类外部路由
 - 2 - 2 类外部路由默认为 2 类外部路由。
- e) 从 **Route Map** 下拉列表中，选择在满足路由的情况下生成默认路由的路由进程。

步骤 5 点击 **OK**。

步骤 6 点击 **Apply** 保存更改。

配置 IPv6 汇总前缀

过程

步骤 1 在 ASDM 主窗口中，依次选择 **配置 > 设备设置 > 路由 > OSPFv3 > 汇总前缀**。

步骤 2 要添加新汇总前缀，请点击 **Add**。要修改现有汇总前缀，请点击 **Edit**。要删除汇总前缀，请点击 **Delete**。

系统将显示“添加汇总前缀”对话框或“编辑汇总前缀”对话框。

步骤 3 从 **Process ID** 下拉列表中选择进程 ID。

步骤 4 在 **IPv6 Prefix/Prefix Length** 字段中输入 IPv6 前缀和前缀长度。

步骤 5 选中 **Advertise** 复选框以通告与指定前缀/掩码相匹配的路由。取消选中此复选框以抑制与指定前缀/掩码相匹配的路由。

步骤 6 在 **Tag** 字段中输入可用作通过路由映射控制重新分发的匹配值的标签值。

步骤 7 点击 **OK**。

步骤 8 点击 **Apply** 保存更改。

重新分发 IPv6 路由

过程

步骤 1 在 ASDM 主窗口中，依次选择 **配置 > 设备设置 > 路由 > OSPFv3 > 重新分发**。

- 步骤 2** 要添加用于将已连接路由重新分发到 OSPFv3 进程中的新参数，请点击 **Add**。要修改用于将已连接路由重新分发到 OSPFv3 进程中的现有参数，请点击 **Edit**。要删除所选参数集，请点击“删除”。系统将显示“添加重新分发”对话框或“编辑重新分发”对话框。
- 步骤 3** 从 Process ID 下拉列表中选择进程 ID。
- 步骤 4** 从 Source Protocol 下拉列表中选择从其重新分发路由的源协议。支持的协议为 **connected**、**static** 和 **OSPF**。
- 步骤 5** 在 Metric 字段中输入指标值。在同一路由器上将路由从一个 OSPF 进程重新分发到另一个 OSPF 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定指标值，则默认指标为 20。
- 步骤 6** 从 Metric Type 下拉列表中选择指标类型。可用选项为 **None**、**1** 和 **2**。
- 步骤 7** （可选）在 Tag 字段中输入标签值。此参数指定连接到每个外部路由的 32 位十进制值，该值可用于在 ASBR 之间传达信息。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值为 0 到 4294967295。
- 步骤 8** 从 Route Map 下拉列表中选择路由映射来检查对从源路由协议到当前路由协议的路由的导入的筛选。如果未指定此参数，则会重新分发所有路由。如果已指定此参数，但未列出路由映射标签，则不会导入任何路由。
- 步骤 9** 要在重新分发中包含已连接路由，请选中 **Include connected** 复选框。
- 步骤 10** 选中 **Match** 复选框以将路由重新分发到其他路由域中，然后选中以下其中一个复选框：
- **Internal**，表示特定自治系统的内部路由
 - **External 1**，表示自治系统的外部路由，但会作为 1 类外部路由导入 OSPFv3
 - **External 2**，表示自治系统的外部路由，但会作为 2 类外部路由导入 OSPFv3
 - **NSSA External 1**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类外部路由导入到 OSPFv3 中
 - **NSSA External 2**，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 2 类外部路由导入到 OSPFv3 中
- 步骤 11** 点击 **OK**。
- 步骤 12** 点击 **Apply** 保存更改。

配置无中断重启

ASA 可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。

在高可用性模式下，当主用设备变为非主用设备且备用设备成为新的主用设备时，OSPF 进程会重新启动。同样，在集群模式下，当控制设备变为非活动状态且数据设备被选为新的控制设备时，OSPF 进程会重新启动。此类 OSPF 转换过程涉及相当长的延迟。您可以配置 NSF 以避免在 OSPF 进程状态更改期间丢失流量。当有计划的无中断软件升级时，NSF 功能也非常有用。

在 OSPFv2 和 OSPFv3 上均支持平稳重启。通过使用 NSF Cisco (RFC 4811 和 RFC 4812) 或 NSF IETF (RFC 3623), 您可以在 OSPFv2 上配置平稳重启。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

配置 NSF 平稳重启功能涉及两个步骤: 配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持 NSF 功能的设备可以向邻居表明其自己的重启活动, 而支持 NSF 感知的设备可以帮助重新启动邻居。

根据某些条件, 可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备:

- 设备可以配置为 NSF 感知的设备, 而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持 NSF 功能或 NSF 感知, 应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。



注释 如果为 OSPFv2 配置了快速呼叫, 则在主用设备重新加载且备用设备激活时不会发生平稳重启。这是因为角色更改所需的时间超过配置的停顿间隔。

为 OSPFv2 配置无中断重启

对于 OSPFv2、思科 NSF 和 IETF NSF, 存在两种平稳重启机制。一次只能为 ospf 实例配置其中一种平稳重启机制。支持 NSF 感知的设备既可以配置为思科 NSF 助手, 也可以配置为 IETF NSF 助手, 但是一次只能在思科 NSF 或 IETF NSF 模式中为 ospf 实例配置支持 NSF 功能的设备。

为 OSPFv2 配置思科 NSF 无中断重启

为 OSPFv2 配置思科 NSF 平稳重启 (适用于支持 NSF 功能的设备或 NSF 感知的设备)。

过程

- 步骤 1** 在 ASDM 主窗口中, 依次选择 Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties。
- 步骤 2** 在 Configuring Cisco NSF 下, 选中 Enable Cisco nonstop forwarding (NSF) 复选框。
- 步骤 3** (可选) 选中 Cancels NSF restart when non-NSF-aware neighboring networking devices are detected 复选框 (如果需要)。
- 步骤 4** (可选) 在 Configuring Cisco NSF helper 下, 取消选中 Enable Cisco nonstop forwarding (NSF) for helper mode 复选框。

注释 默认情况下, 此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用思科 NSF 助手模式。

步骤 5 点击确定 (OK)。

步骤 6 点击应用 (Apply) 保存更改。

为 OSPFv2 配置 IETF NSF 无中断重启

为 OSPFv2 配置思科 IETF NSF 平稳重启（支持 NSF 功能的设备或 NSF 感知的设备）。

过程

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties**。

步骤 2 在“Configuring IETF NSF”下，选中“Enable IETF nonstop forwarding (NSF)”复选框。

步骤 3 （可选）在 Length of graceful restart interval 字段中输入重启间隔。

注释 默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 4 （可选）在“Configuring IETF NSF helper”下，取消选中“Enable IETF nonstop forwarding (NSF) for helper mode”复选框。

默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用 IETF NSF 助手模式。

步骤 5 点击 OK。

步骤 6 点击 Apply 保存更改。

为 OSPFv3 配置无中断重启

为 OSPFv3 配置 NSF 平稳重启功能涉及两个步骤：将一个设备配置为支持 NSF 功能，然后将另一个设备配置为支持 NSF 感知。

过程

步骤 1 在 ASDM 主窗口中，依次选择 **Configuration > Device Setup > Routing > OSPFv3 > Setup > Advanced > Add NSF Properties**。

步骤 2 在 Configuring Graceful Restart 下，选中 Enable Graceful Restart 复选框。

步骤 3 （可选）在 Restart Interval 字段中输入重启间隔值。

注释 默认值为 120 秒。对于低于 30 秒的重启间隔，将终止平稳重启。

步骤 4 在 Configuring Graceful Restart Helper 下，选中 Enable Graceful Restart Helper 复选框。

默认情况下，此复选框处于选中状态。取消选中此复选框将在支持 NSF 感知的设备上禁用平稳重启助手模式。

步骤 5 （可选）选中 **Enable LSA checking** 复选框以启用严格链路状态通告检查。

启用后，它指示助手路由器在以下情况下将终止重新启动路由器的过程：它检测到 LSA 发生会泛洪至重新启动的路由器的更改，或者在发起平稳重启过程时重新启动的路由器的重新传输列表上有已更改的 LSA。

步骤 6 点击 **OK**。

步骤 7 点击 **Apply** 保存更改。

为 OSPF 配置无中断重新启动等待计时器

如果 OSPF 路由器不知道所有邻居是否在数据包中列出，并且重新启动路由器需要保留邻接关系，但它们会在连接到 Hello 数据包的 EO 中设置 RS 位。但是，RS 位值不能超过 RouterDeadInterval 秒。因此，引入 **timers nsf wait** 命令，以将呼叫数据包中的 RS 位设置为小于 RouterDeadInterval 秒。NSF 等待计时器默认值为 20 秒。

开始之前

- 要为 OSPF 配置思科 NSF 等待时间，设备必须支持 NSF 或 NSF 功能。

过程

步骤 1 进入 OSPF 路由器配置模式。

示例：

```
ciscoasa(config)# router ospf
```

步骤 2 输入计时器并指定 nsf。

示例：

```
ciscoasa(config-router)# timers?  
router mode commands/options:  
  lsa      OSPF LSA timers  
  nsf      OSPF NSF timer  
  pacing   OSPF pacing timers  
  throttle OSPF throttle timers  
ciscoasa(config-router)# timers nsf ?
```

步骤 3 输入平稳重启等待间隔。此值的范围为 1 到 65535。

示例：

```
ciscoasa(config-router)# timers nsf wait 200
```

通过使用平稳重启等待间隔，可以确保等待间隔不超过路由器失效间隔。

删除 OSPFv2 配置

删除 OSPFv2 配置。

过程

步骤 1 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 设置。

步骤 2 取消选中 **Enable this OSPF Process** 复选框。

步骤 3 点击应用。

删除 OSPFv3 配置

删除 OSPFv3 配置。

过程

步骤 1 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。

步骤 2 取消选中 **Enable OSPFv3 Process** 复选框。

步骤 3 点击应用。

OSPFv2 示例

以下示例显示如何使用各种可选进程启用和配置 OSPFv2:

1. 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 设置。
2. 点击流程实例 (**Process Instances**) 选项卡，并在“OSPF 流程 1” (OSPF Process 1) 字段中键入 2。
3. 点击区域/网络 (**Area/Networks**) 选项卡，然后点击添加 (**Add**)。
4. 在 Area ID 字段中输入 0。
5. 在 Area Networks 区域中的 IP Address 字段内输入 10.0.0.0。
6. 从 Netmask 下拉列表中选择 255.0.0.0。
7. 点击确定 (**OK**)。
8. 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 重新分发。
9. 点击添加 (**Add**)。

系统将显示 Add/Edit OSPF Redistribution Entry 对话框。

10. 在“协议”(Protocol)区域中, 点击 **OSPF** 单选按钮以选择从其重新分发路由的源协议。选择 OSPF 将从其他 OSPF 路由进程重新分发路由。
11. 从 OSPF Process 下拉列表中选择 OSPF 进程 ID。
12. 在 Match 区域中, 选中 **Internal** 复选框。
13. 在 Metric Value 字段中, 输入 **5** 作为进行重新分发的路由的指标值。
14. 从 Metric Type 下拉列表中, 选择 1 作为 Metric Type 值。
15. 从 Route Map 下拉列表中, 选择 1。
16. 点击确定 (OK)。
17. 在 ASDM 主窗口中, 依次选择配置 > 设备设置 > 路由 > **OSPF** > 接口。
18. 从“属性”(Properties)选项卡中, 选择 **inside** 接口, 然后点击编辑 (Edit)。
系统将显示 Edit OSPF Properties 对话框。
19. 在 Cost 字段中, 输入 **20**。
20. 点击高级 (Advanced)。
21. 在 Retransmit Interval 字段中, 输入 **15**。
22. 在 Transmit Delay 字段中, 输入 **20**。
23. 在 Hello Interval 字段中, 输入 **10**。
24. 在 Dead Interval 字段中, 输入 **40**。
25. 点击确定 (OK)。
26. 在“编辑 OSPF 属性”(Edit OSPF Properties)对话框中的“属性”(Priorities)字段内输入 **20**, 然后点击确定 (OK)。
27. 点击身份验证 (Authentication) 选项卡。
系统将显示 Edit OSPF Authentication 对话框。
28. 在“身份验证”(Authentication)区域中, 点击 **MD5** 单选按钮。
29. 在 MD5 and Key ID 区域中, 在 MD5 Key 字段内输入 **cisco**, 在 MD5 Key ID 字段内输入 **1**。
30. 点击确定 (OK)。
31. 依次选择配置 (Configuration) > 设备设置 (Device Setup) > 路由 (Routing) > **OSPF** > 设置 (Setup), 并点击区域/网络 (Area/Networks) 选项卡。
32. 选择 **OSPF 2** 进程, 然后点击编辑 (Edit)。
系统将显示 Edit OSPF Area 对话框。
33. 在 Area Type 区域中, 选择 **Stub**。

34. 在 Authentication 区域中，选择 **None**，然后在 Default Cost 字段中输入 **20**。
35. 点击确定 (**OK**)。
36. 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > **OSPF** > 设置。
37. 点击流程实例 (**Process Instances**) 选项卡，然后选中 **OSPF 流程 2 (OSPF process 2)** 复选框。
38. 点击高级 (**Advanced**)。
系统将显示 Edit OSPF Area 对话框。
39. 在 Timers 区域中，在 SPF Delay Time 字段内输入 **10**，在 SPF Hold Time 字段内输入 **20**。
40. 在 Adjacency Changes 区域中，选中 **Log Adjacency Change Details** 复选框。
41. 点击确定 (**OK**)。
42. 点击重置 (**Reset**)。

OSPFv3 示例

以下示例显示如何在 ASDM 中配置 OSPFv3 路由：

1. 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 设置。
2. 在 Process Instances 选项卡上，执行以下操作：
 1. 选中 **Enable OSPFv3 Process** 复选框。
 2. 在 Process ID 字段中输入 **1**。
3. 点击 **Areas** 选项卡，然后点击 **Add** 以显示 Add OSPFv3 Area 对话框。
4. 从 OSPFv3 Process ID 下拉列表中，选择 **1**。
5. 在 Area ID 字段中输入 **22**。
6. 从 Area Type 下拉列表中选择 **Normal**。
7. 在 Default Cost 字段中输入 **10**。
8. 选中 **Redistribution imports routes to normal and NSSA areas** 复选框。
9. 在 Metric 字段中输入 **20**。
10. 从 Metric Type 下拉列表中选择 **1**。
11. 选中 **inside** 复选框作为使用的指定接口。
12. 选中 **Enable Authentication** 复选框。
13. 在 Security Policy Index 字段中输入 **300**。
14. 从 Authentication Algorithm 下拉列表中选择 **SHA-1**。

15. 在 Authentication Key 字段中输入 **12345ABCDE**。
16. 从 Encryption Algorithm 下拉列表中选择 **DES**。
17. 在 Encryption Key 字段中输入 **1122334455aabbccdde**。
18. 点击 **OK**。
19. 点击 **Route Summarization** 选项卡，然后点击 **Add** 以显示 Add Route Summarization 对话框。
20. 从 Process ID 下拉列表中选择 **1**。
21. 从 Area ID 下拉列表中选择 **22**。
22. 在 IPv6 Prefix/Prefix Length 字段中输入 **2000:122::/64**。
23. （可选）在 Cost 字段中输入 **100**。
24. 选中 **Advertised** 复选框。
25. 点击 **OK**。
26. 在 ASDM 主窗口中，依次选择配置 > 设备设置 > 路由 > **OSPFv3** > 接口。
27. 点击 **Properties** 选项卡。
28. 选中 **inside** 复选框，然后点击 **Edit** 以显示 Edit OSPF Properties 对话框。
29. 在 Cost 字段中，输入 **20**。
30. 在 Priority 字段中输入 **1**。
31. 选中 **point-to-point** 复选框。
32. 在 Dead Interval 字段中，输入 **40**。
33. 在 Hello Interval 字段中，输入 **10**。
34. 在 Retransmit Interval 字段中，输入 **15**。
35. 在 Transmit Delay 字段中，输入 **20**。
36. 点击 **OK**。
37. 在主 ASDM 窗口中，依次选择配置 > 设备设置 > 路由 > 重新分发。
38. 从 Process ID 下拉列表中选择 **1**。
39. 从 Source Protocol 下拉列表中选择 **OSPF**。
40. 在 Metric 字段中输入 **50**。
41. 从 Metric Type 下拉列表中选择 **1**。
42. 点击 **OK**。
43. 点击 **Apply** 保存更改。

监控 OSPF

您可以显示特定统计信息，例如 IP 路由表、缓存和数据库的内容。您还可以使用所提供的信息确定资源利用率和解决网络问题。您也可以显示有关节点可达性的信息并发现设备数据包通过网络所采用的路由路径。

要在 ASDM 中监控或显示各种 OSPFv2 路由统计，请执行以下步骤：

1. 在 ASDM 主窗口中，依次选择**配置 > 路由 > OSPF LSA**。
2. 您可以选择并监控 OSPF LSA，1 类至 5 类和 7 类。每个窗格显示一种 LSA 类型，如下所示：
 - 1 类 LSA 表示进程下区域中的路由。
 - 2 类 LSA 显示通告路由器的指定路由器的 IP 地址。
 - 3 类 LSA 显示目标网络的 IP 地址。
 - 4 类 LSA 显示 AS 边界路由器的 IP 地址。
 - 5 类 LSA 和 7 类 LSA 显示 AS 外部网络的 IP 地址。
3. 点击 **Refresh** 以更新每个 LSA 类型窗格。
4. 在 ASDM 主窗口中，依次选择**配置 > 路由 > OSPF 邻居**。

在 OSPF Neighbors 窗格中，每行表示一个 OSPF 邻居。此外，OSPF Neighbors 窗格还会显示邻居运行所在的网络、优先级、状态、停顿时间量（以秒为单位）、邻居的 IP 地址及其运行所在的接口。有关 OSPF 邻居的可能状态的列表，请参阅 RFC 2328。

5. 点击 **Refresh** 以更新 OSPF Neighbors 窗格。

要在 ASDM 中监控或显示各种 OSPFv3 路由统计，请执行以下步骤：

1. 在 ASDM 主窗口中，依次选择**配置 > 路由 > OSPFv3 LSA**。
2. 您可以选择并监控 OSPFv3 LSA。从 Link State type 下拉列表中选择链路状态类型，以根据指定的参数显示其状态。支持的链路状态类型为 router、network、inter-area prefix、inter-area router、AS external、NSSA、link 和 intra-area prefix。
3. 点击 **Refresh** 以更新每种链路状态类型。
4. 在 ASDM 主窗口中，依次选择**配置 > 路由 > OSPFv3 邻居**。

在 OSPFv3 Neighbors 窗格中，每行表示一个 OSPFv3 邻居。此外，OSPFv3 Neighbors 窗格还会显示邻居的 IP 地址、优先级、状态、停顿时间量（以秒为单位）及其运行所在的接口。有关 OSPFv3 邻居的可能状态的列表，请参阅 RFC 5340。

5. 点击 **Refresh** 以更新 OSPFv3 Neighbors 窗格。

OSPF 历史记录

表 1: OSPF 的功能历史记录

功能名称	平台版本	功能信息
OSPF 支持	7.0(1)	添加了对使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发和监控路由信息的支持。 引入了以下屏幕: Configuration > Device Setup > Routing > OSPF。
多情景模式下的动态路由	9.0(1)	在多情景模式中支持 OSPFv2 路由。 修改了以下屏幕: Configuration > Device Setup > Routing > OSPF > Setup
集群	9.0(1)	对于 OSPFv2 和 OSPFv3, 在集群环境中支持批量同步、路由同步和跨网络 EtherChannel 负载均衡。
OSPFv3 支持 IPv6	9.0(1)	IPv6 支持 OSPFv3 路由。 引入了以下屏幕: Configuration > Device Setup > Routing > OSPFv3 > Setup、Configuration > Device Setup > Routing > OSPFv3 > Interface、Configuration > Device Setup > Routing > OSPFv3 > Redistribution、Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix、Configuration > Device Setup > Routing > OSPFv3 > Virtual Link, Monitoring > Routing > OSPFv3 LSAs、Monitoring > Routing > OSPFv3 Neighbors。
OSPF 支持快速呼叫	9.2(1)	OSPF 支持快速呼叫数据包功能, 从而产生在 OSPF 网络中导致更快收敛的配置。 修改了以下屏幕: Configuration > Device Setup > Routing > OSPF > Interface > Edit OSPF Interface Advanced Properties
计时器	9.2(1)	添加了新 OSPF 计时器; 弃用了旧 OSPF 计时器。 修改了以下屏幕: Configuration > Device Setup > Routing > OSPF > Setup > Edit OSPF Process Advanced Properties
使用访问列表筛选路由	9.2(1)	现在支持使用 ACL 筛选路由。 引入了以下菜单项: 配置 > 设备设置 > 路由 > OSPF > 过滤规则 > 添加过滤规则
OSPF 监控增强功能	9.2(1)	添加了其他 OSPF 监控信息。
OSPF 重新分发 BGP	9.2(1)	添加了 OSPF 重新分发功能。 添加了以下屏幕: Configuration > Device Setup > Routing > OSPF > Redistribution

功能名称	平台版本	功能信息
OSPF 支持不间断转发 (NSF)	9.3(1)	<p>添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。</p> <p>添加了以下屏幕： Configuration > Device Setup > Routing > OSPF > Setup > NSF Properties、 Configuration > Device Setup > Routing > OSPFv3 > Setup > NSF Properties</p>
OSPF 支持不间断转发 (NSF)	9.13(1)	<p>添加了 NSF 等待计时器。</p> <p>添加了一个新命令，用于为 NSF 重新启动间隔设置计时器。引入此命令是为了确保等待间隔不会长于路由器失效间隔。</p> <p>我们引入了以下命令：</p> <p>timers nsf wait<seconds></p>

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。