IS-IS

本章介绍中间系统到中间系统 (IS-IS) 路由协议。

关于 IS-IS

IS-IS 路由协议是一种链路状态内部网关协议 (IGP)。链路状态协议的主要特征是传播在每个参与设备上建立完整网络连接图所需的信息。然后，该连接图会用于计算到达目的地的最短路径。IS-IS 实施支持 IPv4 和 IPv6。

您可以将路由域划分为一个或多个子域。每个子域称为一个区域，并会分配一个区域地址。同一个区域内的路由称为 1 级路由。在 1 级区域之间的路由称为 2 级路由。路由器称为中间系统 (IS)。IS 可以运行在 1 级、2 级或两者。运行在 1 级的 IS 与同一区域中的其他 1 级 IS 交换路由信息。运行在 2 级的 IS 与其他 2 级路由器交换路由信息，而不管它们是否处于相同的 1 级区域内。2 级路由器集合以及将它们互连的链路形成 2 级子域，子域不能再分区，否则路由无法正常工作。

关于 NET

IS 通过称为网络实体名称 (NET) 的地址来标识。NET 是网络服务接入点 (NSAP) 的地址，标识 IS 上运行的 IS-IS 路由协议实例。NET 的长度为网络是 8 到 20 个八位组，它具有以下三个部分：

- 区域地址 - 此字段长度为 1 到 13 个八位组，由地址的高位八位组组成。

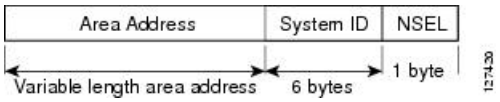
注释 您可以为一个 IS-IS 实例分配多个区域地址；在这种情况下，所有区域地址视为相同。当合并或拆分域中的区域时，多个相同的区域地址非常有用。合并或拆分完成后，您不需要为一个 IS-IS 实例分配超过一个区域地址。

- 系统 ID - 此字段的长度为 6 个八位组，它紧随区域地址之后。当 IS 在 Level 1 运行时，系统 ID 在相同区域中的所有 Level-1 设备中必须是唯一的。当 IS 在 Level 2 运行时，系统 ID 在域中的所有设备中必须是唯一的。

注释 您可以为一个 IS 实例分配一个系统 ID。

- NSEL - N-selector 字段的长度是 1 个八位组，它紧随系统 ID 之后。其必须设置为 00。

图 *1: NET* 格式



IS-IS 动态主机名

在 IS-IS 路由域中，使用系统 ID 代表每个 ASA。系统 ID 是为每个 IS-IS ASA 配置的 NET 的一部分。例如，NET 配置为 49.0001.0023.0003.000a.00 的 ASA 的系统 ID 为 0023.0003.000a。对于网络管理员而言，在 ASA 上进行维护以及故障排除期间，很难记住 ASA 名称与系统 ID 的映射。

输入 **show isis hostname** 命令可显示系统 ID 与 ASA 名称映射表中的条目。

动态主机名机制使用链路状态协议 (LSP) 泛洪来跨整个网络分发 ASA 名称与系统 ID 的映射信息。网络中的每个 ASA 都会尝试安装其路由表中的系统 ID 与 ASA 名称的映射信息。

如果一台一直在网络中通告动态名称类型、长度、值 (TLV) 的 ASA 突然停止通告，则最后收到的映射信息将在动态主机映射表中保留最多一个小时，以便网络遇到问题时网络管理员可以显示映射表中的条目。

IS-IS PDU 类型

ISes 使用协议数据单元 (PDU) 与其对等体交换路由信息。使用中间系统到中间系统 Hello PDU (IIH)、链路状态 PDU (LSP) 和序列号 PDU (SNP) 类型的 PDU。

IIH

IIH 将在已启用 IS-IS 协议的回路上的 IS 邻居之间交换。IIH 包括发送方的系统 ID、分配的区域地质，以及称为发送 IS 的回路上邻居的标识。还可包括其他可选信息。

有两种类型的 IIH：

- 1 级 LAN IIH - 当发送 IS 在该回路上作为 1 级设备运行时，将在多接入回路上发送这些信息。
- 2 级 LAN IIH - 当发送 IS 在该回路上作为 2 级设备运行时，将在多接入回路上发送这些信息。

LSP

IS 将生成 LSP，以通告其直接连接到 IS 的邻居和目标。LSP 通过以下方式进行唯一标识：

- 生成 LSP 的 IS 的系统 ID
- 伪节点 ID - 除非当 LSP 是伪节点 LSP 时，否则此值始终为 0。
- LSP 号（0 到 255）
- 32 位序列号

每当生成新版本的 LSP 时，序列号都会递增。

1 级 LSP 由支持 1 级的 IS 生成。1 级 LSP 将在整个 1 级区域泛洪。由某一区域内所有 1 级 IS 生成的 1 级 LSP 组是 1 级 LSP 数据库 (LSPDB)。某一区域内的所有 1 级 IS 都具有相同的 1 级 LSPDB，因此该区域具有相同的网络连接映射。

2 级 LSP 由支持 2 级的 IS 生成。2 级 LSP 将在整个 2 级子域泛洪。由相应域内所有 2 级 IS 生成的 2 级 LSP 组是 2 级 LSP 数据库 (LSPDB)。相应 2 级子域内的所有 2 级 IS 都具有相同的 2 级 LSPDB，因此该 2 级子域具有相同的连接映射。

SNP

SNP 包含一个或多个 LSP 的摘要说明。对于 1 级和 2 级，都有两种类型的 SNP：

- 完整序列号 PDU (CSNP) 用于针对指定级别发送 IS 具有的 LSPDB 的摘要。
- 部分序列号 PDU (PSNP) 用于针对指定级别发送 IS 在其数据库中具有或者需要获取的 LSP 的子网的摘要。

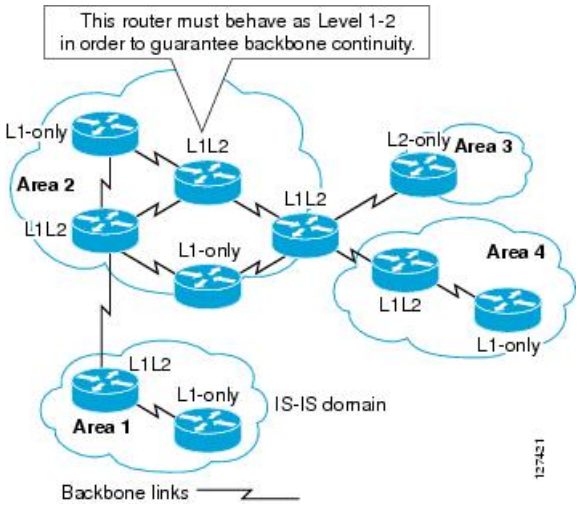
IS-IS 在多接入回路上的操作

多接入回路支持多个 ISes（即两个或更多）在回路上操作。对于多接入回路，必要的先决条件是能够使用组播或广播地址处理多个系统。在多接入回路上支持级别 1 的 IS 在回路上发送级别 1 LAN IIH。在多接入回路上支持级别 2 的 IS 在回路上发送级别 2 LAN IIH。ISes 针对每个级别与回路上的邻居 ISes 形成单独的邻接。

IS 与回路上支持级别 1 的其他 ISes 形成级别 1 邻接，并且具有匹配的区域地址。不支持两个支持级别 1 且具有一组断开连接的区域地址和的 ISes 位于同一多接入回路上。IS 与回路上支持级别 2 的其他 ISes 形成级别 2 邻接。

下图中 IS-IS 网络拓扑中的设备沿网络主干执行级别 1、级别 2 或者级别 1 和级别 2 路由。

图 *2: IS-IS* 网络拓扑中的级别 *1*、级别 *2*、级别 *1-2* 设备



指定 IS 的 IS-IS 选择

如果每个 IS 通告其 LSP 中的多路访问电路上的所有邻接关系，则所需的通告总数将为 N 2（其中 N 是在电路上给定级别运行的 IS 的数量）。为了解决这种可扩展性问题，IS-IS 定义了一个伪节点来表示该多路访问电路。在给定级别的电路上运行的所有 IS 选择其中一个 IS 充当该电路上的指定中间系统 (DIS)。对于电路上活动的每个级别，选择一个 DIS。

该 DIS 负责颁发伪节点 LSP。伪节点 LSP 包括在该电路上运行的所有 IS 的邻居通告。在电路（包括 DIS）上运行的所有 IS 在其非伪节点 LSP 中向伪节点提供邻居通告，而不会在多路访问电路上通告任何邻居。这样，所需的通告总数将作为 N-电路上运行的 IS 数的函数变化。

伪节点 LSP 由以下标识符唯一分类：

- 生成 LSP 的 DIS 的系统 ID
- 伪节点 ID（始终非零）
- LSP 号（0 到 255）
- 32 位序列号

非零伪节点 ID 是伪节点 LSP 与非伪节点 LSP 之间的区别，它由 DIS 选择，在 DIS 所处级别的所有 LAN 电路中是唯一的。

DIS 还负责在电路上发送定期 CSNP。其提供对 DIS 上 LSPDB 的当前内容的全面概述。然后，电路上的其他 IS 可执行以下活动，从而高效且可靠地同步多路访问电路上所有 IS 的 LSPDB：

- 泛洪 DIS 发送的 CSNP 中缺少的或比 CSNP 中所述的更新的 LSP。
- 对于 DIS 发送的 CSNP 中所述的本地数据库中缺少的 LSP 或比 CSNP 集中所述的 LSP 旧的 LSP，通过发送 PSNP 请求 LSP。

IS-IS LSPDB 同步

IS-IS 正常运行需要可靠和高效的进程，来同步每个 IS 上的 LSPDB。在 IS-IS 中，此进程称为更新进程。更新进程在每个受支持的级别独立运行。在本地生成的 LSP 始终是新 LSP。从回路上的邻居收到的 LSP 可能是由某个其他 IS 生成的，也可能是由本地 IS 生成的 LSP 的副本。与本地 LSPDB 的当前内容相比，收到的 LSP 可能较旧、龄期相同或较新。

处理较新的 LSP

在将较新的 LSP 添加到本地 LSPDB 时，它将替代 LSPDB 中相同 LSP 的较旧副本。较新的 LSP 将被标记为在所有回路上发送，在这些回路上，IS 当前在与较新的 LSP 相关联的级别包含一个处于运行状态的邻接 - 不包括在其上接收较新 LSP 的回路。

对于多接入回路，IS 会泛洪较新的 LSP 一次。IS 将检查 DIS 为多接入回路定期发送的 CNSP 组。如果本地 LSPDB 包含一个或多个比 CSNP 组中所述 LSP 更新的 LSP（这包括 CSNP 组中没有的 LSP），则将通过多接入回路重新泛洪这些 LSP。如果本地 LSPDB 包含一个或多个比 CSNP 组中所述内容更旧的 LSP（这包括 CSNP 组中所述但本地 LSPDB 中没有的 LSP），将在多接入回路上发送一个 PSNP，其中包含对需要更新的 LSP 的说明。用于多接入回路的 DIS 将通过发送请求的 LSP 作出响应。

处理较旧的 LSP

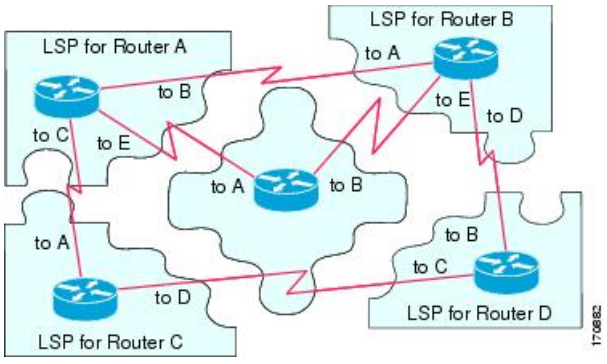
IS 可能会收到比本地 LSPDB 中的副本更旧的 LSP。IS 可能会收到 SNP（完整或部分），说明 LSP 比本地 LSPDB 中的副本更旧。在这两种情况下，IS 都会将本地数据库中的 LSP 标记为在收到较旧的 LSP 或包含该较旧 LSP 的 SNP 回路上泛洪。在向本地数据库添加新的 LSP 后，所采取的操作与上述操作相同。

处理龄期相同的 LSP

由于更新进程的分布式特性，IS 可能会收到与本地 LSPDB 的当前内容相同的 LSP 副本。在多接入回路中，收到龄期相同的 LSP 将被忽略。DIS 为该回路定期传输 CSNP 组，可以作为向发送方隐式确认已经收到 LSP。

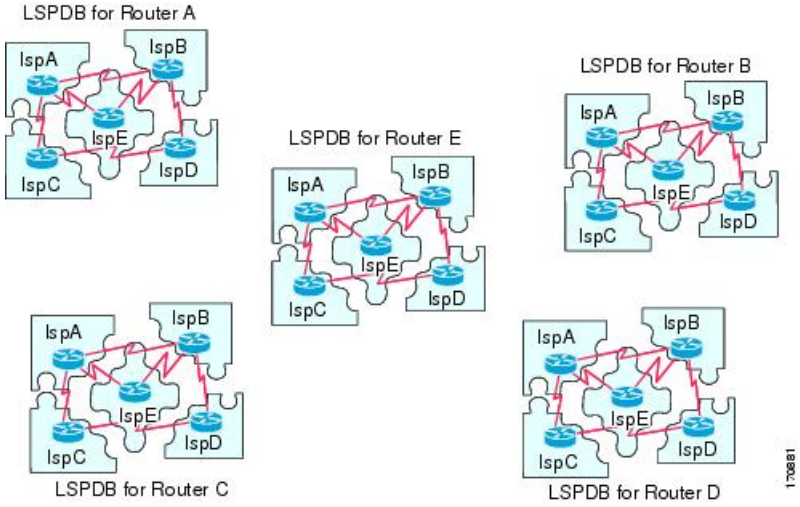
下图显示了如何使用 LSP 创建网络映射。请将网络拓扑视为拼图游戏。每个 LSP（代表一个 IS）都是一块拼图。这对某一区域中的所有 1 级设备或者 2 级子域中的所有 2 级设备都适用。

图 *3: IS-IS* 网络映射



下图显示了 IS-IS 网络中的每个设备，及其在邻居设备之间形成邻接之后已完全更新的链路状态数据库。这对某一区域中的所有 1 级设备或者 2 级子域中的所有 2 级设备都适用。

图 *4:* 包含已同步的 ***LSPDB*** 的 ***IS-IS*** 设备



IS-IS 最短路径计算

LSPDB 的内容发生变化时，每个 IS 都会独立重新运行最短路径计算。该算法基于著名的 Dijkstra 算法来延导向图查找最短路径，在导向图中，ISes 是图形的顶点，ISes 之间的链路是带有非负权重的边缘。将两个 ISes 之间的链路视为图形的一部分之前，将执行双向连接性检查。这样，可以防止在 LSPDB 中使用过时信息，例如，当一个 IS 不再在网络中运行，但又没有清除它在停止运行之前生成的一组 LSP 时。

SPF 的输出是一组元组（目标，下一跳）。目标是特定于协议的。支持多个成本相同的路径，不管是哪种情况，多个下一跳都会与同一目标关联。

对于 IS 支持的每个级别执行单独的 SPF。当级别 1 和级别 2 路径都到达同一目标时，优先选择级别 1 路径。

指示在其他区域有一个或多个级别 2 邻居的级别 2 IS 可能被与必备路径（也称为默认路由）处于同一区域的级别 1 设备所用。级别 2 IS 通过在其级别 1 LSP 0 设置连接位 (ATT) 来指示其与其他区域的连接。

注释 ID 可在每个级别生成多达 256 个 LSP。LSP 通过 0 至 255 之间的数字来标识。LSP 0 具有特定属性，包括设置 ATT 位以指示与其他区域的连接的重要性。当编号 1 至 255 的 LSP 设置了 ATT 位时，都没有意义。

IS-IS 关机协议

您可以关闭 IS-IS（将其置于管理停机状态）以对 IS-IS 协议配置进行更改，而不会丢失您的配置参数。您可以在全局 IS-IS 进程层面或接口层面关闭 IS-IS。如果在关闭该协议后重新启动该设备，则该协议预计会在禁用状态下恢复开机。如果将该协议设置为管理停机状态，将允许网络管理员以管

理方式关闭IS-IS协议的运行，而不会丢失协议配置；对协议配置进行一系列更改，而不必让协议转换的运行通过中间（也许不理想）状态；以及在以后适当时间重新启用该协议。

IS-IS 前提条件

在配置 IS-IS 之前，需要满足以下前提条件：

- 了解 IPv4 和 IPv6。
- 在配置 IS-IS 之前，了解您的网络设计以及您希望流量如何流过。
- 定义区域，准备设备的寻址计划（包括定义 NET）并确定将运行 IS-IS 的接口。
- 在配置设备之前，请准备一个邻接矩阵，显示邻接表中所期待的邻居。这样有助于进行验证。

IS-IS 准则

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

集群准则

仅在在单个接口模式下受支持；不支持跨网络 EtherChannel 模式。

其他准则

IS-IS 不支持双向转发。

配置 IS-IS

本节介绍如何在系统中启用和配置 IS-IS 进程。

过程

步骤 1 全局启用 IS-IS 路由，第 8 页。
步骤 2 启用 IS-IS 身份验证，第 11 页。
步骤 3 配置 IS-IS LSP，第 15 页
步骤 4 配置 IS-IS 汇总地址，第 19 页。
步骤 5 配置 IS-IS 被动接口，第 20 页。
步骤 6 配置 IS-IS 接口，第 21 页。

步骤 7 配置 IS-IS 接口呼叫传送，第 25 页

步骤 8 配置 IS-IS IPv4 地址系列，第 27 页。

步骤 9 配置 IS-IS IPv6 地址系列，第 32 页。

全局启用 IS-IS 路由

IS-IS 配置在两部分中完成。首先，在全局配置模式下配置 IS-IS 进程，然后在路由器配置模式下为 IS-IS 指定 NET 和路由级别。您可在路由器配置模式下为您的网络配置比按接口配置更加有意义的其他常规参数。本节包含这些命令。

接下来，在接口配置模式下对各个接口启用 IS-IS 协议，以便接口参与动态路由并与相邻设备形成邻接关系。您必须先在一个或多个接口上启用路由，然后才可建立邻接关系和实现动态路由。请参阅配置 IS-IS 接口，第 21 页，了解在接口上配置 IS-IS 的过程。

此过程介绍如何在 ASA 上启用 IS-IS 作为 IP 路由协议，以及在路由器配置模式下启用其他常规选项。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 在 ASA 上启用 IS-IS 作为路由协议：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 为路由进程指定 NET：

net *network-entity-title*

示例：

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

NET 会识别用于 IS-IS 的设备。有关 NET 的详细信息，请参阅关于 NET，第 1 页。

步骤 3 （可选）为 IS-IS 路由进程指定路由级别。

is-type [level-1 | level-2-only | level-1-2]

示例：

```
ciscoasa(config-router)# is-type level-1
```

- （可选）**level-1** - 表示区域内路由。ASA 只能理解在其区域内的目标。
- （可选）**level-2-only** - 表示区域内路由。ASA 是主干的一部分，它无法与自己区域内的第 1 级路由器通信。
- （可选）**level-1-2** - ASA 执行第 1 级和第 2 级路由。此路由器运行路由进程的两个实例。它具有一个 LSDB 用于区域中的目标（第 1 级路由），并且运行 SPF 计算来发现区域拓扑。它还具有包含其他所有主干（第 2 级）路由器的 LSP 的另一个 LSDB，并且运行其他 SPF 计算来发现主干的拓扑以及其他所有区域是否存在。

在常规 IS-IS 配置中，ASA 作为第 1 级（区域内部）和第 2 级（区域间）路由器。在多区域 IS-IS 配置中，配置 IS-IS 路由进程的第一个实例默认情况下是第 1-2 级（区域内部和区域间）路由器。配置的 IS-IS 进程的其余实例默认情况下是第 1 级路由器。

注释
我们强烈建议您配置 IS-IS 路由进程的类型。

步骤 4 在 ASA 上启用 IS-IS 动态主机名功能：

hostname dynamic

默认情况下会启用此命令。有关 IS-IS 中动态主机名的详细信息，请参阅 IS-IS 动态主机名，第 2 页。

步骤 5 在 ASA 上为所有接口配置呼叫填充：

hello padding multi-point

默认情况下会启用此命令。它将 IS-IS 呼叫配置为完整 MTU 大小。这允许及早检测因大型帧的传输问题导致的错误，或因相邻接口上的不匹配 MTU 导致的错误。

您可以禁用呼叫填充（**no hello padding multi-point** 用于 IS-IS 路由进程的某个路由器上的所有接口），以避免在两个接口的 MTU 相同或进行平移桥接时浪费网络带宽。当禁用呼叫填充时，ASA 仍然将填充的前五个 IS-IS 呼叫发送到完整的 MTU 大小，以保持发现 MTU 不匹配的优势。

在特权 EXEC 模式下输入 **show clns interface** 命令，以显示已在路由器级别关闭呼叫填充。有关详细信息，请参阅 监控 IS-IS，第 37 页。

步骤 6 （可选）使 ASA 可以在 NLSP IS-IS 邻接关系更改状态（运行或关闭）时生成日志消息：

log-adjacency-changes [all]

此命令默认禁用。当监控大型网络时，记录邻接关系更改非常有用。消息采用以下格式：

示例：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all-（可选）包括非 IIH 事件生成的更改。

步骤 7 （可选）禁用 IS-IS 协议，以便其无法在任何接口上形成任何邻接关系，并清除 LSP 数据库：

protocol shutdown

此命令使您可以禁用特定路由实例的 IS-IS 协议，而不删除任何现有 IS-IS 配置参数。当您输入此命令时，IS-IS 协议会继续在路由器上运行，并且您可以使用当前 IS-IS 配置，但是 IS-IS 不会在任何接口上形成任何邻接关系，而且它还会清除 IS-IS LSP 数据库。要为特定接口禁用 IS-IS，请使用 **isis protocol shutdown** 命令。请参阅配置 IS-IS 接口，第 21 页了解相关程序。

步骤 8 （可选）为 IS-IS IP 前缀分配高优先级：

route priority high tag *tag-value*

示例：

```
ciscoasa(config-router)# route priority high tag 100
```

tag*tag-value* - 为以特定路由标记为前缀的 IS-IS IP 分配高优先级。范围为 1 到 4294967295。

使用此命令可标记优先级较高的 IS-IS IP 前缀，从而在全局路由表中更快地进行处理和安装，实现更快的汇聚。例如，您可以帮助 VoIP 网关地址首先得到处理，从而帮助 VoIP 流量比其他类型的数据包更加快速地进行更新。

步骤 9 （可选）全局更改所有 IS-IS 接口的指标值：

metric *default-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# metric 55 level-1
```

- 默认值 - 要分配给链路的指标值，并且该指标值还用于计算到达目标的链路产生的路径开销。范围为 1 到 63。默认值为 10。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。

当您需要更改所有 IS-IS 接口的默认指标时，我们建议使用 **metric** 命令。这可以避免用户错误，例如意外地从接口中删除设置的指标而不配置新值，以及意外允许该接口恢复为默认指标 10，从而成为网络中的最佳首选接口。

步骤 10 （可选）配置 ASA 以仅生成和接受新式长度值对象 (TLV)：

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

示例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**- 使用具有窄指标的旧样式 TLV。
- **transition**- 指示 ASA 同时接受旧样式和新样式 TLV。

- **wide**- 使用新样式 TLV 以承载更宽的指标。
- （可选）**level-1** - 在路由第 1 级上启用此命令。
- （可选）**level-2** - 在路由第 2 级上启用此命令。
- （可选）**level-1-2** - 在路由第 1 级和第 2 级上启用此命令。

此命令会导致 ASA 仅生成和接受新式 TLV，从而导致 ASA 使用比生成旧式和新式 TLV 时更少的内存和其他资源。

步骤 11 （可选）在所有接口上配置指定 ASA 的优先级：

priority *number-value*

示例：

```
ciscoasa(config-router)# priority 80
```

number-value - ASA 的优先级。范围为 0 到 127。默认值为 64。

步骤 12 （可选）配置 IS-IS 区域的其他手动地址：

max-area-addresses 编号

示例：

```
ciscoasa(config-router)# max-area-addresses 3
```

number - 要添加的手动地址数量。范围为 3 到 254。没有默认值。

此命令使您可以通过配置其他手动地址来最大化 IS-IS 区域的大小。您指定要添加的地址数，并分配一个 NET 地址来创建每个手动地址。有关 NET 的信息，请参阅关于 NET，第 1 页。

步骤 13 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths - 要在路由表中安装的路由数。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

启用 IS-IS 身份验证

IS-IS 路由身份验证可避免从来源引入未经授权或错误的路由消息。您可以为每个 IS-IS 区域或域设置密码，以防止未授权的路由器将错误的路由信息注入到链路状态数据库中，也可以配置 IS-IS 身份验证的类型：即 IS-IS MD5 身份验证或增强的明文身份验证。您还可以按接口设置身份验证。必须

使用相同的身份验证模式和密钥来配置接口上为 IS-IS 消息身份验证配置的所有 IS-IS 邻居，才能建立邻接关系。

有关区域和域的详细信息，请参阅关于 IS-IS，第 1 页。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。

过程

步骤 1 输入 IS-IS 路由器配置模式并配置 IS-IS 区域身份验证密码：

area-password 密码 [**authenticate snp {validate | send-only}**]

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password* - 您分配的密码。
- （可选）**authenticate snp** - 导致系统将密码插入 SNP 中。
- **validate** - 导致系统将密码插入 SNP 中并将密码检入其收到的 SNP 中。
- **send-only**- 导致系统仅将密码插入 SNP 中，但不会将密码检入其收到的 SNP 中。请在软件升级期间使用此关键字，以简化传输。

在区域中的所有 ASA 上执行此命令可防止未授权的路由器在链路状态数据库中注入错误的路由信息。但是，此密码以纯文本形式进行交换，从而仅提供有限的安全性。

该密码会插入第 1 级（站路由器级别）PDU LSP、CSNP 和 PSNP 中。如果您不指定 **authenticate snp** 关键字与 **validate** 或 **send-only** 关键字，则 IS-IS 协议不会将密码插入 SNP 中。

步骤 2 输入 IS-IS 路由器配置模式并配置 IS-IS 域身份验证密码：

domain-password 密码 [**authenticate snp {validate | send-only}**]

示例：

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password* - 您分配的密码。
- （可选）**authenticate snp** - 导致系统将密码插入序列号 PDU (SNP) 中。
- **validate** - 导致系统将密码插入 SNP 中并将密码检入其收到的 SNP 中。

- **send-only**- 导致系统仅将密码插入 SNP 中，但不会将密码检入其收到的 SNP 中。请在软件升级期间使用此关键字，以简化传输。

此密码以纯文本形式进行交换，从而仅提供有限的安全性。

该密码会插入第 2 级（区域路由器级别）PDU LSP、CSNP 和 PSNP 中。如果您不指定 **authenticate snp** 关键字与 **validate** 或 **send-only** 关键字，则 IS-IS 协议不会将密码插入 SNP 中。

步骤 3 全局配置 IS-IS 实例，或按接口配置以仅对正在发送（未接收）的 IS-IS 数据包执行身份验证：

路由器模式：**authentication send-only [level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication send-only level-1
```

接口模式：**isis authentication send-only [level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- （可选）**level-1** - 仅对正在发送（未接收）的第 1 级数据包执行身份验证。
- （可选）**level-2** - 仅对正在发送（未接收）的第 2 级数据包执行身份验证。

在配置身份验证模式和身份验证密钥链之前使用此命令，以便顺利地实施身份验证。如果您不指定第 1 级或第 2 级，则 send only 会同时应用于两个级别。

注释
如果身份验证仅插入正在发送的数据包，而未在正接收的数据包上检入，则对于要在每个 ASA 上配置的密钥，ASA 将有更多时间。使用此命令配置必须通信的所有 ASA 后，请在每个 ASA 上启用身份验证模式和密钥链。

步骤 4 全局或按接口为 IS-IS 实例指定 IS-IS 数据包中使用的身份验证模式类型：

路由器模式：**authentication mode {md5 | text} [level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication mode md5 level-1
```

接口模式：**isis authentication mode {md5 | text} [level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5** - 启用消息摘要 5 身份验证。

- **text** - 使用明文身份验证。
- （可选）**level-1** - 仅为第 1 级数据包启用指定的身份验证。
- （可选）**level-2** - 仅为第 2 级数据包启用指定的身份验证。

如果您使用 **area-password** 或 **domain-password** 配置了明文身份验证，则 isis authentication mode 会替代这两个命令。如果配置 **isis authentication mode**，然后尝试配置 **area-password** 或 **domain-password**，则不允许这样做。如果您不指定第 1 级或第 2 级，则该模式会同时应用于两个级别。

步骤 5 全局或按接口为 IS-IS 启用身份验证：

路由器模式：**authentication key [0 | 8]**密码**[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

接口模式：**isis authentication key [0 | 8]**密码**[level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0** - 指定将采用未加密的密码。
- **8** - 指定将采用加密的密码。
- *password* - 启用身份验证并指定密钥。
- （可选）**level-1** - 仅为第 1 级数据包启用指定的身份验证。
- （可选）**level-2** - 仅为第 2 级数据包启用指定的身份验证。

如果未通过 **key** 命令配置密码，则不执行密钥身份验证。密钥身份验证可以应用于明文或 MD5 身份验证。如要设置模式，请参阅第 4 步。一次仅将一个身份验证密钥应用于 IS-IS。如果您配置第二个密钥，则第一个密钥将被覆盖。如果您不指定第 1 级或第 2 级，则密码会同时应用于两个级别。

步骤 6 为接口配置身份验证密码：

isis password *password* **[level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password* - 您分配至接口的身份验证密码。
- （可选）**level-1** - 单独为第 1 级配置身份验证密码。对于第 1 级路由，ASA 仅用作站路由器。

- （可选）**level-2** - 单独为第 2 级配置身份验证密码。对于第 2 级路由，ASA 仅用作区域路由器。

此命令使您可以防止未授权的路由器与此ASA形成邻接关系，从而保护网络免遭入侵者的侵害。该密码以纯文本形式进行交换，从而提供有限的安全性。您可以使用 **level-1** 和 **level-2** 关键字为不同的路由级别分配不同的密码。

示例

以下示例显示了对第 1 级数据包执行 MD5 身份验证的 IS-IS 实例，以及如何发送属于名为 site1 的密钥链的任何密钥：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

配置 IS-IS LSP

IS 生成 LSP 来通告其邻居和直接连接到 IS-IS 的目标。有关 LSP 的更多详细信息，请参阅IS-IS PDU 类型，第 2 页。

使用以下命令配置 LSP，可以实现更快的收敛配置。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 配置 ASA 以忽略接收时发生内部校验和错误的 IS-IS LSP，而不是清除 LSP：

ignore-lsp-errors

示例：

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS 要求接收方清除具有不正确数据链路校验和的 LSP，从而使数据包的发起程序重新生成该 LSP。如果网络具有导致数据损坏的链路，同时仍然传送具有正确数据链路校验和的 LSP，则可能会发生清除和重新生成大量数据包的连续循环，这可能导致网络无法正常工作。使用此命令可忽略 LSP 而不是将其清除。默认设置为启用。

步骤 3 配置 IS-IS 以仅通告属于被动接口的前缀：

advertise passive-only

此命令将已连接网络的 IP 前缀排除在 LSP 通告之外，从而减少收敛时间，因为在路由器非伪节点 LSP 中通告的前缀较少。

步骤 4 将 IS-IS LSP 配置为已满：

fast-flood *lsp-number*

示例：

```
ciscoasa(config-router)# fast-flood 7
```

（可选）*lsp-number* - 要在开始 SPF 前泛洪的 LSP 数目

此命令从 ASA 发送指定数目的 LSP。这些 LSP 在运行 SPF 之前调用 SPF。加速 LSP 泛洪过程可提高整体收敛时间。范围为 1 到 15。默认值为 5。

注释
我们建议您在路由器运行 SPF 计算之前启用 LSP 快速泛洪。

步骤 5 配置 IS-IS LSP 的 MTU 大小：

lsp-mtu *bytes*

示例：

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes - 以字节为单位的最大数据包大小。字节数必须小于或等于网络中任意链路的最小 MTU。范围为 128 到 4352。

步骤 6 设置 LSP 在 ASA 的数据库中不刷新存在的最长时间：

max-lsp-lifetime 秒

示例：

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds - LSP 的有效期（以秒数为单位）。范围为 1 到 65,535。默认值为 1200。

如果在新 LSP 到达前超出有效期，该 LSP 将从数据库中删除。

步骤 7 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 8 自定义 IS-IS 的 SPF 生成限制：

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

示例：

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *lsp-max-wait* - 表示两次连续的 LSP 生成之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*lsp-initial-wait* - 表示生成第一个 LSP 前的初始等待时间。范围是 1 到 120000 毫秒。默认值为 50 毫秒。

  每个后续的等待间隔均是前一个的两倍，直到等待间隔达到指定的 LSP 最大等待间隔。
- （可选）*lsp-second-wait* - 表示生成第一个和第二个 LSP 之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  此命令控制生成 LSP 之间的延迟。

步骤 9 设置 LSP 刷新间隔：

lsp-refresh-interval 秒

示例：

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

（可选）*seconds* - LSP 的刷新间隔。范围为 1 到 65535 秒。默认值为 900 秒（15 分钟）。

刷新间隔确定该软件在 LSP 中定期发送其始发的路由拓扑信息的速率。这样做是为了防止数据库信息过时。

注释
在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果设置的 LSP 有效期比 LSP 刷新间隔低很多，该软件将缩短 LSP 刷新间隔以防止 LSP 超时。

步骤 10 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 11 配置在 PDU 已满时抑制的路由：

lsp-full suppress {external [interlevel] | interlevel [external] | none}

示例：

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external**- 抑制此 ASA 上的所有重新分发路由。
- **interlevel**- 抑制来自其他级别的所有路由。例如，如果 Level 2 LSP 已满，则将抑制来自 Level 1 的路由。

- **none**- 不抑制任何路由。

在对重新分发到 IS-IS 中的路由数目没有限制的网络（即未配置 **redistribute maximum-prefix** 命令）中，LSP 可能将填满，并且路由会被丢弃。使用 **lsp-full suppress** 命令可提前定义当 LSP 变满时要抑制的路由。

配置 IS-IS 汇总地址

给定级别下可以汇总多个地址组。从其他路由协议获知的路由也可以汇总。用于通告汇总的指标是所有较为具体路由的最小指标。这有助于减小路由表的大小。

如果要创建不发生在网络编号编辑的汇总地址，或者要在禁用了自动路由汇总的ASA上使用汇总地址，则需要手动定义汇总地址。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 创建 IS-IS 的汇聚地址。

address mask tag-number metric-value **summary-address [level-1 | level-1-2 | level-2] tag metric**

示例：

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address* - 为一系列 IP 地址指定的汇总地址。
- *mask* - 用于汇总路由的 IP 子网掩码。
- （可选）**level-1** - 仅重新分发到第 1 级的路由通过配置的地址和掩码值汇总。
- （可选）**level-1-2** - 当重新分发路由到第 1 级和第 2 级时，以及当第 2 级 IS-IS 将第 1 级路由通告为在其区域中可访问时，汇总路由适用。
- （可选）**level-2** - 第 1 级路由了解的路由通过配置的地址和掩码值汇总到第 2 级主干。重新分发到第 2 级 IS-IS 中的路由也会汇总。
- （可选）**tag***tag-number* - 指定用于标记汇总路由的编号。范围为 1 到 4294967295。

- （可选）**metric***metric-value* - 指定应用到汇总路由的指标值。**metric** 关键字分配给链路，并且用于计算到达目标的链路产生的路径开销。您仅可为第 1 级或第 2 级路由配置此指标。范围为 1 到 4294967295。默认值为 10。

输入 **show clns interface** 命令以验证接口的指标值，请参阅 监控 IS-IS，第 37 页 了解更多信息。

配置 IS-IS 被动接口

您可以禁用接口上的 IS-IS hello 数据包和路由更新，同时仍在拓扑数据库中包含接口地址。这些接口不会形成 IS-IS 邻居关系

如果有不希望参加 IS-IS 路由但已连接到要通告网络的接口，请配置被动接口（使用 **passive-interface** 命令），以防止该接口使用 IS-IS。此外，您还可以指定 ASA 用于更新的 IS-IS 版本。备用路由帮助控制 IS-IS 路由信息的通告并禁用在接口上发送和接收 IS-IS 路由更新。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 在 ASA 上配置被动接口：

passive-interface *interface-name*

示例：

```
ciscoasa(config-router)# passive-interface inside
```

- **default** - 抑制所有接口上的路由更新。
- **management**- 抑制 Management 0/1 接口上的更新。
- **management2** - 抑制 Management 0/2 接口上的更新。
- **inside**- 抑制内部接口上的更新。

此命令配置接口 NOT 以形成 IS-IS 邻居邻接关系，并将接口地址包含在 IS-IS 数据库中。

步骤 3 配置 ASA 以通告被动接口：

advertise passive-only

示例：

```
ciscoasa(config-router)# advertise passive-only
```

此命令配置 IS-IS 以仅通过属于被动接口的前缀。它从 LSP 通告中排除连接的网络的 IP 前缀，从而缩短 IS-IS 汇聚时间。

配置 IS-IS 接口

此程序介绍如何为 IS-IS 路由修改各个 ASA 接口。您可以修改以下内容：

- 常规设置，如启用 IS-IS、启用 IS-IS 关机协议、优先级、标签和接口上的邻接筛选器。
- 身份验证密钥和模式 - 有关配置接口上的身份验证的程序，请参阅启用 IS-IS 身份验证，第 11 页。
- 呼叫填充值 - 有关配置接口上的呼叫填充的程序，请参阅配置 IS-IS 接口呼叫传送，第 25 页。
- LSP 设置
- IS-IS 指标计算中使用的接口延迟指标。

开始之前

必须分配一个 NET，并且一些接口必须启用 IS-IS，然后才能使用 IS-IS 路由进程。您只能配置一个进程来执行 2 级（区域间）路由。如果在任何进程上配置了 2 级路由，则所有其他进程都将被自动配置为 1 级。同时，您还可以将此进程配置为执行区域内（1 级）路由。除非是在相关联的路由进程既执行 1 级路由又执行 2 级路由的情况下，否则一个接口不能成为多个区域的组成部分。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。

过程

步骤 1 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

步骤 2 对 IS-IS 邻接的建立进行筛选：

isis adjacency-filter 名称 **[match-all]**

示例：

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- 名称 - 要应用的筛选器集合或表达式的名称。
- （可选）**match-all** - 所有 NSAP 地址都必须与筛选器匹配，才能接受邻接。如果未指定（默认设置），则只需一个地址与筛选器匹配，即可接受邻接。

通过将呼叫中的每个区域地址与系统 ID 结合起来，在传入 IS-IS 呼叫数据包之外建立 NSAP 地址，进而执行筛选。随后，这些NSAP地址中的每个地址都将通过该筛选器。如果任何一个NSAP匹配，则该筛选器将被视为符合条件；除非指定**match-all**关键字，在这种情况下，所有地址都必须符合条件。**match-all** 关键字的功能在执行负面测试时非常有效，如仅在特定地址不存在时接受邻接。

步骤 3 在 IS-IS 接口上的 LSP 通告中通告已连接网络的 IS-IS 前缀：

isis advertise prefix

示例：

```
ciscoasa(config-if)# isis advertise prefix
```

默认情况下会启用此命令。因此，即使不打算分发已连接的路由，它们也会被分发。要停止不必要的已连接路由重新分发并缩短 IS-IS 融合时间，请使用 **no isis advertise prefix** 命令。这将从 LSP 通告中排除已连接网络的 IP 前缀，进而缩短 IS-IS 收敛时间。

注释
逐个 IS-IS 接口配置此命令的 **no** 形式是缩短 IS-IS 收敛时间的小规模解决方案，因为在路由器非伪节点 LSP 中通告的前缀较少。**isis advertise prefix** 命令的替代方法之一是 **advertise passive-only** 命令，这是一个可扩展的解决方案，因为可以逐个 IS-IS 实例配置此命令。

步骤 4 在 IS-IS 接口上启用 IPv6

ipv6 router isis

示例：

```
ciscoasa(config-if)# ipv6 router isis
```

步骤 5 逐个接口配置两次连续 IS-IS LSP 传输之间的时间延迟：

isis lsp-interval *milliseconds*

示例：

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds - 两次连续 LSP 之间的时间延迟。范围为 1 到 4294967298。默认值为 33 毫秒。

在包含大量 IS-IS 邻居和接口的拓扑中，ASA 可能难以处理 LSP 传输和接收造成的 CPU 负载。此命令可以降低 LSP 传输速率（言外之意，也会降低其他系统的接收速率）。

步骤 6 配置 IS-IS 指标的值：

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

示例：

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value* - 分配给链路并且用于计算从每个其他路由器通过网络中的链路到达其他目标的开销的指标。不能为 1 级和 2 级路由配置此指标。范围是从 1 到 63。默认值为 10。
- **maximum**- 从 SPF 计算中排除某一链路或邻接。
- （可选）**level-1** - 指定仅应将此指标用于 1 级（区域内）路由的 SPF 计算。如果未指定可选关键字，则将在 1 级和 2 级路由上启用该指标。
- （可选）**level-2** - 指定仅应将此指标用于 2 级（区域间）路由的 SPF 计算。如果未指定可选关键字，则将在 1 级和 2 级路由上启用该指标。

步骤 7 配置接口上指定 ASA 的优先级：
isis priority *number-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value* - 设置 ASA 的优先级。范围为 0 到 127。默认值为 64。
- （可选）**level-1** - 独立设置 1 级的优先级。
- （可选）**level-2** - 独立设置 2 级的优先级。

该优先级用于确定 LAN 上的哪一个 ASA 将成为指定路由器或 DIS。优先级将在呼叫数据包中通告。优先级最高的 ASA 将成为 DIS。

注释
在 IS-IS 中，没有指定备份的路由器。将优先级设置为 0 将降低此系统成为 DIS 的几率，但不会阻止其成为 DIS。如果优先级更高的路由器上线，则它将接管当前 DIS 的角色。在优先级相等的情况下，最高 MAC 地址将打破平衡。

步骤 8 禁用 IS-IS 协议，这样它将无法在指定接口上形成邻接，并且会将该接口的 IP 地址置于 ASA 生成的 LSP 中：

isis protocol shutdown

示例：

```
ciscoasa(config-if)# isis protocol shutdown
```

此命令将使您能为指定接口禁用 IS-IS 协议，而不会删除配置参数。IS-IS 协议不会为已配置此命令的接口形成任何邻接，并且会将该接口的 IP 地址置于路由器生成的 LSP 中。如果您不希望 IS-IS 在任何接口上形成任何邻接，并且希望清除 IS-IS LSP 数据库，则请使用 **protocol shutdown** 命令。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。

步骤 9 配置每个 IS-IS LSP 的两次重新传输之间的时间量：

isis retransmit-interval 秒

示例：

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

（可选）*seconds* - 每个 LSP 的两次重新传输之间的时间。数字应该大于已连接网络上任意两个路由器之间的预计往返延迟。范围为 0 到 65535。默认值为 5 秒。

请确保保守地设置 *seconds* 参数，否则可能会导致不必要的重新传输。此命令对 LAN（多点）接口没有影响。

步骤 10 配置每个 IS-IS LSP 的两次重新传输之间的时间量：

isis retransmit-throttle-interval *milliseconds*

示例：

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

（可选）*milliseconds* - 相应接口上两次 LSP 重新传输之间的最小延迟。范围为 0 到 65535。

在包含很多 LSP 和很多接口的大型网络中，作为控制 LSP 重新传输流量的一种方式，此命令可能非常有效。此命令可以控制可在接口上重新发送 LSP 的速率。

此命令与控制可在接口上发送 LSP 的速率（由 **isis lsp-interval** 命令控制）的命令不同，也与控制某一 LSP 的两次重新传输之间的时间段（由 **isis retransmit-interval** 命令控制）的命令不同。您可以组合使用这些命令，以控制从一个 ASA 到其邻居的路由流量的提供负载。

步骤 11 在将 IP 前缀置于 IS-IS LSP 中时，在为接口配置的 IP 地址上设置标签。

isis tag *tag-number*

示例：

```
ciscoasa(config-if)# isis tag 100
```

tag-number - 用作 IS-IS 路由上的标签的数字。范围为 1 到 4294967295。

直到使用标签时，才会对设置该标签的路由进行操作，例如，重新分发路由或汇总路由。配置此命令将触发 ASA 生成新的 LSP，因为标签是数据包中新的信息片段。

示例

在此示例中，使用不同的标签值为两个接口设置了标签。默认情况下，已将这两个 IP 地址置于 IS-IS 1 级和 2 级数据库中。不过，如果您使用包含路由映射的 **redistribute** 命令以匹配标签 110，则只会将 IP 地址 172.16. 0.0 置于 2 级数据库中。

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

配置 IS-IS 接口呼叫传送

呼叫数据包负责发现邻居，并维护邻接关系。您可以在接口级别配置以下呼叫传送参数。请参阅全局启用 IS-IS 路由，第 8 页以启用/禁用整个 IS-IS 的呼叫传送。

过程

步骤 1 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

步骤 2 进入接口配置模式可在 ASA 上所有接口的 IS-IS 呼叫协议数据单元 (IIH PDU) 上配置填充：

isis hello padding

示例：

```
ciscoasa(config-if)# isis hello padding
```

呼叫报文会填满MTU，这允许早期检测由于大帧的传输问题导致的错误或由于相邻接口上不匹配的MTU 导致的错误。IS-IS 呼叫传送默认启用。

注释
如果两个接口的 MTU 相同，或者在转换桥接的情况下，可以禁用呼叫传送以避免浪费网络带宽。当呼叫传送被禁用时，ASA 仍然会发送前五个IS-IS呼叫报文以填满MTU大小，从而维持发现MTU不匹配的优势。

步骤 3 指定 IS-IS 发送的连续呼叫数据包之间的时间长度：

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds* - 呼叫数据包之间的时间长度。默认情况下，将通告一个三倍于呼叫间隔（以秒为单位）的值，作为已发送的呼叫数据包中的保持时间。您可以通过配置 **isis hello-multiplier** 命令更改乘数 3。对于较小的呼叫间隔，检测到的拓扑变化更快，但路由流量更多。范围为 0 到 65535。默认值为 10。
- **minimal** - 使系统基于呼叫乘数（通过 **isis hello-multiplier** 命令指定）计算呼叫间隔，以使结果保持时间为 1 秒。
- （可选）**level-1** - 单独配置级别 1 的呼叫间隔。请在 X.25、交换式多兆位数据服务 (SMDS) 和帧中继多路访问网络上使用此配置。
- （可选）**level-2** - 单独配置级别 2 的呼叫间隔。请在 X.25、SMDS 和帧中继多路访问网络上使用此配置。

注释
虽然较慢的呼叫间隔可以节省带宽和CPU使用率，但在有些情况下，要优先使用更快的呼叫间隔，例如使用流量工程 (TE) 隧道的大型配置。如果 TE 隧道使用 IS-IS 作为内部网关协议 (IGP)，并且 IP 路由进程在网络入口处的路由器（头端）上重新启动，则所有 TE 隧道会以此默认呼叫间隔收到重复信号。更快的呼叫间隔可防止此重复信号。要配置更快的呼叫间隔，您需要使用**isis hello-multiplier** 命令手动增加 IS-IS 呼叫间隔。

步骤 4 指定 ASA 宣布邻接关系断开前该邻居必须错失的 IS-IS 呼叫数据包数目：

isis hello-multiplier *multiplier* **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler* - IS-IS 呼叫数据包中通告的保持时间设置为呼叫间隔的呼叫乘数倍数。在通告的保持时间期间未收到任何 IS-IS 呼叫数据包后，邻居宣布与此 ASA 的邻接关系断开。您可以在每个接口的基础上设置保持时间（从而设置呼叫乘数和呼叫间隔），并且一个区域中的不同路由器之间的保持时间可以不同。范围为 3 到 1000。默认值为 3。
- （可选）**level-1** - 单独配置级别 1 邻接关系的呼叫乘数。
- （可选）**level-2** - 单独配置级别 2 邻接关系的呼叫乘数。

在呼叫数据包频繁丢失并且 IS-IS 邻接关系不必要地失败的情况下，使用此命令。

注释
使用较小的呼叫乘数将使收敛更快，但是会导致更加路由不稳定。在需要时将呼叫乘数更改为较大的值有助于网络稳定切勿配置小于默认值 3 的 呼叫乘数。

步骤 5 配置用于 IS-IS 的邻接关系类型：

isis circuit-type [level-1 | level-1-2 | level-2-only]

示例：

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- （可选） **level-1** - 仅为级别 1 邻接关系配置 ASA。
- （可选）**level-1-2** - 为级别 1 和级别 2 邻接关系配置 ASA。
- （可选） **level-2** - 仅为级别 2 邻接关系配置 ASA。

您通常不需要配置此命令。正确的方式是在 ASA 上配置级别。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。您应在区域之间（级别 1-2 路由器）的 ASA 上将某些接口配置为仅级别 2。这会通过发出未使用的级别 1 呼叫数据包节省带宽。

步骤 6 配置定期 CSNP 数据包在广播接口上发送的间隔：

isis csnp-interval 秒 **[level-1 | level-1-2 | level-2]**

示例：

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds* - 多路访问网络上 CSNP 传输之间的时间间隔。此间隔仅适用于指定 ASA。范围为 0 到 65,535。默认值为 10 秒。
- （可选）**level-1** - 单独配置 级别 1 的 CSNP 传输之间的时间间隔。
- （可选）**level-2** - 单独配置 级别 2 的 CSNP 传输之间的时间间隔。

您不太可能需要更改此命令的默认值。

此命令仅适用于指定接口的 DR。仅 DR 会发送 CSNP 数据包以维持数据库同步。您可以单独为级别 1 和级别 2 配置 CSNP 间隔。

配置 IS-IS IPv4 地址系列

允许路由器重新分发从任何其他路由协议、静态配置或已连接的接口获悉的外部前缀或路由。允许重新分发的路由处于第 1 层路由器或第 2 层路由器。

您可以设置邻接、最短路径优先 (SPF)，还可以定义针对 IPv4 地址将路由从另一个路由域重新分发到 ISIS（重新分发）的条件。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。

过程

步骤 1 进入路由器配置模式，配置 IPv4 地址系列：

router isis

示例：

```
ciscoasa(config)# router isis
cisco(config-router)#
```

步骤 2 执行邻接检查，以检查 IS-IS 协议支持：

adjacency-check

示例：

```
cisco(config-router)# adjacency-check
```

步骤 3 定义分配给通过 IS-IS 协议发现的路由的管理距离：

distance *weight*

权重 - 分配给 IS-IS 路由的管理距离。范围为 1 到 255。默认值为 115。

示例：

```
ciscoasa(config-router)# distance 20
```

在 RIB 中插入 IS-IS 路由，并且这些路由影响它们优先于其他协议发现的、到相同目的地址的路由的可能性时，此命令会配置应用于这些 IS-IS 路由的距离。

注释
一般来说，管理距离的值越大，信任评分就越低。管理距离为255意味着根本无法信任路由信息源，应将其忽略。权重值是主观的；目前尚没有量化方法来选择权重值。

步骤 4 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router)# maximum-paths 8
```

路径数 - 要安装到路由表中的路由的数量。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

步骤 5 生成到 IS-IS 路由域中的默认路由：

default-information originate [**route-map** *map-name*]

示例：

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

（可选）**route-map** *map-name* - 如果满足路由映射，则路由进程将生成默认路由。

如果使用此命令配置的 ASA 的路由表中包含到 0.0.0.0 的路由，则 IS-IS 将在其 LSP 中为 0.0.0.0 发出一条通告。如果没有路由映射，则将仅在第 2 层 LSP 中通告默认值。对于第 1 层路由，还有另一种查找默认路由的机制，即查找最近的第 1 层或第 2 层路由器。可以通过查看第 1 层 LSP 中的 ATT 查找最近的第 1 层或第 2 层路由器。通过 **match ip address** *standard-access-list* 命令，您可以指定一个或多个必须存在的 IP 路由，然后 ASA 才能通告 0/0。

步骤 6 以全局方式为第 1 层和第 2 层设置 IS-IS 指标：

metric *default-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- 默认值 - 要分配给链路的指标值，并且该指标值还用于计算到达目标的链路产生的路径开销。范围为 1 到 63。默认值为 10。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。

步骤 7 指定指标样式以及将其应用于哪些层：

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

示例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**- 指示 ASA 使用窄指标的旧样式 TLV。
- **transition**- 指示 ASA 在过渡期间接受旧样式和新样式的 TLV。
- **wide**- 指示 ASA 使用新样式的 TLV，以承载更广泛的指标。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。
- （可选）**level-1-2** - 设置第 1 层和第·2 层 IPv4 或 IPv6 指标。

步骤 8 为第 1 层 - 第 2 层路由器何时应该设置其附加位指定约束：

set-attached-bit route-map *map-tag*

示例：

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag* - 配置的路由映射的标识符。如果指定的路由映射匹配，则路由器将继续设置其附加位。此命令默认禁用。

在当前的 IS-IS 实施中，正如 ISO 10589 中指定的那样，第 1 层-第 2 层路由器将在其在自己的域中看到其他区域或者看到其他域时设置其第 1 层 LSP 附加位。不过，在某些网络拓扑中，不同区域内相邻的第 1 层-第 2 层路由器可能会失去到第 2 层主干的连接。第 1 层路由器随后可将发往区域或域以外的流量发送到可能没有此类连接的第 1 层-第 2 层路由器。

此命令允许对第 1 层-第 2 层路由器的附加位设置进行更好的控制。路由映射可以指定一条或多条 CLNS 路由。如果至少一个匹配地址路由映射子句与第 2 层 CLNS 路由表中的路由相匹配，并且如果已满足设置附加位的所有其他要求，则第 1 层-第 2 层路由器将继续在其第 1 层 LSP 中设置附加位。如果不满足要求，或者没有匹配地址路由映射子句与第 2 层 CLNS 路由表中的路由相匹配，则不会设置附加位。

步骤 9 将 ASA 配置为向其他路由器发送信号，告知它们不要在其 SPF 计算中将该 ASA 用作中间跳：

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

示例：

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （可选）**on-startup** - 设置系统启动时的过载位。根据指定的后续参数或关键字，过载位将在已配置的秒数内或在 BGP 收敛之前保持设置。
- （可选）秒数 - 在系统启动时设置过载位并且保持设置的秒数。范围为 5 到 86400。
- （可选）**wait-for-bgp** - 在配置 **on-startup** 关键字后，将导致在系统启动时设置过载位，并在 BGP 收敛之前保持设置。
- （可选）**suppress** - 导致通过一个或多个后续关键字标识的前缀类型被抑制。
- （可选）**interlevel** - 在配置 **suppress** 关键字后，将阻止通告从其他 IS-IS 层获悉的 IP 前缀。
- （可选）**external** - 在配置 **suppress** 关键字后，将阻止通告从其他协议获悉的 IP 前缀。

此命令将强制 ASA 在其非伪节点 LSP 中设置过载位（也称为跳跃位）。通常，仅当 ASA 遇到问题时，才允许设置过载位。例如，当 ASA 遇到内存不足的问题时，可能是因为链路状态数据库不完整，这将导致路由表不完整或不准确。通过在其 LSP 中设置过载位，其他路由器可以在其 SPF 计算中忽略不可靠的路由器，直到该路由器从其问题中恢复过来。结果是该 IS-IS 区域中的其他路由器不会看到任何通过此路由器的路径。不过，IP 和 CLNS 前缀将直接连接到此路由器。

步骤 10 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 11 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 12 配置 IS-IS 在 SFP 计算期间履行外部指标：

use external-metrics

步骤 13 配置 BGP、Connected、IS-IS、OSPF 或 Static 路由重新分发：

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric 编号

示例：

```
ciscoasa(config-router)# redistribute bgp level-1 metric-type internal metric 6
```

注释
不支持使用与指标匹配的路由映射重新分配静态路由。

metric *number* - 指标的值。范围为 1 到 4294967295。

附加位配置

在下面的示例中，当路由器与 L2 CLNS 路由表中的 49.00aa 相匹配时，附加位将保持已设置状态：

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

配置 IS-IS IPv6 地址系列

您可以设置邻接关系、SPF，并且可以针对 IPv6 地址定义条件以便将其他路由域中的路由重新分发到 IS-IS 中（重新分发）。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 8 页了解相关程序。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
cisco(config-router)#
```

步骤 2 将指标样式指定为宽：

metric-style wide [transition] [level-1 | level-2 | level-1-2]

示例：

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (Optional) **transition**— Instructs the router to accept both old- and new-style TLVs.
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。
- （可选）**level-1-2** - 设置第 1 层和第·2 层 IPv4 或 IPv6 指标。

当您需要更改所有 IS-IS 接口的默认指标时，我们建议使用 **metric** 命令。这可以避免用户错误，例如意外地从接口中删除设置的指标而不配置新值，以及意外允许该接口恢复为默认指标 10，从而成为网络中的最佳首选接口。

步骤 3 进入地址系列配置模式，以配置使用标准 IPv4 或 IPv6 地址前缀的 IS-IS 路由会话：

address-family ipv6 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

步骤 4 执行邻接检查，以检查 IS-IS 协议支持：

adjacency-check

示例：

```
cisco(config-router-af)# adjacency-check
```

步骤 5 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths - 要在路由表中安装的路由数。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

步骤 6 定义分配给通过 IS-IS 协议发现的路由的管理距离：

distance *weight*

weight - 分配给 IS-IS 路由的管理距离。范围为 1 到 255。默认值为 115。

示例：

```
ciscoasa(config-router-af)# distance 20
```

在 RIB 中插入 IS-IS 路由，并且这些路由影响它们优先于其他协议发现的、到相同目的地址的路由的可能性时，此命令会配置应用于这些 IS-IS 路由的距离。

注释
一般来说，管理距离的值越大，信任评分就越低。管理距离为255意味着根本无法信任路由信息源，应将其忽略。权重值是主观的；目前尚没有量化方法来选择权重值。

步骤 7 生成到 IS-IS 路由域中的默认路由：

default-information originate [**route-map** *map-name*]

示例：

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

（可选）**route-map** *map-name* - 如果满足路由映射，则路由进程将生成默认路由。

如果使用此命令配置的 ASA 的路由表中包含到 0.0.0.0 的路由，则 IS-IS 将在其 LSP 中为 0.0.0.0 发出一条通告。如果没有路由映射，则将仅在第 2 层 LSP 中通告默认值。对于第 1 层路由，还有另一种查找默认路由的机制，即查找最近的第 1 层或第 2 层路由器。可以通过查看第 1 层 LSP 中的 ATT 查找最近的第 1 层或第 2 层路由器。通过 **match ip address** *standard-access-list* 命令，您可以指定一个或多个必须存在的 IP 路由，然后 ASA 才能通告 0/0。

步骤 8 将 ASA 配置为向其他路由器发送信号，告知它们不要在其 SPF 计算中将该 ASA 用作中间跳：

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

示例：

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （可选）**on-startup** - 设置系统启动时的过载位。根据指定的后续参数或关键字，过载位将在已配置的秒数内或在 BGP 收敛之前保持设置。
- （可选）秒数 - 在系统启动时设置过载位并且保持设置的秒数。范围为 5 到 86400。
- （可选）**wait-for-bgp** - 在配置 **on-startup** 关键字后，将导致在系统启动时设置过载位，并在 BGP 收敛之前保持设置。
- （可选）**suppress** - 导致通过一个或多个后续关键字标识的前缀类型被抑制。
- （可选）**interlevel** - 在配置 **suppress** 关键字后，将阻止通告从其他 IS-IS 层获悉的 IP 前缀。
- （可选）**external** - 在配置 **suppress** 关键字后，将阻止通告从其他协议获悉的 IP 前缀。

此命令将强制 ASA 在其非伪节点 LSP 中设置过载位（也称为跳跃位）。通常，仅当 ASA 遇到问题时，才允许设置过载位。例如，当 ASA 遇到内存不足的问题时，可能是因为链路状态数据库不完整，这将导致路由表不完整或不准确。通过在其 LSP 中设置过载位，其他路由器可以在其 SPF 计算中忽略不可靠的路由器，直到该路由器从其问题中恢复过来。结果是该 IS-IS 区域中的其他路由器不会看到任何通过此路由器的路径。不过，IP 和 CLNS 前缀将直接连接到此路由器。

步骤 9 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 10 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 11 配置 BGP、Connected、IS-IS、OSPF 或 Static 路由重新分发：
redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric 编号

示例：

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number* - 指标的值。范围为 1 到 4294967295。

步骤 12 具体而言，将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级：

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag*]]

示例：

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2** - 重新分配 IS-IS 路由的来源和目标级别。
- **into** - 将正在重新分发的路由级别与将路由重新分发到的级别分隔开的关键字。
- （可选）**distribute-list** *list-number* - 控制 IS-IS 重新分发的分发列表数。您可以指定分发列表或路由映射，而不是同时指定两者。
- （可选）**route-map** *map-tag* - 控制 IS-IS 重新分发的路由映射的名称。您可以指定分发列表或路由映射，而不是同时指定两者。

注释
您必须指定 **metric-style wide** 命令才能使 **redistribute isis** 命令正常工作。请参阅此程序的第 1 步。

在 IS-IS 中，所有区域都是末节区域，这意味着不会将主干（第 2 级）中的任何路由信息泄漏到末节区域（第 1 级）。仅第 1 级路由器使用到其区域内最近的 Level 1-Level 2 路由器的默认路由。此命令使您可以将第 2 级 IP 路由重新分发到第 1 级区域。此重新分发使仅第 1 级路由器可以选择 IP 前缀的最佳路径来离开区域。这是一个仅 IP 功能，CLNS 路由仍为末节路由。

注释
要提高控制力和稳定性，您可以配置分发列表或路由映射，以控制可以重新分发到第 1 级的第 2 级 IP 路由。这使大型 IS-IS-IP 网络可以使用区域获得更好的可扩展性。

步骤 13 为 IS-IS IPv6 路由创建汇聚前缀：

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

示例：

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address* - X.X.X.X.::X/0-128 形式的 IPv6 前缀。
- （可选）**level-1** - 仅重新分发到第 1 级的路由通过配置的地址和掩码值汇总。
- （可选）**level-1-2** - 将路由重新分发到第 1 级和第 2 级 IS-IS，以及第 2 级 IS-IS 将第 1 级路由通告为在其区域内可访问时，会应用汇总路由。
- （可选）**level-2** - 第 1 级路由了解的路由通过配置的地址和掩码值汇总到第 2 级主干。重新分发到第 2 级 IS-IS 中的路由也会汇总。

监控 IS-IS

可以使用以下命令监控 IS-IS 路由进程。有关命令输出的示例和说明，请参阅命令参考。

监控 IS-IS 数据库

使用以下命令监控 IS-IS 数据库：

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** - 显示第 1 级、第 2 级 IS-IS 链路状态数据库，以及每个 LSP 的详细内容。
- **show isis database verbose** - 显示有关 IS-IS 数据库的详细信息，例如 LSP 的序列号、校验和以及保持时间。

监控 IS-IS 映射表条目

使用以下命令监控 IS-IS 主机名：

show isis hostname- 显示 IS-IS 路由器的路由器名称到系统 ID 映射表条目。

监控 IS-IS IPv4

使用以下命令监控 IS-IS IPv4：

- **show isis ip rib**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的 RIB。
- **show isis ip spf-log**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的 SPF 日志。
- **show isis ip topology**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的拓扑。
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示获知的 IS-IS 和安装的 IPv6 路由。
- **show isis ip unicast**- 显示 IPv4 地址系列特定的 RIB、SPF 日志以及 ISes 路径。

监控 IS-IS IPv6

使用以下命令监控 IS-IS IPv6：

- **show isis ipv6 rib**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的 RIB。
- **show isis ipv6 spf-log**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的 SPF 日志。

- **show isis ipv6 topology**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的拓扑。
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示获知的 IS-IS 和安装的 IPv6 路由。
- **show isis ipv6 unicast**- 显示 IPv6 地址系列特定的 RIB、SPF 日志以及 ISes 路径。

监控 IS-IS 日志

使用以下命令监控 IS-IS 日志：

- **show isis lsp-log**- 显示触发新 LSP 的接口的第 1 级和第 2 级 IS-IS LSP 日志。
- **show isis spf-log**- 显示 ASA 运行 SPF 计算的频率

监控 IS-IS 协议

使用以下命令监控 IS-IS 协议：

show clns protocol - 显示 ASA 上每个 IS-IS 路由进程的协议信息。

监控 IS-IS 邻居和路由

使用以下命令监控 IS-IS 邻居：

- **show isis topology** - 显示所有区域中所有连接的路由器的列表。此命令可验证所有区域中所有路由器的存在性及其连接性。
- **show isis neighbors [detail]** - 显示 IS-IS 邻接关系信息。
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**] - 显示终端系统 (ES)、中间系统 (IS) 和多拓扑 IS-IS (M-ISIS) 邻居。此命令显示通过 IPv6 的多拓扑 IS-IS 了解的邻接关系。
- **show clns is-neighbors** *[interface-name]* **[detail]** - 显示 IS-IS 设备邻接关系的 IS-IS 信息。

监控 IS-IS RIB

使用以下命令监控 IS-IS RIB：

- **show isis rib** [*ip-address* | *ip-address-mask*] - 显示特定路由或 RIB 中存储的主要网络下所有路由的路径。
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示本地重新分发缓存中的前缀。
- **show route isis** 显示路由表的当前状态。

监控 IS-IS 流量

使用以下命令监控 IS-IS 流量：

show clns traffic [since {bootup | show}] - 显示 ASA 已了解的 CLNS 流量统计信息。

调试 IS-IS

使用以下命令调试 IS-IS：

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]- 调试 IS-IS 路由协议的各个方面。

IS-IS 的历史记录

表 *1: IS-IS* 的功能历史记录

功能名称	平台版本	功能信息
IS-IS 路由	9.6(1)	ASA 现在支持中间系统到中间系统 (IS-IS) 路由协议。添加了对使用 IS-IS 路由协议进行路由数据、执行身份验证和重新分发及监控路由信息的支持。 引入了以下命令： **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

IS-IS 示例

本部分针对 IS-IS 的不同方面及介绍拓扑配置示例。

IS-IS 路由配置

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 路由配置

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

同一区域内的动态路由

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
```

```
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

多个区域内的动态路由

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
```

```
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

重叠区域内的动态路由

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
```

```
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301
```

```
oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

路由重分布

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
```

```
 isis priority 120


iRouter
interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

汇总地址

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis
```

```
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

被动接口

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
```

```
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis

iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis

oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis

oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

身份验证

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2
```

```
IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```

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。