路由模式接口和透明模式接口

本章介绍在路由或透明防火墙模式下为所有型号完成接口配置的相关任务。

注释 对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

关于路由和透明模式接口

ASA支持两种类型的接口：路由和桥接。

每个第 3 层路由接口都需要唯一子网上的一个 IP 地址。

桥接接口属于桥接组，且所有接口都在同一网络上。桥接组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。路由模式支持路由和桥接接口，您可以在路由接口和 BVI 之间路由。透明防火墙模式仅支持桥接组和 BVI 接口。

安全级别

每个接口都必须有一个0（最低）到100（最高）的安全级别，包括网桥组成员接口。例如，应将最安全的网络（如内部主机网络）分配至级别100。而连接到互联网的外部网络可分配至级别0。其他网络（例如 DMZ）可指定为介于中间的级别。您可以将多个接口分配至同一安全级别。

是否为 BVI 分配安全级别取决于防火墙模式。在透明模式下，BVI 接口没有安全级别，因为它没有参与接口之间的路由。在路由模式下，如果您选择在 BVI 和其他接口之间路由，则 BVI 接口就有安全级别。对于路由模式，网桥组成员接口的安全级别仅适用于网桥组内部的通信。类似地，BVI 安全级别仅适用于 BVI 间/第 3 层接口通信。

级别控制以下行为：

- 网络访问 - 默认情况下，默许从安全级别较高的接口访问安全级别较低的接口（出站）。较高安全级别接口上的主机可以访问较低安全级别接口上的任何主机。您可以通过将 ACL 应用于接口来限制访问。

  如果为相同安全级别的接口启用通信，那么就会隐式许可这些接口访问处于同一安全级别或更低安全级别的其他接口。

- 检测引擎 - 某些应用检测引擎依赖于安全级别。对于同一安全级别的接口，检测引擎适用于任意方向的流量。
  - NetBIOS 检测引擎 - 仅应用于出站连接。
  - SQL*Net 检测引擎 - 如果 SQL*Net（之前称为 OraServ）端口的控制连接存在于主机对之间，则只有入站数据连接允许通过 ASA。

双 IP 堆栈（IPv4 和 IPv6）

ASA在接口上同时支持 IPv6 和 IPv4 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

31 位子网掩码

对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

31 位子网和集群

您可以在跨集群模式下使用 31 位子网掩码用于，但管理接口和集群控制链路除外。

在单集群模式下，在任何接口上都不能使用 31 位子网掩码。

31 位子网和故障转移

进行故障转移时，如果为 ASA 接口 IP 地址使用 31 位子网，则无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障转移的接口应有一个备用 IP 地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用 IP 地址，ASA 无法执行任何网络测试；只能跟踪链路状态。

对于故障转移和可选的独立状态链路（点对点连接），也可以使用 31 位子网。

31 位子网和管理

如果您有直接连接的管理工作站，则对于 ASA 的 SSH 或 HTTP，或管理工作站上的 SNMP 或 Syslog，可使用点对点连接。

31 位子网不支持的功能

以下功能不支持 31 位子网：

- 网桥组的 BVI 接口 - 网桥组需要至少 3 个主机地址：BVI 和连接到两个网桥组成员接口的两台主机。您必须使用 /29 子网或更小的子网。
- 组播路由

路由和透明模式接口准则和限制

情景模式

- 在多情景模式下，您只能配置已根据配置多情景分配给系统配置中的情景的情景接口。
- 在多情景模式下不支持 PPPoE。
- 对于透明模式下的多情景模式，每个情景必须使用不同的接口；不能跨情景共享接口。
- 对于透明模式下的多情景模式，每个情景通常使用不同子网。您可以使用重叠子网，但是从路由角度而言，需要路由器和 NAT 配置才能实现网络拓扑。
- 多情景模式不支持 DHCPv6 和前缀委派选项。
- 在路由防火墙模式下，多情景模式中不支持网桥组接口。

故障转移、 集群

- 请勿采用本章中的程序配置故障转移接口。有关详细信息，请参阅故障转移。
- 对于集群接口，请参阅“集群”一章了解要求。
- 在使用故障转移时，则必须为数据接口手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。

IPv6

- 所有接口上都支持 IPv6。
- 只能在透明模式下手动配置 IPv6 地址。
- ASA 不支持 IPv6 任播地址。
- 多情景模式、透明模式、集群或故障转移不支持 DHCPv6 和前缀委派选项。

型号准则

- 对于 ASAv50，在透明或路由模式不支持桥接组。
- 对于 Firepower 2100 系列，在路由模式下不支持网桥组。

透明模式和网桥组准则

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- ASA不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 ASA。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 ASAv50，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 2100 系列，在路由模式下不支持网桥组。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。200
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，管理接口不支持 PPPoE。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，ASA - 不支持将 EtherChannel 和 VNI 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 ASA。如果 ASA 的一端有两个邻居运行 BFD，则 ASA 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

默认安全级别

默认安全级别为0。如果将一个接口命名为“inside”，且未明确设置安全级别，则ASA将安全级别设置为 100。

注释 如果更改接口的安全级别，且不希望等待现有连接超时后才使用新安全信息，则可使用 **clear conn** 命令清除连接。

其他准则和要求

- ASA 仅支持数据包中的一个 802.1Q 报头，不支持的多个报头（称为 QinQ 支持）。
- 接口问题（例如频繁的启动/关闭状态更改）会导致浮动连接计时器无法正确应用于通过接口的连接。如果接口状态有问题，可考虑在状态稳定后清除所有连接，以清除无效连接。

配置路由模式接口

要配置路由模式接口，请执行以下步骤：

配置常规路由模式接口参数

此程序介绍如何设置名称、安全级别、IPv4 地址和其他选项。

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 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **port-channel**
- *physical* - 例如，**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management**。请参阅您的型号的硬件安装指南以获取接口名称。

- *physical*.*subinterface* - 例如，**gigabitethernet0/0.100**。
- **vni**
- **vlan**
- 环回
- *mapped_name* - 适用于多情景模式。

注释
对于 Firepower 1010，不能将交换机端口配置为路由模式接口。

步骤 2 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 3 使用以下其中一种方法设置 IP 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址；不支持 DHCP 和 PPPoE。

- 手动设置 IP 地址：

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  备用 *ip_address* 参数用于故障转移。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在这种情况下，不会为网络或广播地址预留 IP 地址。在此情况下，无法设置备用 IP 地址。

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

注释
如果在输入 **ip address dhcp** 命令之前没有使用 **no shutdown** 命令启用接口，某些 DHCP 请求可能无法发送。

- 从 PPPoE 服务器获取 IP 地址：

  ip address pppoe [**setroute**]

  示例：

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  您可以通过手动输入 IP 地址 来选择启用 PPPoE。

  ip address *ip_address mask* **pppoe**

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
  ```

  Setroute 选项设置 PPPoE 客户端尚未建立连接时的默认路由。使用 **setroute** 选项时，无法在配置中使用 静态定义的路由。

  注释
  如果在两个接口（例如主用接口和备用接口）上都启用了 PPPoE，但未配置双重 ISP 支持，则 ASA 只能通过第一个接口发送流量来获取 IP 地址。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为介于 0（最低）到 100（最高）之间的整数。

注释
对于环回接口，不要设置安全级别，因为该接口仅支持进出设备的流量。

步骤 5 （可选）将接口设置为管理专属模式，以便其不允许流量通过。

management-only

默认情况下，管理接口配置为管理专属。

注释
对于环回接口，不要设置管理模式，因为该接口仅支持传入/传出设备的流量。

示例

以下示例为 VLAN 101 配置参数：

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

以下示例在多情景模式下为情景配置进行参数配置。接口 ID 是一个映射名称。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

相关主题

配置 IPv6 寻址，第 15 页
启用物理接口和配置以太网参数
配置 PPPoE，第 8 页

配置 PPPoE

如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，请配置以下参数。

过程

步骤 1 定义您选择的虚拟专用拨号网络 (VPDN) 组名称来表示此连接：

vpdn group *group_name* **request dialout pppoe**

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

步骤 2 如果 ISP 要求身份验证，请选择身份验证协议：

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

针对 ISP 所使用的身份验证类型输入相应的关键字：

使用 CHAP 或 MS-CHAP 时，用户名可能是指远程系统名称，而密码可能是指 CHAP 密钥。

步骤 3 将 ISP 分配的用户名关联到 VPDN 组：

vpdn group *group_name* **localname** *username*

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

步骤 4 为 PPPoE 连接创建用户名和密码对：

vpdn username *username* **password** *password* [**store-local**]

示例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local 选项可在 ASA 上 NVRAM 的特殊位置存储用户名和密码。如果自动更新服务器向 ASA 发送 **clear config** 命令，然后连接中断，ASA 可从 NVRAM 读取用户名和密码并重新进行身份验证来连接访问集中器。

配置网桥组接口

网桥组是指 ASA 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。有关网桥组的详细信息，请参阅 关于网桥组。

要配置网桥组和关联接口，请执行以下步骤。

配置网桥虚拟接口 (BVI)

每个网桥组都需要一个您应为其配置 IP 地址的 BVI。ASA 使用该 IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与所连接的网络位于同一子网。对于 IPv4 流量，任何流量的传递都需要使用 BVI IP。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。

对于路由模式，如果为 BVI 提供一个名称，则 BVI 将参与路由。如果不提供名称，网桥组在透明防火墙模式下将保持隔离状态。

某些型号的默认配置中包括一个网桥组和 BVI。您可以创建其他网桥组和 BVI，并可以在组之间重新分配成员接口。

注释 对于透明模式（适用于受支持的型号）下单独的管理接口，系统会向您的配置自动添加一个不可配置的网桥组 (ID 301)。此网桥组未包含在网桥组限制中。

过程

步骤 1 创建 BVI：

interface bvi *bridge_group_number*

示例：

```
ciscoasa(config)# interface bvi 2
```

bridge_group_number 是介于 1 和 250 之间的整数。稍后，您会将物理接口分配给此网桥组编号。

步骤 2 （透明模式）为 BVI 指定 IP 地址：

ip address *ip_address* [*mask*] [**standby** *ip_address*]

示例：

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

请勿为 BVI 分配主机地址（/32 或 255.255.255.255）。此外，也不要使用所含主机地址数小于 3（上游路由器、下游路由器和 BVI 各一个）的其他子网，例如 /30 子网 (255.255.255.252)。ASA 会丢弃传入子网中第一个和最后一个地址或从其传出的所有 ARP 数据包。因此，如果您使用 /30 子网，并从该子网中为上游路由器分配了一个预留地址，那么ASA将丢弃从下游路由器发送至上游路由器的 ARP 请求。

standby 关键字和地址用于故障转移。

步骤 3 （路由模式）使用以下方法之一设置 IP 地址：

要用于故障转移和集群，您必须手动设置 IP 地址；不支持 DHCP。

- 手动设置 IP 地址：

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  备用 *ip_address* 参数用于故障转移。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

- 从 DHCP 服务器获取 IP 地址。

ip address dhcp [**setroute**]

示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入 **ip address dhcp** 命令之前没有使用 no shutdown 命令启用接口，某些 DHCP 请求可能无法发送。

步骤 4 （路由模式）为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

如果要在网桥组成员之外路由流量，例如路由到外部接口或其他网桥组的成员，则必须为 BVI 命名。*name* 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 5 （路由模式）设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

示例

以下示例设置 BVI 2 地址和备用地址：

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

配置常规网桥组成员接口参数

此程序描述如何为每个网桥组成员接口设置名称、安全级别和网桥组。

开始之前

- 同一网桥组可以包括不同类型的接口：物理接口、VLAN 子接口、VNI 接口和 EtherChannel 接口。管理接口不受支持。 在路由模式下，不支持 EtherChannels 和 VNI。
- 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。
- 对于透明模式，请勿为管理接口使用此程序；请参阅为透明模式配置管理接口，第 13 页配置管理接口。

过程

步骤 1 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **port-channel**
- *physical*—For example, **ethernet**, **gigabitethernet**, **tengigabitethernet**. 管理接口不受支持。请参阅您的型号的硬件安装指南以获取接口名称。
- *physical_or_port-channel.subinterface* - 例如，**gigabitethernet0/0.100**或 **port-channel1.100**。
- **vni**
- **vlan**
- *mapped_name* - 适用于多情景模式。

注释
对于 Firepower 1010，不能将交换机端口配置为网桥组成员。

您不能将逻辑 VLAN 接口和物理路由器接口混合在同一个网桥组中。

注释
在路由模式下，不支持将 **port-channel**和 **VNI** 接口作为网桥组成员。

步骤 2 向网桥组分配接口：

bridge-group 编号

示例：

```
ciscoasa(config-if)# bridge-group 1
```

编号为 1 到 250 之间的整数，必须与 BVI 接口编号匹配。最多可将 64 个接口分配到网桥组。您不能将同一接口分配至多个网桥组。

步骤 3 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside1
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为介于 0（最低）到 100（最高）之间的整数。

相关主题

配置、MTU和 TCP MSS

为透明模式配置管理接口

在透明防火墙模式下，所有接口必须属于网桥组。唯一例外的是管理接口（物理接口、子接口（如果您的型号支持）或由管理接口组成的 EtherChannel 接口（如果您有多个管理接口）），您可以将其配置为单独的管理接口；对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。您不能将任何其他接口类型用作管理接口。您可以在单模式下或为每个情景配置一个管理接口。有关详细信息，请参阅透明模式下的管理接口。

管理接口仅适用于传入和传出设备的流量，不能通过流量。

开始之前

- 请勿将此接口分配给网桥组；不可配置的网桥组 (ID 301) 将自动添加到您的配置中。此网桥组未包含在网桥组限制中。
- 对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。
- 在多情景模式下，您无法跨情景共享任何接口，包括管理接口。您必须连接到数据接口。
- 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，请在。

过程

步骤 1 进入接口配置模式：

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

示例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 参数是 EtherChannel 接口 ID，例如 **port-channel 1**。EtherChannel 接口只能拥有管理成员接口。

在多情景模式下，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。

对于 Firepower 4100/9300 机箱，指定分配给 ASA 逻辑设备的管理类型接口（单独或 EtherChannel）的接口 ID。

步骤 2 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif management
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 3 使用以下其中一种方法设置 IP 地址。

- 手动设置 IP 地址：

  要用于故障转移，您必须手动设置 IP 地址和备用地址；不支持 DHCP。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

  备用 *ip_address* 参数用于故障转移。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入 **ip address dhcp** 命令之前没有使用 no shutdown 命令启用接口，某些 DHCP 请求可能无法发送。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 100
```

number 为 0（最低）到 100（最高）之间的整数。

配置 IPv6 寻址

此部分介绍如何配置 IPv6 寻址。

关于 IPv6

本节包括关于 IPv6 的信息。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要为 BVI（而不必为每个成员接口）配置此地址。还可以为透明模式下的管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或邻居发现功能，例如地址解析。在网桥组中，只有成员接口具有链路本地地址；BVI 没有链路本地地址。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。对于网桥组成员接口，在 BVI 上配置全局地址时，ASA 将为成员接口自动生成链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

注释 如果希望仅配置链路本地地址，请参阅命令参考中的**ipv6 enable**（自动配置）或**ipv6 address link-local**（手动配置）命令。

修改的 EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址（以二进制值 000 开头的地址除外）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。ASA 可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。

配置 IPv6 前缀代理客户端

ASA 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 ASA 可以将这些前缀通过子网分配到其内部接口。

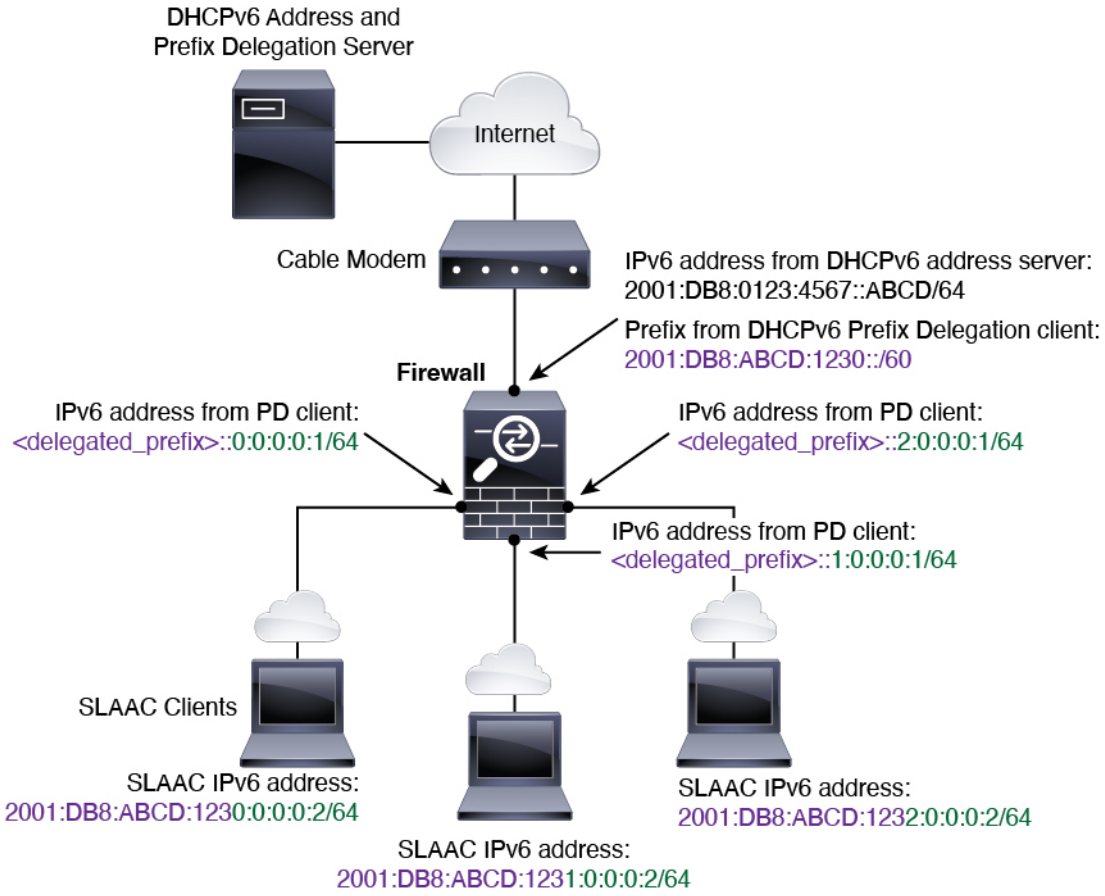
关于 IPv6 前缀授权

ASA 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 ASA 可以将这些前缀通过子网分配到其内部接口。然后，连接到内部接口的主机可以使用无状态地址自动配置 (SLAAC) 获取全局 IPv6 地址。请注意，内部 ASA 接口不会依次充当前缀授权服务器；ASA 只能向 SLAAC 客户端提供全局 IP 地址。例如，如果路由器连接到 ASA，它可以作为 SLAAC 客户端获取其 IP 地址。但是，如果您要为路由器后的网络使用授权的前缀的子网，则必须在路由器的内部接口上手动配置这些地址。

ASA 中包括一个轻型 DHCPv6 服务器，以便 SLAAC 客户端在向 ASA 发送信息请求 (IR) 数据包时，ASA 可以向这些客户端提供 DNS 服务器和域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

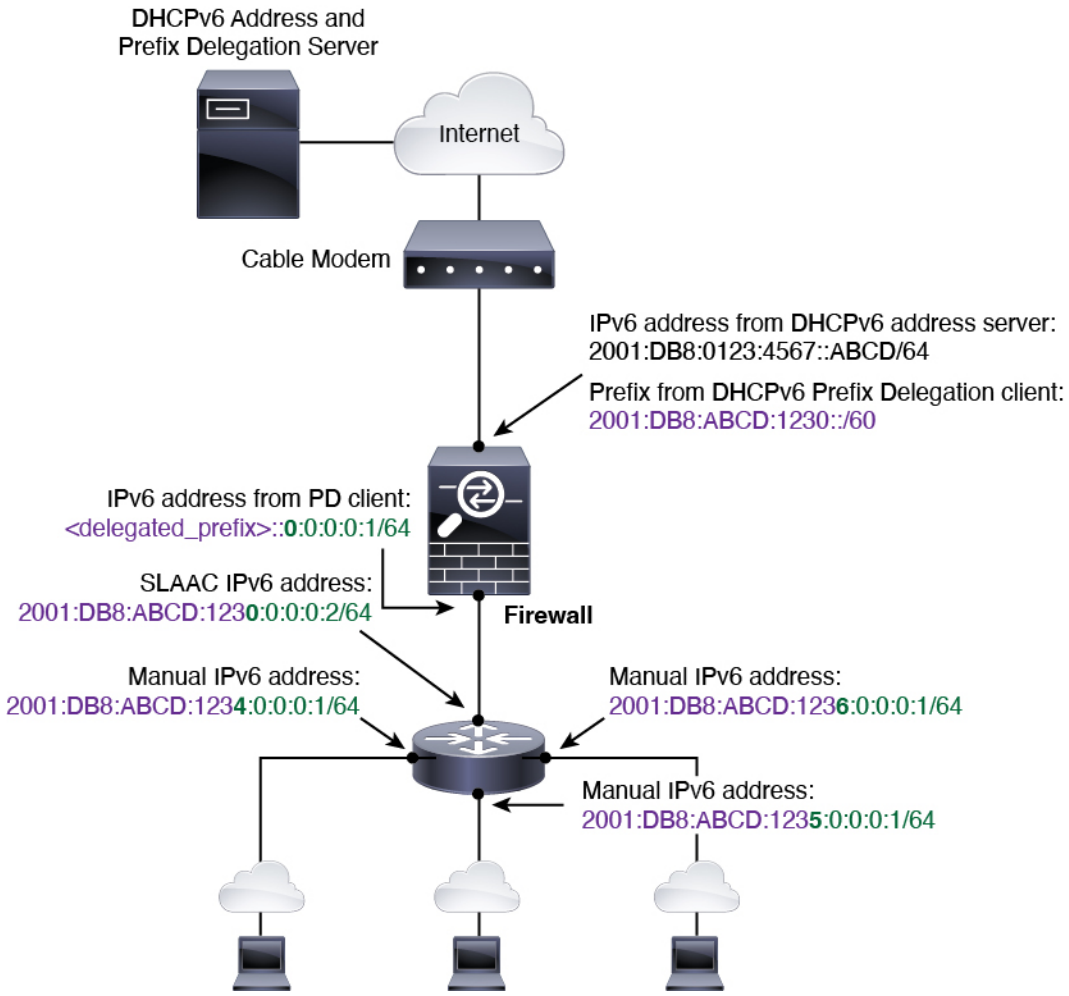
IPv6 前缀授权 /64 子网示例

以下示例显示使用 DHCPv6 地址客户端在外部接口上接收 IP 地址的 ASA。此外，它还会使用 DHCPv6 前缀授权客户端获得一个授权的前缀。ASA 将授权的前缀编入 /64 网络的子网，并使用授权的前缀以及手动配置的子网（::0、::1 或 ::2）和每个接口上的 IPv6 地址 (0:0:0:1) 为其内部接口动态分配全局 IPv6 地址。连接至这些内部接口的 SLAAC 客户端将获得每个 /64 子网上的 IPv6 地址。



IPv6 前缀委派 /62 子网示例

以下示例显示了 ASA 将前缀子网划分到 4 个 /62 子网中:2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62 和 2001:DB8:ABCD:123**C**::/62。ASA 将 2001:DB8:ABCD:1230::/62 上 4 个可用 /64 子网之一用于其内部网络 (::0)。随后您可以手动将其他 /62 子网用于下游路由器。所示的路由器将 2001:DB8:ABCD:1234::/62 上 4 个可用 /64 子网中的 3 个用于其内部接口（::4、::5 和 ::6）。在此情况下，内部路由器接口无法动态获取委派的前缀，因此您需要在 ASA 上查看委派的前缀，然后将该前缀用于您的路由器配置。通常，当租约到期时，ISP 会将同一前缀委派给指定客户端，但如果 ASA 收到新前缀，则您必须修改路由器配置以使用该新前缀。DHCP 唯一标识符 (DUID) 在重新启动时会保持不变。



启用 IPv6 前缀授权客户端

在一个或多个接口上启用 DHCPv6 前缀代理客户端。ASA 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 ASA 接口才能使用代理前缀衍生的地址。

开始之前

- 此功能仅支持路由防火墙模式。
- 此功能不支持多情景模式。
- 此功能不支持集群。
- 无法在仅管理接口上配置此功能。
- 当您使用前缀代理时，必须将 ASA IPv6 邻居发现路由器通告间隔设置为远低于 DHCPv6 服务器分配的前缀的首选有效期，以防 IPv6 流量中断。例如，如果 DHCPv6 服务器将首选前缀代理有效期设置为 300 秒，则您应将 ASA RA 间隔设置为 150 秒。要设置首选有效期，请使用 **show**

ipv6 general-prefix 命令。要设置 ASA RA 间隔，请参阅配置 IPv6 邻居发现，第 22 页；默认值为 200 秒。

过程

步骤 1 对于连接到 DHCPv6 服务器网络的接口，请进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

步骤 2 启用 DHCPv6 前缀代理客户端，并为在此接口上获取的前缀命名：

ipv6 dhcp client pd 名称

示例：

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

name 最长为 200 个字符。

步骤 3 提供有关要接收的代理前缀的一项或多项提示：

ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

示例：

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

通常，您需要请求特定的前缀长度（例如 ::/60），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

步骤 4 请参阅配置全局 IPv6 地址，第 20 页为 ASA 接口分配作为全局 IP 地址的前缀子网。

步骤 5 （可选） 请参阅配置 DHCPv6 无状态服务器为 SLAAC 客户端提供域名和服务器参数。

步骤 6 （可选） 请参阅配置 IPv6 网络设置通告包含 BGP 的前缀。

示例

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
```

```
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

配置全局 IPv6 地址

要为任何路由模式接口和透明或路由模式 BVI 配置全局 IPv6 地址，请执行以下步骤。

多情景模式不支持 DHCPv6 和前缀代理选项。

注释 配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。对于网桥组，在 BVI 上配置全局地址会自动在所有成员接口上配置链路本地地址。

对于子接口，建议您同样手动设置 MAC 地址，这是因为它们使用父接口上相同的固化 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。请参阅 手动配置 MAC 地址。

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 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

在透明模式或路由模式下，为网桥组指定 BVI：

示例：

```
ciscoasa(config)# interface bvi 1
```

在透明模式下，除了 BVI 之外，您还可以指定管理接口：

示例：

```
ciscoasa(config)# interface management 1/1
```

步骤 2 （路由接口）使用以下方法之一设置 IP 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址。对于集群，不支持手动配置链路本地地址。

- 在接口上启用无状态地址自动配置 (SLAAC)：

  ipv6 address autoconfig [**default trust** {**dhcp** | **ignore**}]

  在接口上启用 SLAAC 会根据路由器通告消息中收到的前缀配置 IPv6 地址。启用 SLAAC 时，会基于修改的 EUI-64 接口 ID 为接口自动生成链路本地地址。

  注释
  尽管 RFC 4862 规定配置为 SLAAC 的主机不发送路由器通告消息，但在这种情况下，ASA 会发送路由器通告消息。要抑制消息，请参阅 **ipv6 nd suppress-ra** 命令。

  如果要安装默认路由，请指定 **default trust dhcp** 或 **ignore**。**dhcp** 指定 ASA 仅使用源自受信任源（即源自提供 IPv6 地址的同一台服务器）的路由器通告的默认路由。**ignore** 指定路由器通告可以源自其他网络，这种方法风险可能要高一些。

- 使用 DHCPv6 获取地址：

  ipv6 address dhcp [**default**]

  示例：

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  default 关键字从路由器通告获取默认路由。

- 手动为接口分配全局地址：

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  分配全局地址时，将为接口自动创建 链路本地地址。

  standby 指定辅助设备或故障转移对中的故障转移组 使用的接口地址。

- 通过将指定前缀与使用 Modified EUI-64 格式从接口 MAC 地址生成的接口 ID 配合使用，来为接口分配全局地址。

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

分配全局地址时，将为接口自动创建 链路本地地址。

您不需要指定备用接口；接口 ID 将会自动生成。

- 使用授权的前缀：

  ipv6 address *prefix_name ipv6_address/prefix_length*

  示例：

  ```
  ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ```

  此功能要求 ASA 在不同接口上启用 DHCPv6 前缀授权客户端。请参阅 启用 IPv6 前缀授权客户端，第 18 页。通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:Db8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。

步骤 3 （BVI 接口）为 BVI 手动分配全局地址。对于透明模式下的管理接口，也请使用此方法。

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

示例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

分配全局地址时，将为接口自动创建 链路本地地址。

standby 指定辅助设备或故障转移对中的故障转移组 使用的接口地址。

步骤 4 （可选）在本地链路上的 IPv6 地址中，强制使用修改的 EUI-64 格式的接口标识符。

ipv6 enforce-eui64 *if_name*

示例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 参数是 **nameif** 命令所指定的接口的名称，您将在此接口上启用地址格式执行。

配置 IPv6 邻居发现

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络（本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点（主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可访问及哪些邻居不可访问，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

过程

步骤 1 指定要配置的 IPv6 接口。

interface *name*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

步骤 2 指定重复地址检测 (DAD) 尝试的次数 。

ipv6 nd dad attempts *value*

value 参数的有效值范围为 0 至 600。0 值可在指定的接口上禁用 DAD 处理。默认值为 1 条消息。

DAD 确保新的单播 IPv6 地址在分配之前的唯一性，并确保按链路检测网络中的重复 IPv6 地址。ASA 使用邻居请求消息来执行 DAD。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。

示例：

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

步骤 3 设置 IPv6 邻居请求重新传输的间隔时间。

ipv6 nd ns-interval *value*

value 参数的值范围为 1000 到 3600000 毫秒。

邻居请求消息（ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息（ICPMv6 类型 136）作出应答。

源节点接收邻居通告后，源节点与目标节点即可通信。识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可访问性。当节点要验证邻居的可访问性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。

示例：

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

步骤 4 设置远程 IPv6 节点可访问的时间量。

ipv6 nd reachable-time *value*

value 参数的值范围为 0 到 3600000 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

示例：

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

步骤 5 设置 IPv6 路由器通告传输之间的时间间隔。

ipv6 nd ra-interval [**msec**] *value*

msec 关键字指示提供的值以毫秒为单位。如果此关键字不存在，则提供的值以秒为单位。*value* 参数的有效值范围介于 3 到 1800 秒之间；如果提供了 **msec** 关键字，则范围介于 500 到 1800000 毫秒之间。默认值为 200 秒。

时间间隔值包括在发送出此接口的所有 IPv6 路由器通告中。

如果将 ASA 配置为默认路由器，则传输之间的时间间隔应小于或等于 IPv6 路由器通告有效期。

为防止与其他 IPv6 节点同步，ASA 会随机调整您设置的值（抖动）。

示例：

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

步骤 6 指定本地链路上的节点应将 ASA 视为链路上默认路由器的时间长度。

ipv6 nd ra-lifetime [**msec**] *value*

可选的 **msec** 关键字指示提供的值以毫秒为单位。如未指定，则该值以秒为单位。*value* 参数的值范围为 0 到 9000 秒。输入 0 表示不应将 ASA 视为选定接口的默认路由器。

路由器有效期值包括在发送出接口的所有 IPv6 路由器通告中。此值表示 ASA 作为此接口的默认路由器的益处。

示例：

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

步骤 7 抑制路由器通告。

ipv6 nd suppress-ra

路由器通告消息（ICMPv6 类型 134）会自动发送，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

在不希望 ASA 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

输入此命令会导致 ASA 显示为链路上的常规 IPv6 邻居，而不是显示为 IPv6 路由器。

步骤 8 在 IPv6 路由器通告中添加一个标志，通知 IPv6 无状态地址自动配置 (SLAAC) 客户端，除了派生的 SLAAC 地址外，还使用 DHCPv6 获取 IPv6 地址。

ipv6 nd managed-config-flag

此选项在 IPv6 路由器通告数据包中设置托管地址配置标志。

步骤 9 在 IPv6 路由器通告中添加一个标志，通知 IPv6 SLAAC 客户端使用 DHCPv6 获取 DNS 服务器地址或其他信息。

ipv6 nd other-config-flag

此选项在 IPv6 路由器通告数据包中设置其他地址配置标志。

步骤 10 配置包含在 IPv6 路由器通告中的 IPv6 前缀：

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* | **default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

前缀通告可供邻居设备用于自动配置其接口地址。SLAAC 使用路由器通告消息中提供的 IPv6 前缀，从链路本地地址创建全局单播地址。

默认情况下，接口上使用 **ipv6 addres** 命令配置为地址的前缀在路由器通告中通告。如果使用 **ipv6 nd prefix** 命令为通告配置前缀，则仅通告这些前缀。

要使 SLAAC 正常工作，路由器通告消息中通告的前缀长度必须始终为 64 位。

- **default**- 表示使用默认前缀。
- *valid_lifetime preferred_lifetime* - 指定通告指定的 IPv6 前缀为有效前缀和首选前缀的时间量。地址在首选的有效期内没有任何限制。首选的有效期到期后，该地址会进入已弃用状态；对于已弃用状态的地址，虽然不推荐使用，但并未严格禁止。有效的有效期到期后，地址将变为无效状态，且无法使用。有效的有效期必须大于或等于首选的有效期。值范围为 0 秒至 4294967295 秒。最大值代表无穷大，也可以使用 **infinite** 关键字指定。有效的有效期默认值为 2592000（30 天）。首选的有效期默认值为 604800（7 天）。
- **at** *valid_date preferred_date* - 指示前缀到期的具体日期和时间。指定日期格式为 *month_name day hh*:*mm*。例如，输入 **dec 1 13:00**。
- **no-advertise**- 禁用前缀通告。对于 **default** 前缀，此设置仅适用于 on-link 前缀。除非您为特定 Off-link 前缀指定 **no-advertise**，否则系统仍将通告 Off-link 前缀。
- **no-autoconfig** - 指定该前缀不能用于 IPv6 SLAAC。
- **off-link**- 将指定的前缀配置为关闭链路。该前缀将在通告时清除 L-位。该前缀将不会作为已连接前缀插入到路由表。

在链路上打开（默认情况下）时，指定的前缀会分配给该链路。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可访问。

示例：

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

步骤 11 在 IPv6 邻居发现缓存中配置静态条目。

ipv6 neighbor *ipv6_address if_name mac_address*

以下准则和限制适用于配置静态 IPv6 邻居：

- **ipv6 neighbor** 命令类似于 **arp** 命令。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用复制命令存储配置时，这些条目存储在配置中。
- 使用 **show ipv6 neighbor** 命令可查看 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令可删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。**no ipv6 neighbor** 命令可从邻居发现缓存中删除指定的静态条目；该命令不会从缓存中删除动态条目，这些条目从 IPv6 邻居发现过程中获悉。使用 **no ipv6 enabl** 命令在接口上禁用 IPv6 可删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目（条目的状态更改为 INCMP [Incomplete]）除外。
- 邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令不会从 IPv6 邻居发现缓存中删除静态条目；仅会清除动态条目。
- IPv6 邻居条目的定期刷新生成了 ICMP 系统日志。IPv6 邻居条目的 ASA 默认计时器为 30 秒，因此，ASA 将大约每 30 秒生成 ICMPv6 邻居发现和响应数据包。如果 ASA 拥有用 IPv6 地址配置的故障转移 LAN 和状态接口，则 ASA 将每 30 秒为配置的和链路本地的 IPv6 地址生成 ICMPv6 邻居发现和响应数据包。此外，由于每个数据包将生成多个系统日志（ICMP 连接和本地主机创建或拆卸），因此，似乎一直在不断生成 ICMP 系统日志。可以在常规数据接口上配置 IPv6 邻居条目的刷新时间，但是，不可在故障转移接口上配置。但是，此 ICMP 邻居发现流量对 CPU 的影响最小。

示例：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

监控路由模式和透明模式接口

您可以监控接口统计信息、状态、PPPoE 。

注释 对于 Firepower 和 Cisco Secure Firewall 模型，某些统计信息未使用 ASA 命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

对于平台模式下的 Firepower 2100，另请参阅以下 FXOS connect local-mgmt 命令：

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

有关详细信息，请参阅 FXOS 故障排除指南。

接口统计信息和信息

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show bridge-group**

  显示网桥组信息，如分配的接口、MAC 地址和 IP 地址。

DHCP 信息

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 命令用于显示所有接口的 DHCPv6 信息。如果接口配置用于 DHCPv6 无状态服务器配置（请参阅配置 DHCPv6 无状态服务器），则此命令将列出该服务器正在使用的 DHCPv6 池。如果接口包含 DHCPv6 地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。对于特定接口，可以显示 DHCP 服务器或客户端的消息统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
```

```
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:
```

```
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client** [**pd**] **statistics**

  show ipv6 dhcp client statistics 命令用于显示 DHCPv6 客户端统计信息，并显示已发送和已接收的消息数量的输出结果。**show ipv6 dhcp client pd statistics** 命令显示前缀委派客户端统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                   8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                   1
```

```
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics 命令用于显示故障转移设备之间的事务处理统计信息，包括在DUID信息各个设备之间的同步次数。以下示例显示了此命令提供的信息。

  在主用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  在备用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

- **show ipv6 general-prefix**

  show ipv6 general-prefix 命令显示 DHCPv6 前缀委派客户端获得的所有前缀，该前缀到其他进程的 ASA 分发（“消费端列表”）。以下示例显示此命令提供的信息：

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
    BGP network command         1
    inside (Address command)    1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  显示当前 PPPoE 客户端配置信息。

- **debug pppoe** {**event** | **error** | **packet**}

  启用调试 PPPoE 客户端。

- **show vpdn session** [**l2tp** | **pppoe**] [**id** *sess_id* | **packets** | **state** | **window**]

  查看 PPPoE 会话的状态。

以下示例显示此命令提供的信息：

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 邻居发现

要监控 IPv6 邻居发现参数，请输入以下命令：

- **show ipv6 interface**

  此命令显示为 IPv6 配置的接口的可用性状态（包括接口名称，例如“outside”），并显示指定接口的设置。但是，它会从命令中排除名称并显示已启用 IPv6 的所有接口的设置。命令输出显示以下信息：

  - 接口的名称和状态。
  - 链路本地和全局单播地址。
  - 接口所属的组播组。
  - ICMP 重新定向和错误消息设置。
  - 邻居发现设置。
  - 命令设置为 0 时的实际时间。
  - 正在使用的邻居发现可访问时间。

路由和透明模式接口示例

包括 2 个网桥组的透明模式示例

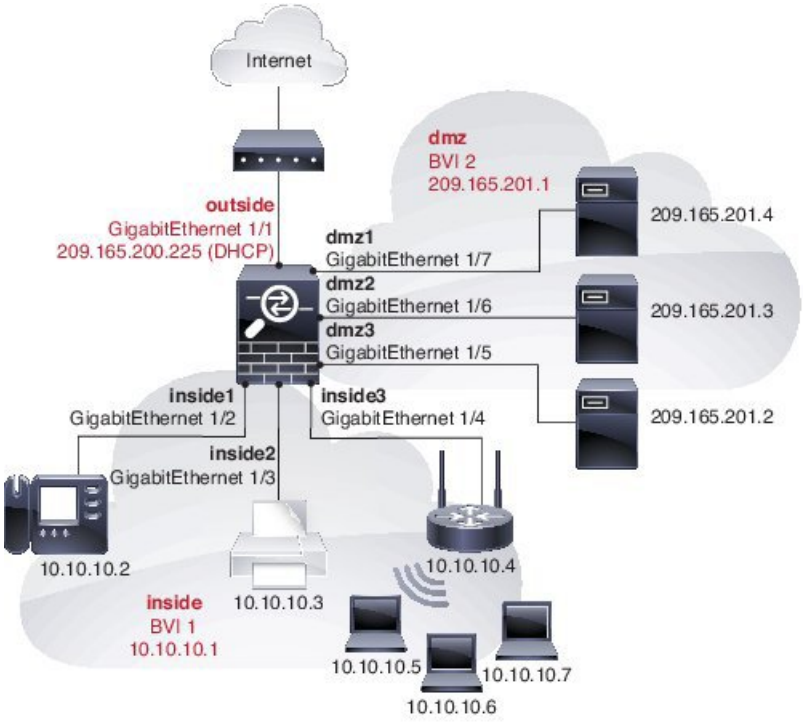
以下透明模式示例包括两个网桥组（每组三个接口）以及一个管理专属接口：

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

与 2 个网桥组的交换 LAN 网段示例

以下示例配置 2 个网桥组（每个网桥组包含 3 个接口）和一个用于 outside 的普通路由接口。在公共 Web 服务器中，网桥组 1 为 inside，网桥组 2 为 dmz。由于网桥组的每个成员属于同一安全级别，而且我们已启用同一安全通信，所以网桥组成员接口在网桥组内可以自由通信。虽然 inside 成员的安全级别为 100，dmz 成员的安全级别也是 100，但这些安全级别不适用于 BVI 间通信；只有 BVI

安全级别才会影响 BVI 间的流量。BVI 和 outside（100、50 和 0）的安全级别隐式允许 inside 到 dmz、inside 到 outside 以及 dmz 到 outside 的流量。向 outside 应用访问规则以允许流量流入 dmz 上的服务器。




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
```

```
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

路由模式和透明模式接口的历史记录

功能名称	平台版本	功能信息
IPv6 邻居发现	7.0(1)	引入了此功能。 引入了以下命令：**ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、**ipv6 enforce-eui64**。
透明模式的 IPv6 支持	8.2(1)	为透明防火墙模式引入了 IPv6 支持。
透明模式的网桥组	8.4(1)	如果您不希望产生安全情景开销，或者希望最大限度地利用安全情景，则可以将接口一起集合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量相互分隔。在单情景模式或每个情景中最多可配置八个网桥组，每组四个接口。 引入了以下命令：**interface bvi** 和 **show bridge-group**
IPv6 DHCP 中继的地址配置标志	9.0(1)	引入了以下命令：**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 个增加到 250 个网桥组。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 修改了以下命令：**interface bvi**、**bridge-group**
每个桥接组的透明模式最大接口数增加到 64	9.6(2)	每个网桥组的最大接口数量已从 4 增加到 64。 未修改任何命令。

功能名称	平台版本	功能信息
IPv6 DHCP	9.6(2)	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 引入或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
集成的路由与桥接	9.7(1)	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

功能名称	平台版本	功能信息
31 位子网掩码	9.7(1)	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。网桥组或组播路由的 BVI 不支持此功能。 修改了以下命令：**ip address**、**http**、**logging host**、**snmp-server**、**ssh**

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。