路由概述

本章介绍有关路由如何在 ASA 内部运行。

确定路径

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

注释 在多情景模式下，仅主用/主用故障转移支持非对称路由。

支持的路由类型

路由器可以使用多种路由类型。ASA 使用以下路由类型：

- 静态与动态
- 单路径与多路径
- 平面与分层
- 链路状态与距离矢量

静态与动态

静态路由算法实际上是网络管理员建立的表映射。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改，则路由软件会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器（所有无法路由的数据包都发送到的路由器的默认路由）指定为所有无法路由的数据包的存储库，从而确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器从最后一个主干路由器传播到最终目标。

路由系统通常会指定一些逻辑节点组，称为域、自治系统或区域。在分层系统中，一个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组（域）中。由于域内路由器只需知道其域中的其他路由器即可，因此可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离矢量

链路状态算法（也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与OSPF路由协议结合使用。

支持的互联网路由协议

ASA 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP（反之亦然），从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网服务提供商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

- 中间系统到中间系统 (IS-IS)

  IS-IS 是链路状态内部网关协议 (IGP)。链路状态协议的主要特点是：传播所需的信息以在每个参与的路由器上建立完整网络连接映射。然后，该映射会用于计算到目标的最短路径。

路由表

ASA对数据流量（通过设备）和管理流量（来自设备）使用单独的路由表。本部分介绍路由表的工作原理。有关管理路由表的信息，另请参阅 管理流量的路由表，第 9 页。

路由表的填充方式

ASA 路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于 ASA 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 ASA 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果ASA设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 ASA在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 ASA支持的路由协议的默认管理距离值。

表 *1:* 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
VPN 路由	1
静态路由	1

路由源	默认管理距离
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 ASA从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 ASA 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 ASA会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 ASA的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 ASA上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

动态路由和故障转移

当主用设备上的路由表发生更改时，在备用设备上同步动态路由。这意味着主用设备上的所有添加、删除或更改都将立即传播到备用设备。如果备用设备在主用/备用就绪 故障转移对中处于活动状态，则它会有与前一个主用设备相同的路由表，因为路由作为 故障转移批量同步和连续复制过程的一部分进行同步。

动态路由和集群

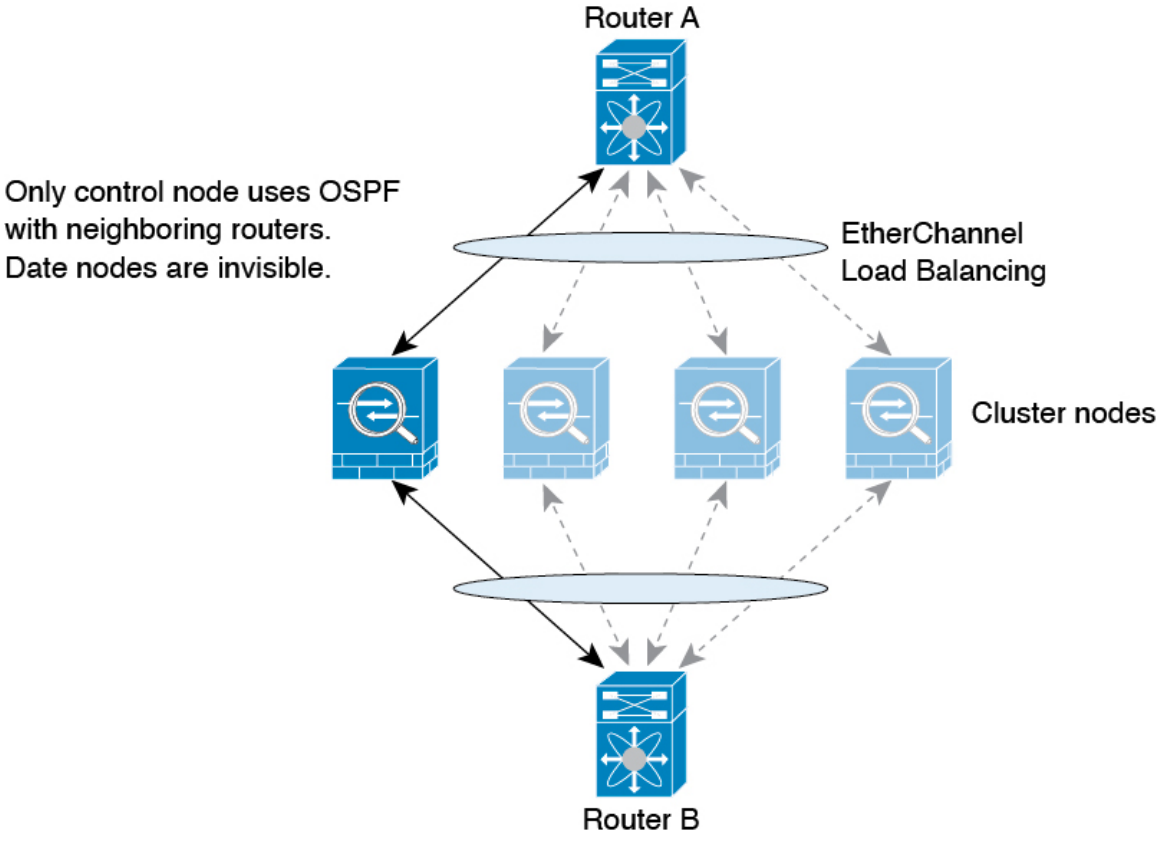
本部分介绍如何使用动态路由和集群。

跨区以太网通道模式下的动态路由

注释 跨区以太网通道模式不支持 IS-IS。

在跨区以太网通道模式下：路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *1:* 跨区以太网通道模式下的动态路由



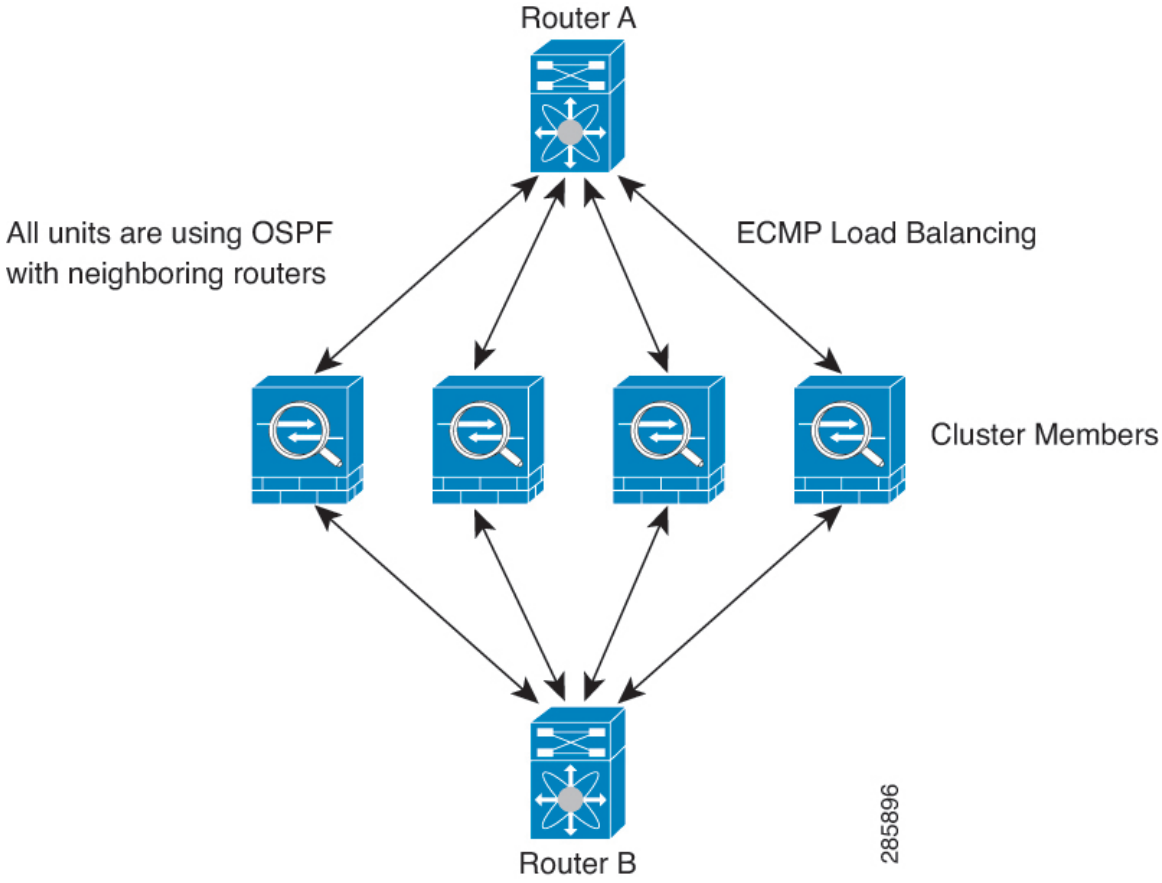
在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *2:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一台 ASA。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每台 ASA 在与外部路由器通信时，会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些ASA接口分组到同一流量区域中。请参阅配置流量区域。

多情景模式下的动态路由

在多情景模式下，每个情景维护单独的路由表和路由协议数据库。因而您可以在每个情景中独立配置 OSPFv2 和 EIGRP。您可以在某些情景中配置 EIGRP，并在相同或不同的情景中配置 OSPFv2。在混合情景模式下，您可以在处于路由模式下的情景中启用任何动态路由协议。在多情景模式下，不支持 RIP 和 OSPFv3。

下表列出了 EIGRP 及 OSPFv2 的属性、用于将路由分发到 OSPFv2 和 EIGRP 进程中的路由映射、以及在 OSPFv2 中用于筛选路由更新（多情景模式下进入或离开某个区域）的前缀列表：

EIGRP	OSPFv2	路由映射和前缀列表
每个情景支持一个实例。	每个情景支持两个实例。	N/A
在系统情景中禁用。		N/A
两个情景可能使用相同或不同的自治系统编号。	两个情景可能使用相同或不同的区域 ID。	N/A
两个情景的共享接口可能会运行多个 EIGRP 实例。	两个情景的共享接口可能会运行多个 OSPP 实例。	N/A
支持跨共享接口的 EIGRP 实例交互。	支持跨共享接口的 OSPFv2 实例交互。	N/A
在单模式下可用的所有 CLI 在多情景模式下也可用。		
每个 CLI 仅在对其进行了使用的情景中起作用。		

路由资源管理

资源类（称为路由）指定可存在于情景中的路由表条目的最大数量。这可解决一个情景影响另一个情景中的可用路由表条目的问题，您也可以对每个情景的最大路由条目数进行更好的控制。

由于没有明确的系统限制，因此只能为此资源限制指定绝对值，不能使用百分比限制。此外，每个情景没有最小限制和最大限制，因此默认类不会进行更改。如果您在某个情景中为静态或动态路由协议（已连接、静态、OSPF、EIGRP 和 RIP）添加新的路由，但情景的资源限制已被耗尽，则路由添加失败，并会生成系统日志消息。

管理流量的路由表

作为一项标准安全实践，通常需要将管理（关联设备）流量与数据流量分开并隔离。要实现这种隔离，ASA 设备为管理专用流量和数据流量使用单独的路由表。单独的路由表意味着您也可以创建用于数据和管理的单独默认路由。

每个路由表的流量类型

关联设备流量始终使用数据路由表。

关联设备流量（根据类型）在默认情况下使用管理专用路由表或数据路由表。如果在默认路由表中找不到匹配项，则会检查其他路由表。

- 管理专用路由表关联设备流量包括使用 HTTP、SCP、TFTP、**copy** 命令、智能许可、Smart Call Home、**trustpoint**、**trustpool**等打开远程文件的功能。
- 数据路由表关联设备流量包括所有其他功能，如 ping、DNS、DHCP 等。

管理专用路由表中包含的接口

管理专用接口包括所有 管理 x/x 接口以及您配置为管理专用接口的所有接口。

回退到其他路由表

如果在默认路由表中找不到匹配项，则会检查其他路由表。

使用非默认路由表

如果您需要传出流量退出默认路由表中不存在的接口，则您可能需要在配置接口时指定接口，而不是依赖于回到另一个表。ASA 仅检查指定接口的路由。例如，如果需要 ping 命令来退出管理专用接口，请在 ping 函数中指定该接口。否则，如果数据路由表中具有默认路由，则将匹配默认路由且绝不回到管理路由表。

动态路由

管理专用路由表支持独立于数据接口路由表的动态路由。给定的动态路由进程必须在管理专用接口或数据接口上运行；不能将两种类型混用。 当不使用单独的管理路由表从早期版本升级时，如果混用使用同一动态路由进程的数据接口和管理接口，则管理接口将被丢弃。

面向 VPN 要求的管理访问功能

如果配置了管理访问功能，以允许对使用 VPN 时并非从其进入 ASA 的接口进行管理访问，那么由于使用单独的管理和数据路由表所带来的路由顾虑，VPN 终端接口和管理访问接口需要为同一类型：二者需要同为管理专用接口或普通数据接口。

管理接口识别

配置为仅管理的接口被视为管理接口。

在以下配置中，GigabitEthernet0/0 和 Management0/0 接口被视为管理接口。

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

等价多路径 (ECMP) 路由

ASA支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。ASA使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

禁用代理 ARP 请求

当主机将IP流量发送到同一以太网网络上的其他设备时，该主机需要知道该设备的MAC地址。ARP是一个第 2 层协议，用于将 IP 地址解析为 MAC 地址。主机发送 ARP 请求，询问“谁有此 IP 地址？”拥有该 IP 地址的设备回答“我有该 IP 地址；这是我的 MAC 地址。”

当设备使用自身的 MAC 地址响应 ARP 请求时，会使用代理 ARP，即使该设备不具有 IP 地址也如此。配置 NAT 并指定与 ASA 接口位于同一网络的映射地址时，ASA 使用代理 ARP。仅当 ASA 使用代理 ARP 宣布已为目标映射地址分配 MAC 地址时，流量才可以到达主机。

在极少数情况下，您可能要为 NAT 地址禁用代理 ARP。

如果您有一个与现有网络重叠的 VPN 客户端地址池，则 ASA 默认会在所有接口上发送代理 ARP 请求。如果有另一个接口位于同一个第2层域中，则该接口将会看到ARP请求，并以自身接口的MAC地址进行回应。结果将是面向内部主机的VPN客户端的返回流量转至错误的接口并被丢弃。在这种情况下，您应在不需要代理 ARP 请求的接口上禁用代理 ARP 请求。

过程

步骤 1 依次选择**配置** > **设备设置** > **路由** > **代理 ARP/邻居发现**。

Interface 字段会列出接口名称。Enabled 字段显示代理 ARP/邻居发现面向全局地址已启用 (Yes) 还是已禁用 (No)。

步骤 2 要为选定接口启用代理 ARP/邻居发现，请点击 **Enable**。默认情况下，将为所有接口启用代理 ARP/邻居发现。

步骤 3 要为选定接口上禁用代理 ARP/邻居发现，请点击 **Disable**。

步骤 4 点击 **Apply** 以将设置保存到运行配置。

显示路由表

要在 ASDM 中显示路由表中的所有路由，请依次选择**监控** > **路由** > **路由**。每行代表一个路由。

路由历史记录概述

表 *2:* 路由历史记录概述

功能名称	平台版本	功能信息
管理接口的路由表	9.5(1)	为了分隔和隔离管理流量与数据流量，对于管理流量添加了单独的 对于 ASA 每个情景的 IPv4 和 IPv6，分别为管理和数据创建了单独 表。而且，对于 ASA 的每个情景，在 RIB 和 FIB 中添加了两个额外 表。 更新了以下屏幕：

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。