配置ASA以传递IPv6流量

目录

简介
先决条件
要求
使用的组件
背景信息
IPv6功能信息
IPv6概述
IPv6在IPv4上的改进
提高编址能力
报头格式简化
改进对扩展和选项的支持
流标记功能
身份验证和隐私功能
配置
网络图
配置IPv6的接口
配置IPv6路由
配置IPv6的静态路由
使用OSPFv3配置IPv6的动态路由
验证
故障排除
排除L2连接故障(ND)
IPv4 ARP与IPv6 ND
ND调试
ND数据包捕获
ND系统日志
排除基本IPv6路由故障
IPv6的路由协议调试
IPv6的有用Show命令
使用IPv6的数据包跟踪器
与IPv6相关的ASA调试的完整列表
常见IPv6相关问题
子网配置不正确
修改的EUI 64编码
客户端默认使用临时IPv6地址
IPv6常见问题
能否同时在同一接口上传递IPv4和IPv6的流量？

[能否将IPv6和IPv4 ACL同时应用到同一接口？](#)
[ASA是否支持IPv6的QoS?](#)
[是否应将NAT与IPv6配合使用？](#)
[为什么在show failover命令输出中看到本地链***路IPv6***地址？](#)
[已知警告/增强请求](#)
[相关信息](#)

简介

本文档介绍如何配置思科自适应安全设备(ASA)，以便在ASA 7.0(1)及更高版本中传递互联网协议版本6(IPv6)流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco ASA 7.0(1)及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

目前，IPv6在市场渗透率方面仍相对较新。但是，IPv6配置帮助和故障排除请求稳步增加。本文档旨在满足这些需求并提供：

- IPv6使用概况
- ASA上的基本IPv6配置
- 有关如何通过ASA排除IPv6连接故障的信息
- 思科技术支持中心(TAC)确定的最常见IPv6问题和解决方案列表

  注意：鉴于IPv6仍处于早期阶段，作为全球IPv4替换，本文档将定期更新以保持准确性和相关性。

IPv6功能信息

以下是有关IPv6功能的一些重要信息：

- IPv6协议是ASA 7.0(1)版中首次引入的。
- 在ASA版本8.2(1)中引入了对透明模式下IPv6的支持。

IPv6概述

IPv6协议是在20世纪90年代中后期开发的，主要是因为公有IPv4地址空间迅速耗尽。尽管网络地址转换(NAT)极大地帮助了IPv4并延迟了此问题，但不可否认的是，最终需要替换协议。IPv6协议于1998年12月在RFC 2460中正式详述。您可以在官方RFC 2460文档中阅读有关该协议的更多信息，该文档位于Internet工程任务组(IETF)网站上。

IPv6在IPv4上的改进

本节介绍IPv6协议与旧IPv4协议相比的改进。

提高编址能力

IPv6协议将IP地址大小从32位增加到128位，以支持更高级别的寻址层次结构、更多的可寻址节点以及更简单的地址自动配置。通过向组播地址添加范围字段，提高了组播路由的可扩展性，并定义了一种新的*类型的*地址，称为任播*地址*。这用于将数据包发送到组中的任意一个节点。

报头格式简化

某些IPv4报头字段已被丢弃或设置为可选字段，以降低数据包处理的常见情况处理成本，并限制IPv6报头的带宽成本。

改进对扩展和选项的支持

对IP报头选项编码方式的更改可实现更高效的转发，减少对选项长度的严格限制，并为将来引入新选项提供更大的灵活性。

流标记功能

添加新功能，以便能够标记属于发送方请求特殊处理的特定业务流*的*数据包，例如非默认服务质量(QoS)*或实时服务*。

身份验证和隐私功能

为IPv6指定了用于支持身份验证、数据完整性和（可选）数据机密性的扩展。

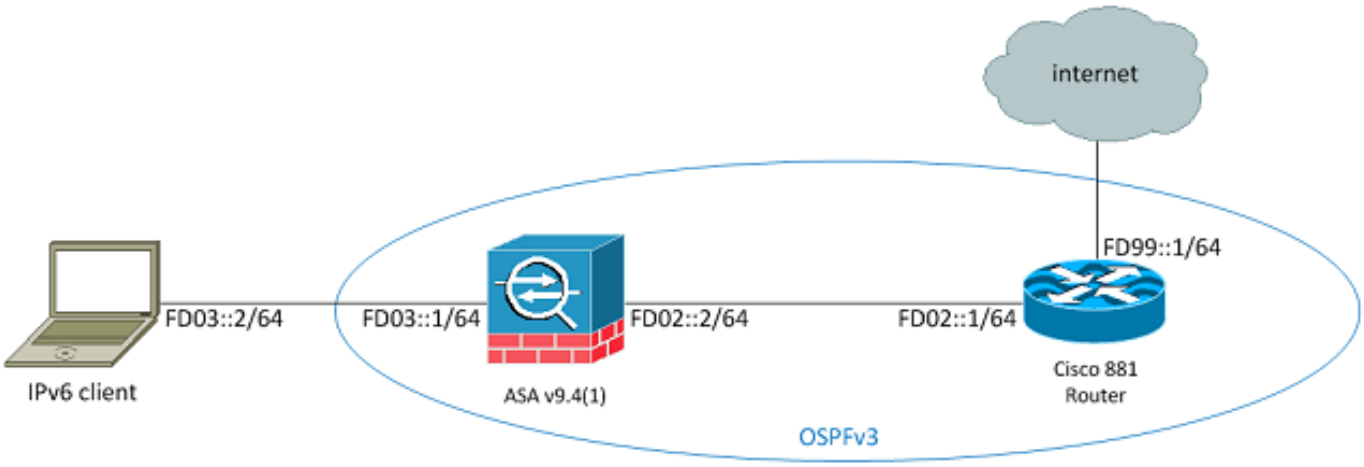
配置

本节介绍如何配置Cisco ASA以使用IPv6。

> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

以下是本文档中使用的示例的IPv6拓扑：



配置IPv6的接口

要通过ASA传递IPv6流量，必须首先在至少两个接口上启用IPv6。本示例介绍如何启用IPv6，以便将流量从Gi0/0的**内部接**口传递到Gi0/1**的外部接口**：

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 enable

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 enable
```

现在，您可以在两个接口上配置IPv6地址。

> **注意**：在本示例中，使用唯一本地地址(ULA)空间fc00::/7中的地址，因此所有地址都以**FD**(例如，fdxx:xxxx:xxxx.....。）此外，在写入IPv6地址时，可以使用双冒号(**::**)来表示一行零，**FD01::1/64**与**FD01:0000:0000:0000:0000**相同**0:0000:0000:0001**。

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 address fd03::1/64
ASAv(config-if)# nameif inside
ASAv(config-if)# security-level 100

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 address fd02::2/64
```

```
ASAv(config-if)# nameif outside
ASAv(config-if)# security-level 0
```

现在，您应该具有与外部VLAN上上游路由器（地址为fd02::1）的基本第2层(L2)/第3层(L3)**连接**:

```
ASAv(config-if)# ping fd02::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd02::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

配置IPv6路由

与IPv4一样，即使与直连子网中的主机存在IPv6连接，您仍必须拥有到外部网络的路由才能知道如何到达它们。第一个示例显示如何配置静态默认路由，以便通过下一跳地址为fd02::1的外部接口到达所有IPv6**网络**。

配置IPv6的静态路由

使用以下信息为IPv6配置静态路由：

```
ASAv(config)# ipv6 route outside 0::0/0 fd02::1
ASAv(config)# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
S   ::/0 [1/0]
via fd02::1, outsideASAv(config)#
```

如图所示，现在可以连接到外部子网上的主机：

```
ASAv(config)# ping fd99::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd99::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASAv(config)#
```

> **注意**：如果需要动态路由协议来处理IPv6的路由，则您也可以配置该协议。这将在下一节介绍。

使用OSPFv3配置IPv6的动态路由

首先，您应检查上游思科881系列集成多业务路由器(ISR)上的开放最短路径优先第3版(OSPFv3)配置：

```
C881#show run | sec ipv6
ipv6 unicast-routing

!--- This enables IPv6 routing in the Cisco IOS®.

.....
ipv6 ospf 1 area 0
address-family ipv6 unicast
passive-interface default
no passive-interface Vlan302

!--- This is the interface to send OSPF Hellos to the ASA.

default-information originate always

!--- Always distribute the default route.

redistribute static
ipv6 route ::/0 FD99::2

!--- Creates a static default route for IPv6 to the internet.
```

以下是相关接口配置：

```
C881#show run int Vlan302
interface Vlan302
....
ipv6 address FD02::1/64
ipv6 ospf 1 area 0
C881#
```

您可以使用ASA数据包捕获来验证OSPF *Hello*数据包是否从外部接口上的ISR发现：

```
ASAv(config)# show run access-list test_ipv6
access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# show cap
capture capout type raw-data access-list test_ipv6 interface outside
[Capturing - 37976 bytes]
ASAv(config)# show cap capout

367 packets captured

1: 11:12:04.949474 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
2: 11:12:06.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
   3: 11:12:07.854768       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
4: 11:12:07.946545 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
5: 11:12:08.949459 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
6: 11:12:09.542772 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
```

```
[hlim 1]
....
  13: 11:12:16.983011       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
14: 11:12:18.947170 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
15: 11:12:19.394831 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
16: 11:12:19.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
  21: 11:12:26.107477       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
ASAv(config)#
```

在上一个数据包捕获中，您可以看到OSPF(ip-proto-89)数据包从IPv6本地链路地址到达，该地址与ISR上的正确接口对应：

```
C881#show ipv6 interface brief
......
Vlan302 [up/up]
    FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

现在，您可以在ASA上创建OSPFv3进程，以便与ISR建立邻接关系：

```
ASAv(config)# ipv6 router ospf 1
ASAv(config-rtr)# passive-interface default
ASAv(config-rtr)# no passive-interface outside
ASAv(config-rtr)# log-adjacency-changes
ASAv(config-rtr)# redistribute connected
ASAv(config-rtr)# exit
```

将OSPF配置应用到ASA外部接口：

```
ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 ospf 1 area 0
ASAv(config-if)# end
```

这应会导致ASA在IPv6子网上发送广播OSPF Hello数据包。输入show ipv6 ospf neighbor命令以验证与路由器的邻接关系：

```
ASAv# show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
    14.38.104.1 1     FULL/BDR        0:00:33     14              outside
```

您还可以确认ISR上的邻居ID，因为它默认使用配置的最高IPv4地址作为ID:

```
C881#show ipv6 ospf 1
 Routing Process "ospfv3 1" with ID 14.38.104.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
static
 Originate Default Route with always

!--- Notice the other OSPF settings that were configured.

Router is not originating router-LSAs with maximum metric
```

```
....

C881#
```

ASA现在应该已从ISR获取默认IPv6路由。要确认此情况，请输入**show ipv6 route命**令：

```
ASAv# show ipv6 route

IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
O 2001:aaaa:aaaa:aaaa::/64 [110/10]
via ::, outside
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
OE2  ::/0 [110/1], tag 1

!--- Here is the learned default route.

    via fe80::c671:feff:fe93:b516, outside
ASAv#
```

ASA上IPv6的接口设置和路由功能的基本配置现已完成。

验证

当前没有可用于此配置的验证过程。

故障排除

IPv6连接故障排除步骤遵循的方法大多与IPv4连接故障排除方法相同，但有一些不同。从故障排除的角度来看，IPv4和IPv6之间最重要的区别之一是地址解析协议(ARP)在IPv6中不再存在。IPv6不使用ARP来解析本地LAN网段上的IP地址，而是使用称为邻居发现(ND)的协议。

了解ND利用互联网控制消息协议第6版(ICMPv6)进行介质访问控制(MAC)地址解析也很重要。有关IPv6 ND的详细信息，请参阅CLI手册1的IPv6邻居发现部分的ASA IPv6配置指南中的：*Cisco ASA系列一般操作CLI配置指南9.4*或RFC 4861中。

目前，大多数与IPv6相关的故障排除都涉及ND、路由或子网配置问题。这可能是因为IPv4和IPv6之间的主要区别也是这些。ND的工作方式与ARP不同，内部网络编址也有很大不同，因为IPv6中极不鼓励使用NAT，私有编址不再像在IPv4中那样被利用（在RFC 1918之后）。 理解这些差异和/或解决L2/L3问题后，第4层(L4)及以上层的故障排除过程与IPv4使用的故障排除过程基本相同，因为

TCP/UDP和更高层协议的功能基本相同（不管使用的IP版本如何）。

排除L2连接故障(ND)

用于排除L2与IPv6连接故障的最基本命令是**show ipv6 neighbor [nameif]** 命令，该命令相当于**IPv4的**show arp。

下面是示例输出：

```
ASAv(config)# show ipv6 neighbor outside
IPv6 Address Age Link-layer Addr State Interface
fd02::1                                    0 c471.fe93.b516  REACH   outside
fe80::c671:feff:fe93:b516                 32 c471.fe93.b516  DELAY   outside
fe80::e25f:b9ff:fe3f:1bbf 101 e05f.b93f.1bbf STALE outside
fe80::b2aa:77ff:fe7c:8412 101 b0aa.777c.8412 STALE outside
fe80::213:c4ff:fe80:5f53 101 0013.c480.5f53 STALE outside
fe80::a64c:11ff:fe2a:60f4 101 a44c.112a.60f4 STALE outside
fe80::217:fff:fe17:af80 99 0017.0f17.af80 STALE outside
ASAv(config)#
```

在此输出中，您可以看到IPv6地址**fd02::1**的成功解析，该地址属于MAC地址为**c471.fe93.b516的设备**。

> **注意**：您可能会注意到，同一路由器接口的MAC地址在上一输出中出现两次，因为路由器还为该接口分配了自分配的本地链路地址。本地链路地址是设备特定地址，只能用于直连网络上的通信。路由器不通过本地链路地址转发数据包，而是仅用于直连网段上的通信。许多IPv6路由协议（如OSPFv3）使用本地链路地址来共享L2网段的路由协议信息。

要清除ND缓存，请输入**clear ipv6 neighbors**命令。如果特定主机的ND发生故障，您可以输入**debug ipv6 nd**命令，并执行数据包捕获和验证系统日志，以确定发生在L2级别的情况。请记住，IPv6 ND使用ICMPv6消息来解析IPv6地址的MAC地址。

IPv4 ARP与IPv6 ND

请考虑IPv4的ARP和IPv6的ND的此比较表：

IPv4 ARP	IPv6节点
ARP请求（谁拥有10.10.10.1？）	邻居请求
ARP应答(10.10.10.1 is at dead.dead.dead)	邻居通告

在下一个场景中，ND无法解析位于外部接口*上的fd02::1*主机的MAC地址。

ND调试

以下是debug ipv6 nd**命令的输**出：

```
ICMPv6-ND: Sending NS for fd02::1 on outside

!--- "Who has fd02::1"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
ICMPv6-ND: DELETE -> INCMP: fd02::1
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NA for fd02::2 on outside

!--- "fd02::2 is at dead.dead.dead"

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
ICMPv6-ND: DELETE -> INCMP: fd02::1

!--- Here is where the ND times out.

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
```

在此调试输出中，*似乎*从未收到来自**fd02::2的**邻居通告。您可以检查数据包捕获，以确认这是否是真实情况。

ND数据包捕获

> **注意**：自ASA版本9.4(1)起，IPv6数据包捕获仍需要访问列表。已提交增强请求，以便使用思科漏洞ID CSCtn09836跟踪此项。

配置访问控制列表(ACL)和数据包捕获：

```
ASAv(config)# access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# cap capout interface outside access-list test_ipv6
```

从ASA发起对**fd02::1**的ping:

```
ASAv(config)# show cap capout
....
23: 10:55:10.275284 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
24: 10:55:10.277588 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
26: 10:55:11.287735 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
27: 10:55:11.289642 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
28: 10:55:12.293365 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
29: 10:55:12.298538 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
32: 10:55:14.283341 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
33: 10:55:14.285690 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
35: 10:55:15.287872 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
36: 10:55:15.289825 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
```

```
[class 0xe0]
```
如数据包捕获所示，收到来自fd02::**1的邻居通**告。但是，由于某种原因，通告未得到处理，如调试输出所示。为了进一步检查，您可以查看系统日志。

ND系统日志

以下是一些ND系统日志示例：

```
May 13 2015 10:55:10: %ASA-7-609001: Built local-host identity:fd02::2
May 13 2015 10:55:10: %ASA-6-302020: Built outbound ICMP connection for faddr
ff02::1:ff00:1/0 gaddr fd02::2/0 laddr fd02::2/0(any)
May 13 2015 10:55:10: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:10: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:11: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:11: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:12: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:12: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:14: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:14: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:15: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:15: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
```

在这些系统日志中，您可以看到，来自ISR的ND邻居通告数据包在**fd02::1**处被丢弃，原因是修改的扩展唯一标识符(EUI)64（修改的EUI-64）格式检查失败。

> **提示：**有关此特定*问题的详细信息，请参*阅本文档的修改的EUI-64地址编码部分。此故障排除逻辑也可应用于所有类型的丢包原因，例如当ACL不允许特定接口上的ICMPv6，或当单播反向路径转发(uRPF)检查失败时，这两种情况都可能导致IPv6的L2连接问题。

排除基本IPv6路由故障

使用IPv6时的路由协议故障排除步骤与使用IPv4时的故障排除步骤基本相同。使用**debug**和**show**命令以及数据包捕获，对于尝试确定路由协议未按预期运行的原因非常有用。

IPv6的路由协议调试

本节提供IPv6的有用调试命令。

全局IPv6路由调试

您可以使用**debug ipv6 routing debug**对所有IPv6路由表更改进行故障排除：

```
ASAv# clear ipv6 ospf 1 proc

Reset OSPF process? [no]: yes
ASAv# IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, Delete 2001:aaaa:aaaa:aaaa::/64 from table
IPv6RT0: ospfv3 1, Delete backup for fd02::/64
IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ospfv3 1, Delete ::/0 from table
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Add 2001:aaaa:aaaa:aaaa::/64 to table
IPv6RT0: ospfv3 1, Added next-hop :: over outside for 2001:aaaa:aaaa:aaaa::/64,
[110/10]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516
nh_source fe80::c671:feff:fe93:b516 via interface outside route-type 16
IPv6RT0: ospfv3 1, Add ::/0 to table
IPv6RT0: ospfv3 1, Added next-hop fe80::c671:feff:fe93:b516 over outside for ::/0,
[110/1]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Route add 2001:aaaa:aaaa:aaaa::/64 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Reuse backup for fd02::/64, distance 110
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516 nh_source fe80::c671:feff:fe93:b516 via interface outside
route-type 16
IPv6RT0: ospfv3 1, Route add ::/0 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
```

OSPFv3调试

您可以使用**debug ipv6 ospf** 命令对OSPFv3问题进行故障排除：

```
ASAv# debug ipv6 ospf ?

adj OSPF adjacency events
database-timer OSPF database timer
events OSPF events
flood OSPF flooding
graceful-restart OSPF Graceful Restart processing
hello OSPF hello events
ipsec OSPF ipsec events
lsa-generation OSPF lsa generation
```

```
lsdb OSPF database modifications
packet OSPF packets
retransmission OSPF retransmission events
spf OSPF spf
```

以下是OSPFv3进程重新启动后启用的所有调试的输出示例：

```
ASAv# clear ipv6 ospf 1
OSPFv3: rcv. v:3 t:1 l:44 rid:192.168.128.115
aid:0.0.0.0 chk:a9ac inst:0 from outside
OSPFv3: Rcv hello from 192.168.128.115 area 0 from outside fe80::217:fff:fe17:af80
interface ID 142
OSPFv3: End of hello processingpr
OSPFv3: rcv. v:3 t:1 l:44 rid:14.38.104.1
aid:0.0.0.0 chk:bbf3 inst:0 from outside
OSPFv3: Rcv hello from 14.38.104.1 area 0 from outside fe80::c671:feff:fe93:b516
interface ID 14
OSPFv3: End of hello processingo
ASAv# clear ipv6 ospf 1 process

Reset OSPF process? [no]: yes
ASAv#
OSPFv3: Flushing External Links
Insert LSA 0 adv_rtr 172.16.118.1, type 0x4005 in maxage
OSPFv3: Add Type 0x4005 LSA ID 0.0.0.0 Adv rtr 172.16.118.1 Seq 80000029 to outside
14.38.104.1 retransmission list
....

!--- The neighbor goes down:

OSPFv3: Neighbor change Event on interface outside
OSPFv3: DR/BDR election on outside
OSPFv3: Elect BDR 14.38.104.1
OSPFv3: Elect DR 192.168.128.115
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Prefix DR LSA intf outside
OSPFv3: Schedule Prefix Stub LSA area 0
OSPFv3: 14.38.104.1 address fe80::c671:feff:fe93:b516 on outside is dead, state DOWN
....

!--- The neighbor resumes the exchange:

OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0xd09 opt 0x0013 flag 0x7 len 28
 mtu 1500 state EXSTART
OSPFv3: First DBD and we are not SLAVE
OSPFv3: rcv. v:3 t:2 l:168 rid:14.38.104.1
     aid:0.0.0.0 chk:5aa3 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x914 opt 0x0013 flag 0x2 len 168
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the MASTER
OSPFv3: outside Nbr 14.38.104.1: Summary list built, size 0
OSPFv3: Send DBD to 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x1 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:192.168.128.115
     aid:0.0.0.0 chk:295c inst:0 from outside
OSPFv3: Rcv DBD from 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x7 len 28
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the SLAVE
OSPFv3: outside Nbr 192.168.128.115: Summary list built, size 0
OSPFv3: Send DBD to 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x0 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:14.38.104.1
     aid:0.0.0.0 chk:8d74 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x0 len 28
```

```
 mtu 1500 state EXCHANGE
....

!--- The routing is re-added to the OSPFv3 neighbor list:

OSPFv3: Add Router 14.38.104.1 via fe80::c671:feff:fe93:b516, metric: 10
 Router LSA 14.38.104.1/0, 1 links
   Link 0, int 14, nbr 192.168.128.115, nbr int 142, type 2, cost 1
     Ignore newdist 11 olddist 10
```

增强型内部网关路由协议 (EIGRP)

ASA上的EIGRP不支持使用IPv6。请参阅CLI手册1的“EIGRP指*南”部分：Cisco ASA系列常规操作CLI配置指南9.4,*了解详细信息。

边界网关协议 (BGP)

当使用IPv6时，**debug** 命令可用于排除BGP故障：

```
ASAv# debug ip bgp ipv6 unicast  ?

X:X:X:X::X IPv6 BGP neighbor address
keepalives BGP keepalives
updates BGP updates
<cr>
```

IPv6的有用Show命令

您可以使用以下**show**命令来排除IPv6问题：

- **show ipv6 route**
- **show ipv6 interface brief**
- **show ipv6 ospf <process ID>**
- **show ipv6 traffic**
- **show ipv6 neighbor**
- **show ipv6 icmp**

使用IPv6的数据包跟踪器

您可以在ASA上以与IPv4相同的方式将内置的Packet Tracer功能与IPv6配合使用。以下示例使用Packet Tracer功能来模拟位于**fd03::2**的内部主机，该主机尝试连接到位于**5555::1**的Web服务器Internet，其默认路由通过OSPF从881接**口获**知：

```
ASAv# packet-tracer input inside tcp fd03::2 10000 5555::1 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
```

```
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd59ca0f0, priority=1, domain=permit, deny=false
       hits=2734, user_data=0x0, cs_id=0x0, l3_type=0xdd86
       src mac=0000.0000.0000, mask=0000.0000.0000
       dst mac=0000.0000.0000, mask=0100.0000.0000
       input_ifc=inside, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop fe80::c671:feff:fe93:b516 using egress ifc  outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd589cc30, priority=1, domain=nat-per-session, deny=true
       hits=1166, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=6
       src ip/id=::/0, port=0, tag=any
       dst ip/id=::/0, port=0, tag=any
       input_ifc=any, output_ifc=any

<<truncated output>>

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

ASAv#
```

请注意，出口MAC地址是881接口的本地链路地址。如前所述，对于许多动态路由协议，路由器使用本地链路IPv6地址来建立邻接关系。

与IPv6相关的ASA调试的完整列表

以下是可用于排除IPv6问题的调试：

```
ASAv# debug ipv6 ?

dhcp IPv6 generic dhcp protocol debugging
dhcprelay IPv6 dhcp relay debugging
icmp ICMPv6 debugging
interface IPv6 interface debugging
mld IPv6 Multicast Listener Discovery debugging
```

```
nd IPv6 Neighbor Discovery debugging
ospf OSPF information
packet IPv6 packet debugging
routing IPv6 routing table debugging
```

常见IPv6相关问题

本节介绍如何排除最常见的IPv6相关问题。

子网配置不正确

许多IPv6 TAC案例的生成是由于对IPv6如何运行缺乏普遍了解，或由于管理员尝试使用IPv4特定进程实施IPv6。

例如，TAC发现，Internet服务提供商(ISP)向管理员分配\56个IPv6地址块。 然后，管理员将地址和完整的\56子网分配给ASA外部接口，并选择一些内部范围供内部服务器使用。但是，使用IPv6时，所有内部主机也应使用可路由的IPv6地址，并且IPv6地址块应根据需要细分为更小的子网。在此场景中，您可以创建许多\64子网作为已分配的\56块的一部分。

> **提示：**有关其他信息，请参阅RFC 4291。

修改的EUI 64编码

可以配置ASA，以要求修改EUI-64编码的IPv6地址。根据RFC 4291,EUI允许主机为自己分配唯一的64位IPv6接口标识符(EUI-64)。 此功能是IPv4的优势，因为它消除了使用DHCP分配IPv6地址的要求。

如果配置ASA以通过**ipv6 enforce-eui64 nameif**命令要求进行此增强，则它可能会丢弃来自本地子网上其他主机的许多邻居发现请求和通告。

> **提示：**有关详细信息，请参阅了解IPv6 EUI-64位地址思科支持社区文档。

客户端默认使用临时IPv6地址

默认情况下，许多客户端操作系统(OS)（如Microsoft Windows 7和8版、Macintosh OS-X和基于Linux的系统）使用自分配的临时*IPv6地址*，通过IPv6无状态地址自动配置(SLAAC)实现扩展的隐私。

思科TAC在某些情况下发现，这会在环境中造成意外问题，因为主机会从临时地址而不是静态分配的地址生成流量。因此，ACL和基于主机的路由可能导致流量被丢弃或路由不正确，从而导致主机通信失败。

有两种方法可用于解决这种情况。可以在客户端系统上单独禁用此行为，也可以在ASA和Cisco IOS®路由器上禁用此行为。在ASA或路由器端，您必须修改触发此行为的路由器通告(RA)消息标志。

要在单个客户端系统上禁用此行为，请参阅下一节。

Microsoft Windows

要在Microsoft Windows系统上禁用此行为，请完成以下步骤：

1. 在Microsoft Windows中，打开提升的命令提示符（以管理员身份运行）。
2. 输入此命令以禁用随机IP地址生成功能，然后按**Enter**:

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

3. 输入以下命令以强制Microsoft Windows使用EUI-64标准：

```
netsh interface ipv6 set privacy state=disabled
```

4. 重新启动计算机以应用更改。

Macintosh OS-X

在终端中，输入以下命令以禁用主机上的IPv6 SLAAC，直到下次重新启动：

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=0
```

要使配置永久化，请输入以下命令：

```
sudo sh -c 'echo net.inet6.ip6.use_tempaddr=0 >> /etc/sysctl.conf'
```

Linux

在终端外壳中，输入以下命令：

```
sysctl -w net.ipv6.conf.all.use_tempaddr=0
```

从ASA全局禁用SLAAC

用于解决此行为的第二种方法是修改从ASA发送到客户端的RA消息，这会触发SLAAC的使用。要修改RA消息，请在接口配置模式下输入以下命令：

```
ASAv(config)# interface gigabitEthernet 1/1
ASAv(config-if)# ipv6 nd prefix 2001::db8/32 300 300 no-autoconfig
```

此命令修改ASA发送的RA消息，以便不设置A位标志，并且客户端不生成临时IPv6地址。

提示：有关其[他信息，](#)请参阅RFC 4941。

IPv6常见问题

本节介绍有关IPv6使用的一些常见问题。

能否同时在同一接口上传递IPv4和IPv6的流量？

Yes.您只需在接口上启用IPv6，并为接口分配IPv4和IPv6地址，同时处理这两种类型的流量。

能否将IPv6和IPv4 ACL同时应用到同一接口？

您可以在9.0(1)版以前的ASA版本中执行此操作。 自ASA 9.0(1)版起，ASA上的所有ACL都是统一的，这意味着ACL支持同一ACL中IPv4和IPv6条目的混合。

在ASA 9.0(1)及更高版本中，ACL只需合并在一起，而单个统一ACL则通过access-group命令应用于接口。

ASA是否支持IPv6的QoS?

Yes.ASA支持IPv6的管制和优先级队列，其方式与IPv4相同。

自ASA 9.0(1)版起，ASA上的所有ACL都是统一的，这意味着ACL支持同一ACL中IPv4和IPv6条目的混合。因此，在类映射上实施的任何与ACL匹配的QoS命令都会对IPv4和IPv6流量采取操作。

是否应将NAT与IPv6配合使用？

虽然ASA上可以为IPv6配置NAT，但鉴于几乎无限量的可用、可全局路由的IPv6地址，IPv6中不建议使用NAT，也不必要使用NAT。

如果IPv6场景中需要NAT，可以在CLI手册2的“IPv6 NAT指南”部分找到有关如何配*置NAT的详细信息：Cisco ASA系列防火墙CLI配置指南，9.4*。

> **注意：**在使用IPv6实施NAT时，应考虑一些准则和限制。

为什么在show failover命令输出中看到本地链*路IPv6*地址？

在IPv6中，ND使用本地链路地址来执行L2地址解析。因此，**show failover**命令输出中受监控接口的IPv6地址显示本地链路地址，而不是接口上配置的全局IPv6地址。这是预料之中的现象。

已知警告/增强请求

以下是有关IPv6使用的一些已知警告：

- Cisco Bug ID CSCtn09836 â *ASA 8.x capture "match"子句不捕获IPv6流量*
- Cisco Bug ID CSCuq85949 - *ENH:对WCCP的ASA IPv6支持*
- Cisco Bug ID CSCut78380 â *ASA IPv6 ECMP路由不对流量进行负载均衡*

相关信息

- **RFC 2460 - Internet协议，版本6(IPv6)规范**

- RFC 4291 - IP第6版寻址架构
- RFC 4861 Â IP版本6(IPv6)的邻居发现
- CLI手册1:Cisco ASA系列General Operations CLI配置指南，9.4 - IPv6
- 通过IPv4+IPv6的AnyConnect SSL到ASA配置
- 技术支持与文档— Cisco Systems