配置ASA通过IPv6流量

目录

简介

本文描述如何配置Cisco可适应安全工具(ASA)为了通过互联网协议在ASA版本7.0(1)和以上的版本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

本文档中的信息根据Cisco ASA版本7.0(1)和以上。

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仍然是相对新的根据市场渗透。然而， IPv6配置帮助和故障排除请求不断地增加。本文目的将针对那些需要和提供：

- IPv6使用情况概述
- 在ASA的基本IPv6配置
- 关于如何的信息通过ASA排除故障IPv6连接
- 最普通的IPv6问题和解决方案的列表，如识别由Cisco技术支持中心(TAC)

注意：在的情况下IPv6仍然在早期作为IPv4更换全局，本文周期地将更新为了维护准确性和相关性。

IPv6功能信息

这是关于IPv6功能的一些重要信息：

- IPv6协议在ASA版本7.0(1)首先介绍。
- IPv6的支持在透明模式在ASA版本8.2(1)介绍。

IPv6概述

IPv6协议开发20世纪90年代中后期，主要由于这样的事实公共IPv4地址空间快速移动朝耗尽。虽然网络地址转换(NAT)大量地帮助IPv4并且延迟此问题，变得不容置疑更换协议最终是需要的。IPv6协议在十二月的RFC 2460正式被选派了1998年。您能闻悉更多在正式RFC 2460文档的协议，位于在互联网工程任务组(IETF)网站。

在IPv4的IPv6改进

此部分描述包括与IPv6协议与更旧的IPv4协议的改进。

提高编址能力

IPv6协议增加从32个位的IP地址大小到128个位为了支持更多级别寻址分级结构、很多可寻址的节点和地址的更加简单的自动配置。组播路由的可扩展性由一个*范围*字段的新增内容组播地址的改善。 另外，地址新类型，呼叫*anycast地址*，定义。这在组中用于为了发送数据包到所有一个节点。

报头格式简化

一些IPv4报头字段丢弃了或使可选择为了减少普通案例处理成本数据包处理和为了限制IPv6报头的带宽开销。

扩展和选项的改善的支持

更改就象IP报头选项编码在将来允许更有效的转发、较不严密限额在长度选项和较大适应性新的选项介绍的。

流标记的功能

一个新的功能被添加为了启用属于特定的流量*运输流量*发送方请求特殊处理，例如非默认服务质量(QoS)或*实时服务的*标记数据包。

验证和保密性功能

使用为了支持验证的扩展，数据完整性和(可选)数据机密性为IPv6指定。

配置

此部分描述如何配置思科ASA为使用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

这是使用在本文中的示例的IPv6拓扑：

配置IPv6的接口

为了通过IPv6流量ASA，您必须首先启用在至少两个接口的IPv6。此示例描述如何使IPv6为了通过从内部接口的流量在**Gi0/0**到在**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
```

您能当前配置在两个的IPv6地址接口。

> **注意**：在本例中，使用在fc00::/7唯一本地地址(ULA)空间的地址，因此所有地址开始与**FD** (例如，fdxx：xxxx：xxxx....影响。并且，当您写入IPv6地址时，您能使用双冒号(：：)为了代表零线路，以便**FD01::1/64**是相同的象**FD01:0000:0000:0000:0000:0000:0000:00001**。

```
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
```

您应该当前有基本层2 (对一上游路由器的L2)/Layer 3 (L3)连接在地址**fd02::1的**外层VLAN的：

```
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

正如IPv4，即使有IPv6连接用在直接连接的子网的主机，您必须仍然有路由到外部网络为了会到达他们。第一示例显示如何配置静态默认路由为了通过与**fd02::1**下一跳地址的外部接口到达所有IPv6网络。

配置IPv6的静态路由

请使用此信息为了配置IPv6的静态路由：

```
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)#
```

如显示，当前有连接到在一外部子网的一台主机：

```
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：如果动态路由协议希望为了处理IPv6的路由，则您能配置那。这在下一部分描述。

配置IPv6的动态路由与OSPFv3

首先，您应该检查在上行Cisco 881系列集成业务路由器(ISR)的开放最短路径第一版本3 (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.
```

这是相关接口配置：

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

您能使用ASA数据包捕获为了验证OSPF *Hello数据包*从在外部接口的ISR被看到：

```
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，您能看到OSPF (ip-proto-89)数据包从IPv6链路本地地址到达，对应于在ISR的正确接口：

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

您能当前创建在ASA的一OSPFv3进程为了设立与ISR的一邻接：

```
C881#show ipv6 interface brief
......
Vlan302 [up/up]
```

```
    FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

运用OSPF配置对ASA外部接口：

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

这应该造成ASA发送在IPv6子网的广播OSPF Hello数据包。输入**show ipv6 ospf neighbor**命令为了验证邻接用路由器：

```
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
```

默认情况下，因为使用最较高的已配置的IPv4地址ID您能也确认在ISR的邻居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应该当前了解从ISR的默认Ipv6 route。为了确认此，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#
```

接口设置和路由功能的基本配置IPv6的在ASA当前完成。

验证

当前没有可用于此配置的验证过程。

故障排除

IPv6连接的故障排除程序跟随用于为了排除故障IPv4连接的多数同样方法，与一些差异。从故障排除方面，其中一IPv4之间的最重要的差异和IPv6是地址解析服务(ARP)在IPv6不再存在。而不是使用ARP为了解决在本地LAN网段的IP地址， IPv6使用呼叫邻接发现的一份协议。

应该了解的是ND有效利用互联网控制消息协议媒体访问控制(MAC)地址解析的版本6 (ICMPv6)。关于IPv6 ND的更多信息可以在*CLI书1的*IPv6邻居发现部分的ASA IPv6配置指南找到*：Cisco ASA系列一般操作CLI配置指南， 9.4*或在RFC 4861。

目前，多数IPv6-related故障排除介入ND、路由或者子网配置问题。这可能归结于事实这些也是IPv4和IPv6之间的关键区别。 ND工作跟ARP和不同内部网络网络地址也相当不同的，因为使用NAT在IPv6高度被劝阻，并且私有寻址不再被有效利用是在IPv4的方法(在RFC 1918以后)。一旦这些差异了解并且/或者L2/L3问题是解决的，在Layer4 (L4)的故障排除流程以上根本是相同的象用于IPv4的那，因为TCP/UDP和更高层协议根本作用使用)的同样(不管IP版本。

排除故障L2连接(ND)

使用为了排除故障L2与IPv6的连接的多数基本命令是**显示IPv6邻接[nameif]**命令，是**show arp**等同IPv4的。

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，您能为**fd02::1** IPv6地址看到成功的解决方法，属于有**c471.fe93.b516** MAC地址的设备。

> **注意**：您也许注意同一路由器接口MAC地址在上一个输出中两次出现，因为路由器也有此接口的一个自己分配的链路本地地址。链路本地地址是能只使用在直连网络的通信的一个设备特有的地址。路由器不通过链路本地地址转发数据包，但是相当他们仅是为在直连网络分段的通信。许多IPv6路由协议(例如OSPFv3)使用链路本地地址为了共享关于L2分段的路由协议信息

。

为了清除ND缓存，请输入**clear ipv6 neighbors**命令。如果ND为特定主机失效，您能输入**调试IPv6 nd**命令，以及执行数据包捕获并且验证Syslog，为了确定发生在L2级别的那。切记IPv6 ND使用ICMPv6消息为了解决IPv6地址的MAC地址。

IPv4 ARP与IPv6 ND

细想ARP和ND此对照表IPv4的IPv6的：

IPv4 ARP	IPv6 ND
ARP请求(谁有10.10.10.1 ？)	邻接垦请
ARP应答(10.10.10.1在dead.dead.dead)	邻接广告

在下个方案中， ND不能解决在外部接口查找*fd02::1*主机的MAC地址。

ND调试

这是**调试IPv6 nd**命令输出：

```
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debug输出中，*看来*从**fd02::2的**邻接广告从未接收。您能检查数据包捕获为了确认这是否实际上是实际情形。

ND数据包捕获

> **注意**：自ASA版本9.4(1)，访问列表为IPv6数据包捕获仍然要求。提出增强请求为了跟踪此与Cisco Bug ID CSCtn09836。

配置访问控制表(ACL)和数据包捕获：

```
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
```

启动ping对从ASA的fd02::1 ：

```
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]
```

如数据包捕获所显示，从fd02::1的邻接广告接收。由于某种原因然而，如debug输出所显示，广告没有处理。 对于进一步考试，您能查看Syslog。

ND Syslog

这是一些示例ND Syslog ：

```
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Syslog内，您能看到从ISR的ND邻接通告信息包在**fd02::1**是丢弃的由于失败的已修改延长的唯一标识符(EUI) 64 (已修改EUI-64)格式检查。

> **提示**：参考本文的*已修改EUI-64地址编码*部分关于此特定问题的更多信息。此故障排除逻辑可以应用到各种各样的丢弃原因，例如，当ACL不允许在一个特定接口时的ICMPv6或，当单播逆向路径转发(URPF)检查失败发生时，其中之二能导致L2与IPv6的连通性问题。

排除故障基本IPv6路由

路由协议的故障排除程序，当使用时IPv6根本是相同的作为那些，当使用时IPv4。使用**Debug与Show**调试指令，以及数据包捕获，是有用的与尝试查明原因路由协议不正常运行正如所料。

IPv6的路由协议调试

此部分为IPv6提供有用的调试指令。

路由调试的全局IPv6

您能使用**路由**调试的**调试IPv6**为了排除故障所有IPv6路由表更改：

```
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

您能使用**ospf命令调试的IPv6**为了排除故障OSPFv3问题：

```
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
```

这是启用的所有的一示例输出调试，在OSPFv3进程重新启动后：

```
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)

在ASA的EIGRP不支持使用IPv6。*参考CLI书1的*EIGRP部分的指南*：思科ASA系列一般操作CLI配置指南， 9.4*欲知更多信息。

边界网关协议 (BGP)

当使用时，此**debug命令**可以用于为了排除故障BGP IPv6 ：

```
ASAv# debug ip bgp ipv6 unicast  ?

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

IPv6的有用的show命令

您能使用这些显示命令为了排除故障IPv6问题：

- show ipv6 route
- show ipv6 interface brief
- 显示IPv6 ospf <process ID>
- show ipv6 traffic
- 显示IPv6邻居
- 显示IPv6 icmp

与IPv6的数据包跟踪程序

您能以在ASA的IPv6使用内置的数据包跟踪程序功能以与与IPv4相似的方式。这是数据包追踪器功能用于为了模拟内部主机在fd03::2，尝试连接到Web服务器在5555::1在互联网查找用默认路由从881接口了解通过OSPF:的示例

```
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#
```

注意出口MAC地址是881接口的链路本地地址。如被提及以前，为许多动态路由协议，路由器请使用链路本地IPv6地址为了设立邻接。

IPv6-Related ASA调试完整列表

这是能使用为了排除故障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
```

普通的IPv6-Related问题

此部分描述如何排除故障最普通的IPv6-related问题。

不正确地配置的子网

许多IPv6 TAC案例生成的归结于一般缺乏关于IPv6如何的知识作用，或者由于管理员尝试实现与使用的IPv6 IPv4-specific进程。

例如， TAC看到了管理员由互联网服务提供商分配IPv6地址\56块的案件。管理员然后分配一个地址和全双工\56子网对ASA外部接口并且选择若干内部范围使用内部的服务器。然而，与IPv6，所有内部主机应该也使用可路由的IPv6地址，并且IPv6地址块应该是被分解为的更加小的子网当必要时。在此方案中，您能创建许多\64子网，当分配了\56块的零件。

提示：其他信息的参考的RFC 4291。

已修改EUI 64编码

ASA可以配置为了要求已修改EUI-64-encoded IPv6地址。EUI，根据RFC 4291，提供主机分配一个唯一64位IPv6接口标识符(EUI-64)。因为去除需求为IPv6地址分配，使用DHCP此功能是一个优点超过IPv4。

如果ASA配置为了通过**nameif命令的IPv6 enforce-eui64**要求此增强，则从在本地子网的其他主机可能将丢弃许多邻居发现垦请和广告。

提示：欲知更多信息，参考了解IPv6 EUI-64位地址Cisco支持社区文档。

默认情况下客户端使用临时IPv6地址

默认情况下，许多客户端操作系统(Oss)，例如Microsoft Windows版本7和8， Macintosh OS X和基于linux的系统，使用自己分配的*临时*IPv6地址延长的保密性通过IPv6无状态的地址自动配置(SLAAC)。

Cisco TAC看到了这的环境引起意外问题的一些案件，因为主机生成从临时地址而不是静态分配的地址的流量。结果， ACL和招待基础的路由也许导致流量变得已丢失或不正确地路由，造成主机通信发生故障。

有使用为了论及此情况的两个方法。行为在客户端系统可以单个禁用，或者您能禁用在ASA和Cisco IOS路由器的此行为。在ASA或路由器端，您必须修改触发此行为Message标志位的路由器通告(RA)。

参考以下部分为了禁用在各自的客户端系统的此行为。

Microsoft Windows

完成这些步骤为了禁用在Microsoft Windows系统的此行为：

1. 在Microsoft Windows中，请打开一高的Prompt命令(运行作为管理员)。
2. 输入此命令为了禁用随机的IP地址生成功能，然后按回车：
   netsh interface ipv6 set global randomizeidentifiers=disabled
3. 输入此命令为了强制Microsoft Windows使用EUI-64标准：
   netsh interface ipv6 set privacy state=disabled
4. 重新启动计算机为了应用更改。

Macintosh OS X

在终端中，请输入此命令为了禁用在主机的IPv6 SLAAC直到下辆重新启动：

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

为了做配置永久性，请输入此命令：

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

Linux

在一终端的shell中，请输入此命令：

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

禁用SLAAC全局从ASA

第二种方法使用为了寻址的此行为是修改从ASA传送给客户端，触发使用SLAAC的RA信息。为了修改RA消息，请输入从*接口配置模式的*此命令：

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

此命令修改由ASA传送的RA信息，以便A位标志没有设置，并且客户端不生成一个临时IPv6地址。

> **提示**：其他信息的参考的RFC 4941。

IPv6常见问题

此部分关于使用IPv6描述一些常见问题。

能否通过IPv4和IPv6的流量在同一个接口，同时？

可以。您必须启用在接口的IPv6和分配一IPv4和一个IPv6地址对接口，并且同时处理两种流量类型。

能否应用IPv6和IPv4 ACL到同一个接口？

您在ASA版本早于版本9.0(1)能执行此。自ASA版本9.0(1)，在ASA的所有ACL*统一*，因此意味着ACL支持在同样ACL的IPv4和IPv6条目的混合。

在ASA版本9.0(1)和以上， ACL一起合并，并且单个，统一的ACL应用对接口通过**access-group命令**。

ASA是否支持IPv6的QoS ？

可以。ASA相似地支持管制和优先级队列IPv6的执行与IPv4。

自ASA版本9.0(1)，在ASA的所有ACL*统一*，因此意味着ACL支持在同样ACL的IPv4和IPv6条目的混合。结果，在类映射被立法匹配ACL的所有QoS命令采取在IPv4和IPv6流量的行动。

应该以IPv6使用NAT ？

虽然NAT可以为在ASA的IPv6配置，使用在IPv6的NAT是高度被劝阻和多余的，给最近的无限的相当数量联机，全球可发送的IPv6地址。

如果NAT在IPv6方案要求，您在*CLI书2的*IPv6 NAT指南部分能找到关于如何的更多信息配置它*：思科ASA系列防火墙CLI配置指南， 9.4*。

> **注意**：有应该考虑的一些指南和限制，当您实现与IPv6时的NAT。

为什么看到链路本地IPv6地址在*show failover*命令输出中？

在IPv6， ND使用链路本地地址为了执行L2地址解析。为此，受监视接口的IPv6地址在**show failover命令**输出中显示链路本地地址在接口配置而不是的全局IPv6地址。这是预料之中的现象。

已知问题说明/增强请求

这是一些已知问题说明关于使用IPv6 ：

- Cisco Bug ID CSCtn09836 âÂ Â *ASA 8.x捕获"匹配"条款不捉住IPv6流量*
- Cisco Bug ID CSCuq85949 âÂ Â *ENH ：ASA WCCP的IPv6支持*
- Cisco Bug ID CSCut78380 âÂ Â *ASA IPv6 ECMP路由不装载平衡流量*

相关信息

- **RFC 2460 âÂ Â 互联网协议，版本6 (IPv6)规格**
- **RFC 4291 âÂ Â IP版本6 (IPv6)寻址体系结构**
- **RFC 4861 âÂ Â IP版本6 (IPv6)的邻居发现**
- **CLI书1 ：思科ASA系列一般操作CLI配置指南， 9.4 âÂ Â IPv6**
- **在IPv4+IPv6的AnyConnect SSL对ASA配置**
- **技术支持&文档âÂ Â Cisco系统**