配置ASA以傳遞IPv6流量

目錄

簡介

本文檔介紹如何配置思科自適應安全裝置(ASA)以便在ASA 7.0(1)及更高版本中傳遞網際網路協定第6版(IPv6)流量。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Cisco ASA 7.0(1)及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

目前，IPv6在市場滲透方面仍相對較新。但是，IPv6配置幫助和故障排除請求穩步增加。本文旨在解決這些需求並提供：

- IPv6使用情況的概述
- ASA上的基本IPv6配置
- 有關如何通過ASA排除IPv6連線故障的資訊
- 最常見的IPv6問題和解決方案清單，由思科技術支援中心(TAC)確定

  附註：由於IPv6作為IPv4的全球替代品仍處於早期階段，因此本文檔將定期更新，以保持準確性和相關性。

IPv6功能資訊

以下是有關IPv6功能的一些重要資訊：

- IPv6協定最初是在ASA 7.0(1)版中引入的。
- ASA 8.2(1)版引入了透明模式對IPv6的支援。

IPv6概述

IPv6協定是在1990年代中期到後期開發的，主要是因為公共IPv4地址空間迅速耗盡。雖然網路位址轉譯(NAT)在很大程度上協助了IPv4並延遲了此問題，但不可否認的是，最終還是需要替代通訊協定。IPv6協定在1998年12月的RFC 2460中正式詳述。您可以在Internet工程任務組(IETF)網站上的官方RFC 2460文檔中閱讀有關該協定的詳細資訊。

基於IPv4的IPv6改進

本節介紹IPv6協定與舊版IPv4協定相比有哪些改進。

擴展定址能力

IPv6協定將IP地址大小從32位增加到128位，以支援更高級別的定址層級、更多數量的可定址節點和更簡單的地址自動配置。通過在組播地址中增加*scope*欄位，提高了組播路由的可擴充性，並定義了一種稱為任播地址的*新*型地址。這是用來將封包傳送到群組中的任何一個節點。

標題格式簡化

某些IPv4標頭欄位已丟棄或設為可選，以便減少資料包處理的常見處理成本並限制IPv6標頭的頻寬成本。

改進了對擴展和選項的支援

IP報頭選項的編碼方式發生改變，可實現更高效的轉發，對選項長度的限制更少，並且在將來引入新選項時具有更大的靈活性。

流標籤功能

新增了一項新功能，可啟用屬於傳送者要求特殊處理的特定流量(例如非預設服務品質(QoS)或即時服*務)的封包的標*記。

身份驗證和隱私功能

為IPv6指定了用於支援身份驗證、資料完整性和（可選）資料機密性的擴展。

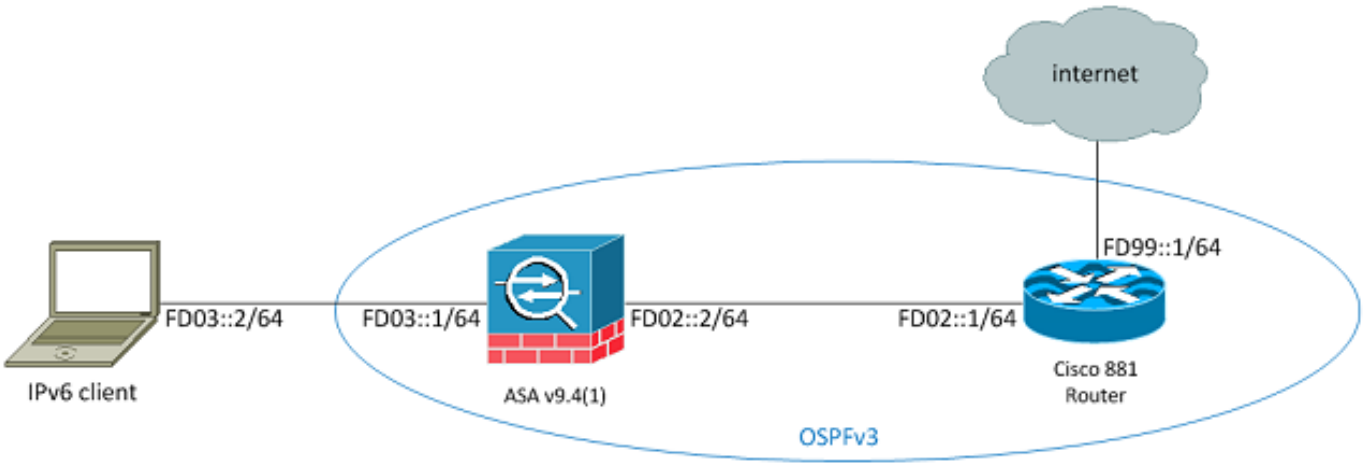
設定

本節介紹如何配置Cisco ASA以使用IPv6。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

本文檔中使用的示例為IPv6拓撲：



配置IPv6介面

為了通過ASA傳遞IPv6流量，必須首先在至少兩個介面上啟用IPv6。以下示例說明如何啟用IPv6，以便將流量從**Gi0/0上的內部介面傳遞到Gi0/1上的外部介面**：

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

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

現在，您可以在兩個介面上配置IPv6地址。

> **附註**：在本示例中，使用fc00::/7的唯一本地地址(ULA)空間中的地址，因此所有地址都以**FD**開頭(例如，fdxx:xxxx:xxxx....)。 此外，在寫入IPv6地址時，可以使用雙冒號(**::**)來表示一行0，以便**FD01::1/64**與**FD01:0000:0000:0000:0000:0000:0000:0000:00000:000001**相同。

```
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
```

現在，您應該具有到外部VLAN上地址為**fd02::1**的上游路由器的基本第2層(L2)/第3層(L3)連線。

```
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

與IPv4一樣，即使與直連子網中的主機存在IPv6連線，您仍然必須擁有通往外部網路的路由，以便知道如何到達它們。第一個示例展示如何配置靜態預設路由，以便通過下一跳地址為**fd02::1**的外部介面到達所有IPv6網路。

配置IPv6的靜態路由

使用以下資訊配置IPv6的靜態路由：

```
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)#
```

如圖所示，現在已連線到外部子網上的主機：

```
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)#
```

> **附註**：如果需要動態路由協定來處理IPv6的路由，您也可以進行配置。下一節將對此進行說明。

使用OSPFv3配置IPv6的動態路由

首先，您應該檢查上游Cisco 881系列整合多業務路由器(ISR)上的開放最短路徑優先版本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.
```

以下是相關的介面組態：

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

您可以使用ASA資料包捕獲驗證是否從外部介面上的ISR看到OSPF *Hello*資料包：

```
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)#
```

在上一次資料包捕獲中，您可以看到OSPF(ip-proto-89)資料包從IPv6本地鏈路地址到達，該地址對應於ISR上的正確介面：

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

現在，您可以在ASA上建立OSPFv3進程，以便與ISR建立鄰接關係：

```
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
```

將OSPF配置應用於ASA外部介面：

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

這應該會導致ASA在IPv6子網中傳送廣播OSPF Hello資料包。輸入show ipv6 ospf neighbor命令以驗證與路由器的鄰接關係：

```
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
```

您還可以確認ISR上的鄰居ID，因為預設情況下，ISR使用配置最高的IPv4地址作為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現在應該已經從ISR獲取預設IPv6路由。若要確認這一點，請輸入**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介面設定和路由功能的基本配置現已完成。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

IPv6連線的故障排除過程遵循大多數用於排除IPv4連線故障的方法，但略有差異。從故障排除的角度來看，IPv4和IPv6之間最重要的區別之一是IPv6中不再存在地址解析協定(ARP)。IPv6不是使用ARP來解析本地LAN網段上的IP地址，而是使用稱為鄰居發現(ND)的協定。

同樣重要的是要瞭解，ND利用網際網路控制訊息通訊協定第6版(ICMPv6)進行媒體存取控制(MAC)位址解析。有關IPv6 ND的詳細資訊，請參閱CLI手冊1的IPv6鄰居發現部分中的ASA IPv6配*置指南：Cisco ASA系列常規操作CLI配置指南9.4*或RFC 4861中。

目前，大多數與IPv6相關的故障排除都涉及ND、路由或子網配置問題。這可能是因為這也是IPv4和IPv6之間的主要區別。ND的工作方式與ARP不同，而內部網路定址也截然不同，因為IPv6極力不鼓勵使用NAT，而私有定址不再像IPv4那樣使用（在RFC 1918之後）。 一旦瞭解這些差異和/或解決了第2/L3層問題，第4層(L4)及更高層的故障排除過程與IPv4的故障排除過程基本相同，因為

TCP/UDP和更高層的協定功能基本相同（無論使用的IP版本如何）。

排除L2連線(ND)故障

用於IPv6的L2連線故障排除的最基本命令是**show ipv6 neighbor [nameif]**命令，該命令等效於IPv4的**show arp**。

以下是輸出範例：

```
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)#
```

在此輸出中，可以看到IPv6地址的成功解析**fd02::1**，它屬於MAC地址為**c471.fe93.b516的裝置**。

> **附註**：您可能會注意到，同一路由器介面MAC地址在先前輸出中出現兩次，因為路由器也具有此介面的自行分配的本地鏈路地址。本地鏈路地址是裝置特定的地址，只能用於直連網路上的通訊。路由器不通過本地鏈路地址轉發資料包，而是僅用於直連網段上的通訊。許多IPv6路由協定（如OSPFv3）使用本地鏈路地址來共用第2層網段上的路由協定資訊。

若要清除ND快取，請輸入**clear ipv6 neighbors**命令。如果特定主機的ND失敗，可以輸入**debug ipv6 nd**命令，還可以執行資料包捕獲並驗證系統日誌，以確定在L2級別發生哪些情況。請記住，IPv6 ND使用ICMPv6消息來解析IPv6地址的MAC地址。

IPv4 ARP與IPv6 ND

請考慮以下用於IPv4的ARP和用於IPv6的ND的比較表：

IPv4 ARP	IPv6 ND
ARP請求（誰有10.10.10.1？）	鄰居請求
ARP應答（10.10.10.1位於dead.dead.dead）	鄰居通告

在下一個場景中，ND無法解析位於外部介面上的*fd02::1*主機的MAC地址。

ND調試

以下是**debug ipv6 nd**命令的輸出：

```
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
```

在此調試輸出中，*似乎*從未收到來自**fd02::2**的鄰居通告。您可以檢查封包擷取，以確認是否實際發生這種情況。

ND資料包捕獲

> **附註**：從ASA 9.4(1)版開始，IPv6資料包捕獲仍需要訪問清單。已提交增強請求，以便使用Cisco錯誤ID CSCtn09836追蹤此情況。

設定存取控制清單(ACL)和封包擷取：

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

從ASA：發**起對fd02::1**的ping命令

```
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]
```

如封包擷取所示，系統會收到來自**fd02::1**的鄰居通告。但是，由於某種原因未處理播發，如調試輸出所示。為了進一步檢查，您可以檢視系統日誌。

ND系統日誌

以下是一些ND系統日誌示例：

```
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
```

在這些系統日誌中，您可以看到**fd02::1**處來自ISR的ND鄰居通告資料包由於未通過修改的擴展唯一識別符號(EUI)64（修改的EUI-64）格式檢查而被丟棄。

> **提示：**有關此特定問題的詳細資訊，請參閱本文檔的*修改的EUI-64地址編碼*部分。此疑難排解邏輯也可套用於各種捨棄原因，例如當ACL不允許特定介面上的ICMPv6時，或當發生單點傳送反向路徑轉送(uRPF)檢查失敗時，這兩種情況都可能導致IPv6的L2連線問題。

基本IPv6路由故障排除

使用IPv6時對路由協定的故障排除過程與使用IPv4時的故障排除過程基本相同。使用**debug**和**show**命令以及封包擷取可用於嘗試確定路由通訊協定沒有按預期運作的原因。

IPv6的路由協定調試

本節提供用於IPv6的有用調試命令。

全域性IPv6路由調試

您可以使用**debug ipv6 routing** 對所有IPv6路由表更改進行故障排除：

```
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調試

您可以使用**debug ipv6 ospf** 命令來排除OSPFv3故障：

```
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
```

以下是重新啟動OSPFv3進程後啟用的所有調試的示例輸出：

```
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
```

增強型內部閘道路由通訊協定(EIGRP)

ASA上的EIGRP不支援使用IPv6。請參閱CLI手冊1的EIGRP指導*一節：Cisco ASA系列常規操作CLI配置指南9.4版*，瞭解更多資訊。

邊界閘道通訊協定(BGP)

使用IPv6時，可以使用此**debug**命令來排除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>
```

用於IPv6的有用的Show命令

可以使用以下**show**命令來排除IPv6故障：

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

使用IPv6的封包追蹤器

在ASA上的IPv6中可採用與IPv4相同的方式使用內建的Packet Tracer功能。以下示例使用Packet Tracer功能來模擬**fd03::2**處的內部主機，該主機嘗試使用通過OSPF從**881**介面獲取的預設路由連線到Internet上的**555::1**的Web伺服器：

```
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#
```

請注意，輸出MAC地址是881介面的本地鏈路地址。如前所述，對於許多動態路由協定，路由器使用本地鏈路IPv6地址來建立鄰接關係。

與IPv6相關的ASA調試的完整清單

以下是可用於排除IPv6問題的調試：

```
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
```

常見的IPv6相關問題

本節介紹如何解決最常見的IPv6相關問題。

子網配置不正確

許多IPv6 TAC案例的產生是因為對IPv6的運作方式普遍缺乏瞭解，或者是因為管理員嘗試使用IPv4特定的流程來實施IPv6。

例如，TAC已發現網際網路服務提供商(ISP)為管理員分配了\56塊IPv6地址的情況。 然後，管理員將地址和完整的\56子網分配給ASA外部介面，並選擇一些內部範圍用於內部伺服器。但是，對於IPv6，所有內部主機也應使用可路由IPv6地址，並且IPv6地址塊應根據需要細分為較小的子網。在此方案中，您可以建立許多\64子網，作為已分配的\56塊的一部分。

> **提示：**請參閱RFC 4291以瞭解其他資訊。

修改的EUI 64編碼

可以配置ASA以要求修改的EUI-64編碼IPv6地址。根據RFC 4291,EUI允許主機為自己分配唯一的64位IPv6介面識別符號(EUI-64)。 此功能相對於IPv4是一項優勢，因為它消除了使用DHCP進行IPv6地址分配的要求。

如果ASA配置為需要通過**ipv6 enforce-eui64 nameif**命令進行此增強，則它可能會從本地子網上的其他主機丟棄許多鄰居發現請求和通告。

> **提示：**有關詳細資訊，請參閱瞭解IPv6 EUI-64位地址思科支援社群文檔。

客戶端預設使用臨時IPv6地址

預設情況下，許多客戶端作業系統(OS)（例如Microsoft Windows 7和8版、Macintosh OS-X以及基於Linux的系統）通過IPv6無狀態地址自動配置(SLAAC)使用自分配的臨時*IPv6地址來擴展隱私*。

Cisco TAC已遇到一些情況，由於主機從臨時地址而不是靜態分配的地址生成流量，因此這會導致環境中出現意外問題。因此，ACL和基於主機的路由可能導致流量被丟棄或路由不正確，從而導致主機通訊失敗。

有兩種方法可用於解決這種情況。可以在客戶端系統上單獨禁用此行為，也可以在ASA和Cisco IOS®路由器上禁用此行為。在ASA或路由器端，必須修改觸發此行為的路由器通告(RA)消息標誌。

請參閱以下各節，以在各個客戶端系統上禁用此行為。

Microsoft Windows

完成以下步驟，以便在Microsoft Windows系統上禁用此行為：

1. 在Microsoft Windows中，開啟提升的命令提示符（以管理員身份運行）。
2. 輸入以下命令可停用隨機IP位址產生功能，然後按下**Enter**鍵：

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

3. 輸入以下命令可強制Microsoft Windows使用EUI-64標準：

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

4. 重新啟動電腦以應用更改。

Macintosh OS-X

在終端機中，輸入以下命令可在下次重新啟動之前禁用主機上的IPv6 SLAAC:

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

若要將組態設定為永久，請輸入以下命令：

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

Linux

在終端shell中，輸入以下命令：

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

從ASA全域性禁用SLAAC

用於解決此行為的第二種方法是修改從ASA傳送到客戶端的RA消息，這將觸發SLAAC的使用。若要修改RA訊息，請在*介面組態模*式下輸入以下命令：

```
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傳送的RA消息，以便不設定A位標誌，並且客戶端不生成臨時IPv6地址。

提示：請參閱RFC 4941以瞭解其他資訊。

IPv6常見問題

本節介紹一些與IPv6的使用相關的常見問題。

是否可以同時在同一介面上傳遞IPv4和IPv6的流量？

會。您只需在介面上啟用IPv6，並為介面分配IPv4和IPv6地址，它同時處理兩種型別的流量。

是否可以將IPv6和IPv4 ACL同時應用於同一個介面？

您可以在早於版本9.0(1)的ASA版本中執行此操作。 自ASA 9.0(1)版起，ASA上的所有ACL都為*unified*，這意味著ACL支援相同ACL中混合使用IPv4和IPv6條目。

在ASA 9.0(1)及更高版本中，ACL僅合併在一起，而單個統一ACL通過**access-group**命令應用到介面。

ASA是否支援IPv6的QoS?

會。ASA支援IPv6的策略和優先順序隊列，與支援IPv4的方式相同。

自ASA 9.0(1)版起，ASA上的所有ACL都為*unified*，這意味著ACL支援相同ACL中混合使用IPv4和IPv6條目。因此，在匹配ACL的類對映上實施的任何QoS命令都會對IPv4和IPv6流量執行操作。

我應該將NAT與IPv6結合使用嗎？

雖然可以在ASA上為IPv6配置NAT，但是由於可用的、可全域性路由的IPv6地址數量幾乎是無限的，因此極不建議在IPv6中使用NAT，而且也不必要。

如果IPv6場景中需要NAT，您可以在CLI手冊2的IPv6 NAT指南部分找到有關如何配置NAT的更*多資訊：Cisco ASA系列防火牆CLI配置指南9.4*。

> **附註**：在使用IPv6實施NAT時應考慮一些准則和限制。

為什麼在*show failover*命令輸出中看到本地鏈路IPv6地址？

在IPv6中，ND使用本地鏈路地址來執行L2地址解析。因此，**show failover**命令輸出中受監控介面的IPv6地址會顯示本地鏈路地址，而不是介面上配置的全域性IPv6地址。這是預期行為。

已知警告/增強請求

以下是使用IPv6時的一些已知警告：

- 思科漏洞ID CSCtn09836 ââ âSA *ASA 8.x capture「match」子句未捕獲IPv6流量*
- 思科錯誤ID CSCuq85949 ââ Enhâ *ENH:適用於WCCP的ASA IPv6支援*
- 思科錯誤ID CSCut78380ââS â*ASA IPv6 ECMP路由無法負載平衡流量*

相關資訊

- RFC 2460 âInternetâ â協議第6版(IPv6)規範

- RFC 4291 ãâ Ipâ第6版定址架構
- RFC â 4861 IP第ãâ版本6(IPv6)的鄰居發現
- CLI手冊1:Cisco ASA系列常規操作CLI配置指南，9â.4â âIPv6
- AnyConnect SSL over IPv4+IPv6到ASA配置
- Cisco Systems技術â支ãâ與檔案