Configuración del ASA para pasar el tráfico IPv6

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Información sobre la Función IPv6
Descripción general de IPv6
Mejoras de IPv6 sobre IPv4
Capacidades de direccionamiento ampliadas
Simplificación del formato de encabezado
Soporte mejorado para extensiones y opciones
Capacidad de etiquetado de flujo
Funciones de autenticación y privacidad
Configurar
Diagrama de la red
Configuración de Interfaces para IPv6
Configuración del routing IPv6
Configuración del Ruteo Estático para IPv6
Configuración del Ruteo Dinámico para IPv6 con OSPFv3
Verificación
Troubleshoot
Resolución de problemas de conectividad L2 (ND)
ARP IPv4 frente a IPv6 ND
ND Debugs
Capturas de paquetes ND
ND Syslogs
Solución de problemas de routing IPv6 básico
Depuraciones de protocolo de ruteo para IPv6
Comandos show útiles para IPv6
Rastreadores de paquetes con IPv6
Lista completa de depuraciones de ASA relacionadas con IPv6
Problemas comunes relacionados con IPv6
Subredes configuradas incorrectamente
Codificación EUI 64 modificada
Los clientes utilizan direcciones IPv6 temporales de forma predeterminada
Preguntas frecuentes sobre IPv6
¿Puedo pasar tráfico para IPv4 e IPv6 en la misma interfaz al mismo tiempo?

¿Puedo aplicar ACL IPv6 e IPv4 a la misma interfaz?
¿El ASA admite QoS para IPv6?
¿Debo utilizar NAT con IPv6?
¿Por qué veo las direcciones IPv6 locales de link en el resultado del comando ***show failover***?
Solicitudes de advertencias/mejoras conocidas
Información Relacionada

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para pasar el tráfico de protocolo de Internet versión 6 (IPv6) en ASA versión 7.0(1) y posteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en las versiones 7.0(1) y posteriores de Cisco ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Actualmente, IPv6 es aún relativamente nuevo en términos de penetración en el mercado. Sin embargo, la asistencia para la configuración de IPv6 y las solicitudes de resolución de problemas han aumentado de forma constante. El propósito de este documento es atender esas necesidades y proporcionar:

- Descripción general del uso de IPv6
- Las configuraciones básicas de IPv6 en el ASA
- Información sobre cómo resolver problemas de conectividad IPv6 a través de ASA
- Una lista de los problemas y soluciones IPv6 más comunes, según lo identificado por el Cisco Technical Assistance Center (TAC)

Nota: Dado que IPv6 aún se encuentra en las primeras etapas como reemplazo de IPv4 a

nivel mundial, este documento se actualizará periódicamente para mantener la precisión y la relevancia.

Información sobre la Función IPv6

A continuación se ofrece información importante sobre la funcionalidad de IPv6:

- El protocolo IPv6 se introdujo por primera vez en ASA versión 7.0(1).
- El soporte para IPv6 en modo transparente se introdujo en la versión 8.2(1) de ASA.

Descripción general de IPv6

El protocolo IPv6 se desarrolló de mediados a finales de los años 90, principalmente debido al hecho de que el espacio público de direcciones IPv4 se desplazó rápidamente hacia el agotamiento. Aunque la traducción de direcciones de red (NAT) ayudó de forma drástica a IPv4 y retrasó este problema, se volvió innegable que finalmente se necesitaría un protocolo de reemplazo. El protocolo IPv6 se detalló oficialmente en RFC 2460 en diciembre de 1998. Puede leer más sobre el protocolo en el documento oficial RFC 2460, ubicado en el sitio web de Internet Engineering Task Force (IETF).

Mejoras de IPv6 sobre IPv4

Esta sección describe las mejoras que se incluyen con el protocolo IPv6 en comparación con el protocolo IPv4 anterior.

Capacidades de direccionamiento ampliadas

El protocolo IPv6 aumenta el tamaño de la dirección IP de 32 bits a 128 bits para admitir más niveles de jerarquía de direcciones, un número mucho mayor de nodos direccionables y una configuración automática de direcciones más sencilla. La escalabilidad del ruteo multicast se mejora mediante la adición de un *campo de alcance* a las direcciones multicast. Además, se define un nuevo tipo de dirección, denominada *dirección de difusión*. Esto se utiliza para enviar un paquete a cualquier nodo de un grupo.

Simplificación del formato de encabezado

Algunos campos de encabezado IPv4 se han eliminado o se han convertido en opcionales para reducir el costo de procesamiento de casos comunes de la gestión de paquetes y para limitar el costo de ancho de banda del encabezado IPv6.

Soporte mejorado para extensiones y opciones

Los cambios en la forma en que se codifican las opciones del encabezado IP permiten un reenvío más eficiente, límites menos estrictos en la longitud de las opciones y una mayor flexibilidad para

la introducción de nuevas opciones en el futuro.

Capacidad de etiquetado de flujo

Se agrega una nueva capacidad para habilitar el etiquetado de paquetes que pertenecen a *flujos* de tráfico específicos para los cuales el remitente solicita una gestión especial, como calidad de servicio (QoS) no predeterminada o servicio *en tiempo real*.

Funciones de autenticación y privacidad

Las extensiones que se utilizan para soportar la autenticación, la integridad de los datos y la confidencialidad (opcional) de los datos se especifican para IPv6.

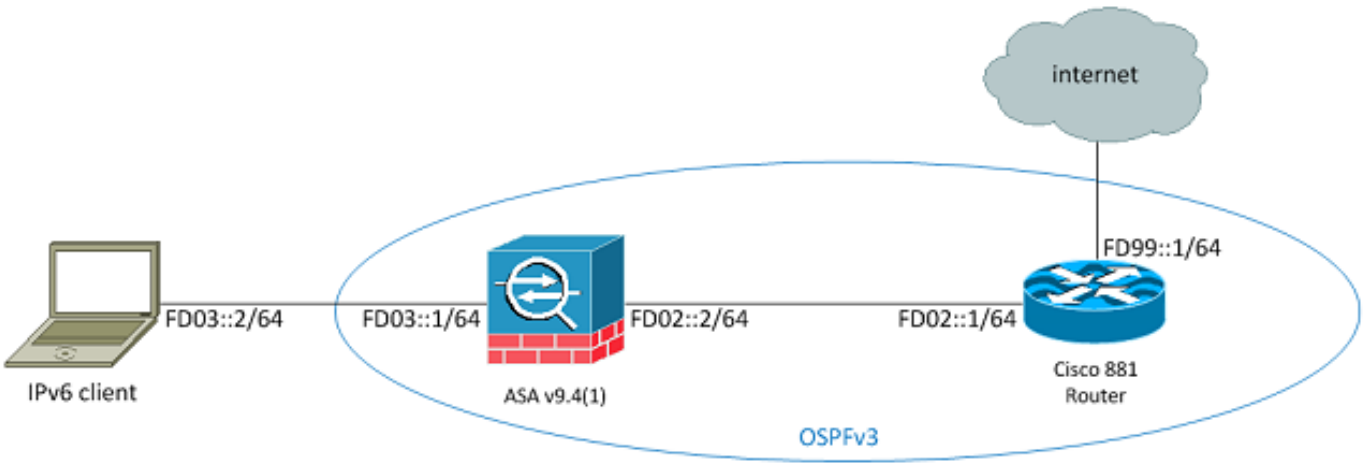
Configurar

Esta sección describe cómo configurar Cisco ASA para el uso de IPv6.

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Esta es la topología IPv6 para los ejemplos que se utilizan en este documento:



Configuración de Interfaces para IPv6

Para pasar el tráfico IPv6 a través de un ASA, primero debe habilitar IPv6 en al menos dos interfaces. Este ejemplo describe cómo habilitar IPv6 para pasar tráfico desde la interfaz interna en **Gi0/0** a la interfaz exterior en **Gi0/1**:

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

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

Ahora puede configurar las direcciones IPv6 en ambas interfaces.

> **Nota:** En este ejemplo, se utilizan las direcciones en el espacio de direcciones locales únicas (ULA) de fc00::/7, de modo que todas las direcciones comienzan con **FD** (como fdxx:xxxx:xxxx....). Además, cuando escribe direcciones IPv6, puede utilizar dos puntos (**::**) para representar una línea de ceros de modo que **FD01::1/64** sea igual que **FD01:0000:0000:0000:0000:000:0 000:0000:0001**.

```
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
```

Ahora debe tener la conectividad básica de Capa 2 (L2)/Capa 3 (L3) a un router ascendente en la VLAN externa en la dirección **fd02::1**:

```
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
```

Configuración del routing IPv6

Al igual que con IPv4, aunque hay conectividad IPv6 con los hosts en la subred conectada directamente, debe tener las rutas a las redes externas para saber cómo alcanzarlas. El primer ejemplo muestra cómo configurar una ruta estática predeterminada para alcanzar todas las redes IPv6 a través de la interfaz externa con una dirección de salto siguiente de **fd02::1**.

Configuración del Ruteo Estático para IPv6

Utilice esta información para configurar el ruteo estático para IPv6:

```
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)#
```

Como se muestra, ahora hay conectividad a un host en una subred externa:

```
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)#
```

> **Nota:** Si se desea un protocolo de ruteo dinámico para manejar el ruteo para IPv6, también puede configurarlo. Esto se describe en la siguiente sección.

Configuración del Ruteo Dinámico para IPv6 con OSPFv3

En primer lugar, debe examinar la configuración de Open Shortest Path First Version 3 (OSPFv3) en el router de servicios integrados (ISR) de Cisco serie 881 ascendente:

```
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.
```

Esta es la configuración de interfaz relevante:

```
C881#show run int Vlan302
```

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

Puede utilizar capturas de paquetes ASA para verificar que los paquetes OSPF *Hello* se vean desde el ISR en la interfaz exterior:

```
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)#
```

En la captura de paquetes anterior, puede ver que los paquetes OSPF (ip-proto-89) llegan de la dirección local de link IPv6, que corresponde a la interfaz correcta en el ISR:

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

Ahora puede crear un proceso OSPFv3 en el ASA para establecer una adyacencia con el ISR:

```
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
```

Aplique la configuración OSPF a la interfaz externa ASA:

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

Esto debería hacer que el ASA envíe los paquetes OSPF Hello de difusión en la subred IPv6. Ingrese el comando **show ipv6 ospf neighbor** para verificar la adyacencia con el router:

```
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
```

También puede confirmar el ID de vecino en el ISR, ya que utiliza la dirección IPv4 configurada más alta para el ID de forma predeterminada:

```
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#
```

El ASA ahora debería haber aprendido la ruta IPv6 predeterminada del ISR. Para confirmar esto, ingrese el comando **show ipv6 route**:

```
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#
```

La configuración básica de los parámetros de interfaz y las funciones de routing para IPv6 en el ASA ya ha finalizado.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Los procedimientos de resolución de problemas para la conectividad IPv6 siguen la mayor parte de la misma metodología utilizada para resolver problemas de conectividad IPv4, con algunas diferencias. Desde la perspectiva de la solución de problemas, una de las diferencias más importantes entre IPv4 e IPv6 es que el protocolo de resolución de direcciones (ARP) ya no existe en IPv6. En lugar de utilizar ARP para resolver las direcciones IP en el segmento LAN local, IPv6 utiliza un protocolo denominado Neighbor Discovery (ND).

También es importante comprender que ND aprovecha el protocolo de mensajes de control de Internet versión 6 (ICMPv6) para la resolución de direcciones de control de acceso a medios (MAC). Puede encontrar más información sobre IPv6 ND en la guía de configuración de ASA IPv6 de la sección Detección de Vecinos IPv6 del *Libro CLI 1: Guía de Configuración de la CLI de Cisco ASA Series General Operations, 9.4* o en RFC 4861.

Actualmente, la mayoría de los problemas relacionados con IPv6 incluyen problemas de configuración de subred, enrutamiento o ND. Esto se debe probablemente al hecho de que estas son también las principales diferencias entre IPv4 e IPv6. ND funciona de forma diferente que ARP, y el direccionamiento de red interna también es muy diferente, ya que el uso de NAT se desaconseja mucho en IPv6 y el direccionamiento privado ya no se aprovecha de la forma en que estaba en IPv4 (después de RFC 1918). Una vez que se entienden estas diferencias y/o se resuelven los problemas de L2/L3, el proceso de solución de problemas en la capa 4 (L4) y superiores es esencialmente el mismo que el utilizado para IPv4 porque los protocolos TCP/UDP y de capa superior funcionan esencialmente igual (independientemente de la versión IP que se utilice).

Resolución de problemas de conectividad L2 (ND)

El comando más básico que se utiliza para resolver problemas de conectividad L2 con IPv6 es el comando **show ipv6 neighbor [nameif]**, que es el equivalente del comando **show arp** para IPv4.

A continuación se presenta un ejemplo de salida:

```
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)#
```

En este resultado, puede ver la resolución exitosa para la dirección IPv6 de **fd02::1**, que pertenece al dispositivo con una dirección MAC de **c471.fe93.b516**.

> **Nota:** Es posible que observe que la misma dirección MAC de la interfaz del router aparece dos veces en la salida anterior porque el router también tiene una dirección local de link autoasignada para esta interfaz. La dirección local del link es una dirección específica del dispositivo que sólo se puede utilizar para la comunicación en la red conectada directamente. Los routers no reenvían paquetes a través de direcciones locales de link, sino que más bien son sólo para la comunicación en el segmento de red directamente conectado. Muchos protocolos de ruteo IPv6 (como OSPFv3) utilizan direcciones locales de link para compartir información de protocolo de ruteo en el segmento L2.

Para borrar la memoria caché ND, ingrese el comando **clear ipv6 neighbors**. Si el ND falla para un host determinado, puede ingresar el comando **debug ipv6 and**, así como realizar capturas de paquetes y verificar los registros del sistema, para determinar lo que ocurre en el nivel L2. Recuerde que IPv6 ND utiliza mensajes ICMPv6 para resolver las direcciones MAC para las direcciones IPv6.

ARP IPv4 frente a IPv6 ND

Considere esta tabla de comparación de ARP para IPv4 y ND para IPv6:

ARP IPv4	IPv6 ND
PETICIÓN ARP (Quién tiene 10.10.10.1?)	Solicitud de vecino
ARP REPLY (10.10.10.1 está en dead.dead.dead)	Anuncio de vecino

En el siguiente escenario, el ND no puede resolver la dirección MAC del host *fd02::1* que se encuentra en la interfaz exterior.

ND Debugs

A continuación se muestra el resultado del comando **debug ipv6 nd**:

```
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
```

En este resultado de depuración, *parece* que los Anuncios de Vecino de **fd02::2** nunca se reciben. Puede verificar las capturas de paquetes para confirmar si este es realmente el caso.

Capturas de paquetes ND

> **Nota:** A partir de la versión 9.4(1) de ASA, las listas de acceso siguen siendo necesarias para las capturas de paquetes IPv6. Se ha presentado una solicitud de mejora para realizar un seguimiento de esto con el ID de bug de Cisco CSCtn09836.

Configure la Lista de control de acceso (ACL) y las capturas de paquetes:

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

Inicie un ping a **fd02::1** desde el ASA:

```
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]
```

Como se muestra en las capturas de paquetes, se reciben los Anuncios de Vecino de **fd02::1**. Sin embargo, los anuncios no se procesan por alguna razón, como se muestra en las salidas de depuración. Para un examen más detallado, puede ver los syslogs.

ND Syslogs

A continuación se muestra un ejemplo de los syslogs ND:

```
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
```

Dentro de estos syslogs, puede ver que los paquetes de anuncio de ND Neighbor del ISR en **fd02::1** se descartan debido a las verificaciones fallidas del formato Modified Extended Unique Identifier (EUI) 64 (Modified EUI-64).

> **Consejo:** Consulte la sección *Codificación de Direcciones EUI-64 Modificada* de este documento para obtener más información sobre este problema específico. Esta lógica de solución de problemas también se puede aplicar a todos los tipos de motivos de caída, como cuando las ACL no permiten ICMPv6 en una interfaz específica o cuando se producen fallos de verificación de Unicast Reverse Path Forwarding (uRPF), que pueden causar problemas de conectividad L2 con IPv6.

Solución de problemas de routing IPv6 básico

Los procedimientos de resolución de problemas para los protocolos de ruteo cuando se utiliza IPv6 son esencialmente los mismos que cuando se utiliza IPv4. El uso de los comandos **debug** y **show**, así como las capturas de paquetes, son útiles con intentos de determinar la razón por la que un protocolo de ruteo no se comporta como se esperaba.

Depuraciones de protocolo de ruteo para IPv6

Esta sección proporciona los útiles comandos debug para IPv6.

Depuraciones globales de routing IPv6

Puede utilizar el comando **debug ipv6 routing** debug para resolver todos los cambios de la tabla de ruteo IPv6:

```
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
```

Depuraciones de OSPFv3

Puede utilizar el comando **debug ipv6 ospf** para resolver problemas de OSPFv3:

```
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
```

Este es un ejemplo de salida para todas las depuraciones que se habilitan después de reiniciar el proceso OSPFv3:

```
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
```

Protocolo de routing de gateway interior mejorado (EIGRP)

El EIGRP en el ASA no admite el uso de IPv6. Consulte la sección Pautas para EIGRP del *Libro CLI 1: Guía de Configuración de Cisco ASA Series General Operations CLI, 9.4* para obtener más información.

Border Gateway Protocol (BGP)

Este comando **debug** se puede utilizar para resolver problemas de BGP cuando se utiliza IPv6:

```
ASAv# debug ip bgp ipv6 unicast  ?

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

Comandos show útiles para IPv6

Puede utilizar estos comandos **show** para resolver problemas de IPv6:

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

Rastreadores de paquetes con IPv6

Puede utilizar la funcionalidad de seguimiento de paquetes integrada con IPv6 en el ASA de la misma manera que con IPv4. Aquí hay un ejemplo donde se utiliza la funcionalidad de packet-tracer para simular el host interno en **fd03::2**, que intenta conectarse a un servidor web en **5555::1** que se encuentra en Internet con la ruta predeterminada que se aprende de la interfaz **881** a través de OSPF:

```
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#
```

Observe que la dirección MAC de egreso es la dirección local del link de la interfaz 881. Como se mencionó anteriormente, para muchos protocolos de ruteo dinámicos, los routers utilizan direcciones IPv6 locales de link para establecer adyacencias.

Lista completa de depuraciones de ASA relacionadas con IPv6

Estos son los debugs que se pueden utilizar para resolver problemas de IPv6:

```
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
```

Problemas comunes relacionados con IPv6

Esta sección describe cómo resolver los problemas más comunes relacionados con IPv6.

Subredes configuradas incorrectamente

Muchos casos del TAC de IPv6 se generan debido a una falta general de conocimientos sobre cómo funciona IPv6 o a intentos del administrador de implementar IPv6 con el uso de procesos específicos de IPv4.

Por ejemplo, el TAC ha visto casos en los que un proveedor de servicios de Internet (ISP) ha asignado un bloque \56 de direcciones IPv6 a un administrador. A continuación, el administrador asigna una dirección y la subred \56 completa a la interfaz externa de ASA y elige algún rango interno para utilizar en los servidores internos. Sin embargo, con IPv6, todos los hosts internos también deben utilizar direcciones IPv6 enrutables, y el bloque de direcciones IPv6 debe dividirse en subredes más pequeñas según sea necesario. En este escenario, puede crear muchas subredes \64 como parte del bloque \56 que se ha asignado.

> **Consejo:** Consulte RFC 4291 para obtener información adicional.

Codificación EUI 64 modificada

El ASA se puede configurar para requerir direcciones IPv6 codificadas por EUI-64 modificadas. La EUI, según RFC 4291, permite que un host se asigne un identificador de interfaz IPv6 único de 64 bits (EUI-64). Esta función es una ventaja sobre IPv4, ya que elimina el requisito de utilizar DHCP para la asignación de direcciones IPv6.

Si el ASA se configura para requerir esta mejora a través del comando **ipv6 enforce-eui64 nameif**, es probable que descarte muchas solicitudes y anuncios de Neighbor Discovery de otros hosts en la subred local.

> **Consejo:** Para obtener más información, consulte el documento Introducción a IPv6 EUI-64 Bit Address Cisco Support Community.

Los clientes utilizan direcciones IPv6 temporales de forma predeterminada

De forma predeterminada, muchos sistemas operativos de cliente (OS), como Microsoft Windows

versiones 7 y 8, Macintosh OS-X y sistemas basados en Linux, utilizan direcciones IPv6 *temporales* autoasignadas para ampliar la privacidad mediante la configuración automática de direcciones sin estado (SLAAC) IPv6.

El TAC de Cisco ha visto algunos casos en los que esto causó problemas inesperados en entornos porque los hosts generan tráfico a partir de la dirección temporal y no de la dirección asignada estáticamente. Como resultado, las ACL y las rutas basadas en el host pueden hacer que el tráfico se pierda o se rutee incorrectamente, lo que hace que la comunicación del host falle.

Hay dos métodos que se utilizan para abordar esta situación. El comportamiento se puede inhabilitar individualmente en los sistemas cliente, o puede inhabilitar este comportamiento en los routers ASA y Cisco IOS®. En el lado de ASA o del router, debe modificar el indicador de mensaje de anuncio de router (RA) que activa este comportamiento.

Consulte las secciones siguientes para inhabilitar este comportamiento en los sistemas de clientes individuales.

Microsoft Windows

Complete estos pasos para inhabilitar este comportamiento en los sistemas Microsoft Windows:

1. En Microsoft Windows, abra un símbolo del sistema elevado (ejecute como administrador).

2. Ingrese este comando para inhabilitar la función de generación aleatoria de direcciones IP y luego presione **Intro**:

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

3. Ingrese este comando para obligar a Microsoft Windows a utilizar el estándar EUI-64:

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

4. Reinicie la máquina para aplicar los cambios.

Macintosh OS-X

En un terminal, ingrese este comando para inhabilitar el SLAAC IPv6 en el host hasta el siguiente reinicio:

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

Para hacer que la configuración sea permanente, ingrese este comando:

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

Linux

En un shell de terminal, ingrese este comando:

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

Desactivar SLAAC globalmente desde el ASA

El segundo método que se utiliza para abordar este comportamiento es modificar el mensaje RA

que se envía desde el ASA a los clientes, lo que activa el uso de SLAAC. Para modificar el mensaje RA, ingrese este comando desde el modo *Configuración de la Interfaz*:

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

Este comando modifica el mensaje RA que envía el ASA para que no se establezca el indicador A-bit y los clientes no generen una dirección IPv6 temporal.

> **Consejo:** Consulte RFC 4941 para obtener información adicional.

Preguntas frecuentes sobre IPv6

En esta sección se describen algunas preguntas frecuentes sobre el uso de IPv6.

¿Puedo pasar tráfico para IPv4 e IPv6 en la misma interfaz al mismo tiempo?

Yes. Simplemente debe habilitar IPv6 en la interfaz y asignar una dirección IPv4 y una dirección IPv6 a la interfaz, y gestiona ambos tipos de tráfico simultáneamente.

¿Puedo aplicar ACL IPv6 e IPv4 a la misma interfaz?

Puede hacerlo en las versiones de ASA anteriores a la versión 9.0(1). A partir de la versión 9.0(1) de ASA, todas las ACL en el ASA están *unificadas*, lo que significa que una ACL soporta una mezcla de entradas IPv4 e IPv6 en la misma ACL.

En las versiones 9.0(1) y posteriores de ASA, las ACL simplemente se fusionan juntas y la ACL unificada única se aplica a la interfaz a través del comando **access-group**.

¿El ASA admite QoS para IPv6?

Yes. El ASA admite políticas y colas de prioridad para IPv6 de la misma manera que lo hace con IPv4.

A partir de la versión 9.0(1) de ASA, todas las ACL en el ASA están *unificadas*, lo que significa que una ACL soporta una mezcla de entradas IPv4 e IPv6 en la misma ACL. Como resultado, cualquier comando de QoS que se implemente en un mapa de clase que coincida con una ACL tomará acción tanto en el tráfico IPv4 como en el tráfico IPv6.

¿Debo utilizar NAT con IPv6?

Aunque NAT se puede configurar para IPv6 en el ASA, el uso de NAT en IPv6 es altamente desalentado e innecesario, dada la cantidad casi infinita de direcciones IPv6 disponibles y globalmente enrutables.

Si se requiere NAT en un escenario de IPv6, puede encontrar más información sobre cómo configurarlo en la sección Pautas de NAT IPv6 del *Libro 2 de la CLI: Guía de Configuración de Cisco ASA Series Firewall CLI, 9.4*.

> **Nota:** Hay algunas pautas y limitaciones que deben tenerse en cuenta cuando se implementa NAT con IPv6.

¿Por qué veo las direcciones IPv6 locales de link en el resultado del comando *show failover*?

En IPv6, ND utiliza direcciones locales de link para realizar la resolución de direcciones L2. Por esta razón, las direcciones IPv6 para las interfaces monitoreadas en la salida del comando **show failover** muestran la dirección local del link y no la dirección IPv6 global configurada en la interfaz. Debe ocurrir lo siguiente.

Solicitudes de advertencias/mejoras conocidas

A continuación se presentan algunas advertencias conocidas con respecto al uso de IPv6:

- El Id. de bug Cisco CSCtn09836 âÂ Â *La cláusula "match" de captura ASA 8.x no detecta el tráfico IPv6*
- Id. de bug Cisco CSCuq85949 âÂ Â *ENH: Compatibilidad con ASA IPv6 para WCCP*
- Id. de error de Cisco CSCut78380 âÂ *El routing ECMP de IPv6 de ASA no equilibra la carga del tráfico*

Información Relacionada

- RFC 2460 Especificación protocolo de Internet, versión 6 (IPv6)
- RFC 4291. Â arquitectura de direccionamiento de IP versión 6
- RFC 4861 (Â Neighbor Discovery para IP versión 6 (IPv6)
- Libro CLI 1: Guía de Configuración de CLI de Cisco ASA Series General Operations, 9.4 â Â IPv6
- Configuración de AnyConnect SSL sobre IPv4+IPv6 a ASA
- Soporte técnico y documentaciónâÂÂ Cisco Systems