# Configure el ASA para pasar el tráfico del IPv6

## Contenido

# Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) para pasar el tráfico de la versión 6 del protocolo de Internet (IPv6) en las Versiones de ASA 7.0(1) y posterior.

# Prerequisites

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

# Antecedentes

Actualmente, el IPv6 sigue siendo relativamente nuevo en términos de penetración de mercado. Sin embargo, la asistencia para la configuración del IPv6 y las peticiones del troubleshooting han aumentado constantemente. El propósito de este documento es dirigir esas necesidades y proporcionar:

- Una descripción general del uso del IPv6
- Las configuraciones básicas del IPv6 en el ASA
- Información sobre cómo resolver problemas la Conectividad del IPv6 con el ASA
- Una lista de los problemas y de las soluciones mas comunes del IPv6, según lo identificado

por el Centro de Asistencia Técnica de Cisco (TAC)

**Note**: Dado que el IPv6 todavía está en las fases tempranas como reemplazo del IPv4 global, este documento será periódicamente actualizado para mantener la exactitud y la importancia.

## Información de la característica del IPv6

Aquí está una cierta información importante sobre las funciones del IPv6:

- El protocolo del IPv6 primero fue introducido en la Versión de ASA 7.0(1).
- El soporte para el IPv6 en el modo transparente fue introducido en la Versión de ASA 8.2(1).

## Descripción del IPv6

El protocolo del IPv6 fue desarrollado al mediados de a los últimos años 90, sobre todo debido al hecho de que el espacio de la dirección público del IPv4 se movió rápidamente hacia el agotamiento. Aunque el Network Address Translation (NAT) ayudara dramáticamente al IPv4 y retrasara este problema, llegó a ser innegable que un protocolo del reemplazo sería eventual necesario. El protocolo del IPv6 fue detallado oficialmente en el RFC 2460 en diciembre 1998. Usted puede leer más sobre el protocolo en el documento oficial del RFC 2460, situado en el sitio web de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF).

## Mejoras del IPv6 sobre el IPv4

Esta sección describe las mejoras que se incluyen con el protocolo del IPv6 contra el más viejo protocolo del IPv4.

### Capacidades de dirección ampliadas

El protocolo del IPv6 aumenta el tamaño de la dirección IP a partir de 32 bits a los bits 128 para soportar más niveles de dirigir la jerarquía, un número mucho mayor de Nodos direccionables, y una autoconfiguración más simple de los direccionamientos. El scalability del ruteo multicast es mejorado mediante la adición de un campo del *alcance a las* direcciones Multicast. Además, un tipo nuevo de direccionamiento, llamó *dirección Anycast*, se define. Esto se utiliza para enviar un paquete a cualquier un nodo en un grupo.

### Simplificación del formato de encabezamiento

Se han caído o se han hecho algunos campos del encabezado del IPv4 opcionales para reducir el costo de procesamiento del común-caso del paquete que dirigía y para limitar el costo de ancho de banda de la encabezado del IPv6.

### Soporte mejorado para las Extensiones y las opciones

Cambia de la manera que las opciones del encabezado IP se codifican tienen en cuenta la expedición más eficiente, los límites menos rigurosos en la longitud de las opciones, y la mayor flexibilidad para la introducción de nuevas opciones en el futuro.

#### Capacidad de etiquetado del flujo

Una nueva capacidad se agrega para habilitar el etiquetado de los paquetes que pertenecen a los *flujos del* tráfico determinado para los cuales el remitente pide la dirección especial, tal como Calidad de Servicio (QoS) no valor por defecto o *servicio en tiempo real*.

#### Capacidades de la autenticación y de la aislamiento

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

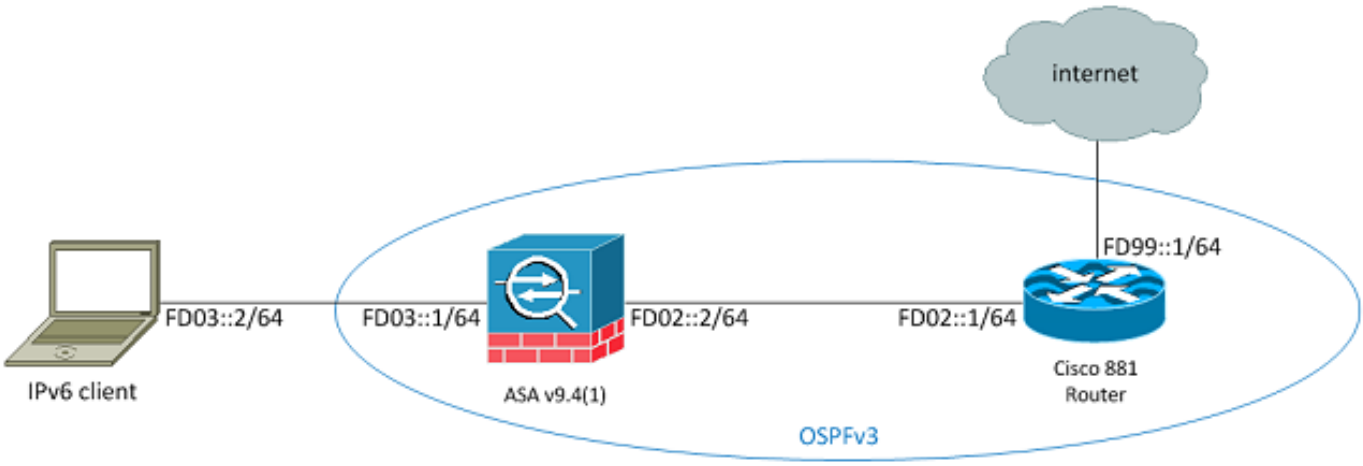
# Configurar

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

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

## Diagrama de la red

Ésta es la topología del IPv6 por los ejemplos que se utilizan en este documento:




## Interfaces de la configuración para el IPv6

Para pasar el tráfico del IPv6 con un ASA, usted debe primero habilitar el IPv6 en por lo menos dos interfaces. Este ejemplo describe cómo permitir al IPv6 para pasar el tráfico de la interfaz

interior 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
```

Usted puede ahora configurar los direccionamientos del IPv6 en ambas interfaces.

> **Note**: En este ejemplo, los direccionamientos en el espacio único de las direcciones locales (ULA) de fc00::/7 se utilizan, así que todos los direccionamientos comienzan con el **FD** (por ejemplo, fdxx: xxxx: xxxx….). También, cuando usted escribe los direccionamientos del IPv6, usted puede utilizar los dos puntos dobles (**::**) para representar una línea de ceros de modo que **FD01::1/64** sea lo mismo que **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
```

Usted debe ahora tener la capa básica 2 Conectividad (L2)/Layer 3 (L3) a un router ascendente en el VLA N exterior en el direccionamiento **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
```

## El rutear del IPv6 de la configuración

Igual que con el IPv4, aunque hay Conectividad del IPv6 con los host en la subred conectada directamente, usted debe todavía tener las rutas a las redes externas para saber alcanzarlas. El primer ejemplo muestra cómo configurar una Static Default ruta para alcanzar todas las redes del IPv6 vía la interfaz exterior con una dirección del salto siguiente de **fd02::1**.

### Static Routing de la configuración para el IPv6

Utilice esta información para configurar el Static Routing para el 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)#
```

> **Note**: Si un Dynamic Routing Protocol se desea para manejar la encaminamiento para el IPv6, después usted puede configurar eso también. Esto se describe en la siguiente sección.

## Dynamic Routing de la configuración para el IPv6 con OSPFv3

Primero, usted debe examinar la configuración abierta del trayecto más corto primero versión 3 (OSPFv3) en el router por aguas arriba de los Servicios integrados de las Cisco 881 Series (ISR):

```
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.
```

Aquí está la configuración de la interfaz pertinente:

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

Usted puede utilizar a las capturas de paquetes ASA para verificar que los paquetes OSPF de saludo están vistos del 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 del paquete anterior, usted puede ver que los paquetes OSPF (**ip-proto-89**) llegan de la dirección local del link del 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#
```

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

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

```
FD02::1
C881#
```

Aplique la configuración de OSPF a la interfaz exterior ASA:

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

Esto debe hacer el ASA enviar los paquetes OSPF de saludo del broadcast en la subred del IPv6. Ingrese el **comando neighbor OSPF del IPv6 de la demostración** 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
```

Usted puede también confirmar el ID de vecino en el ISR, pues utiliza el direccionamiento configurado más alto del IPv4 para el ID por abandono:

```
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 debe ahora haber aprendido la ruta predeterminada del IPv6 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 las configuraciones y de las funciones de ruteo de la interfaz para el IPv6 en el ASA es completa ahora.

# Verificación

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

# Troubleshooting

Los procedimientos deTroubleshooting para la Conectividad del IPv6 siguen la mayor parte de la misma metodología que se utiliza para resolver problemas la Conectividad del IPv4, con algunas diferencias. De una perspectiva del troubleshooting, una de las diferencias más importantes entre el IPv4 y el IPv6 es que el Address Resolution Protocol (ARP) existe no más en el IPv6. En vez del uso del ARP para resolver los IP Addresses en el segmento local de LAN, el IPv6 utiliza un protocolo llamado la detección de vecino (ND).

Es también importante entender esa versión 6 (ICMPv6) del protocolo Protocolo de control de mensajes de Internet (ICMP) de las palancadas ND para el address resolution del Media Access Control (MAC). Más información sobre el IPv6 ND se puede encontrar en la guía de configuración del IPv6 ASA en la sección de la detección de vecino del IPv6 del *libro 1 CLI: Guía de configuración CLI de los funcionamientos generales de la serie de Cisco ASA, 9.4* o en el RFC 4861.

Actualmente, la mayoría del troubleshooting relacionado a IPv6 implica el ND, la encaminamiento, o los problemas de la configuración de subred. Ésta es probablemente a causa al hecho de que éstas son también las diferencias fundamentales entre el IPv4 y el IPv6. Los trabajos ND diferentemente que el ARP, y la dirección de la red interna es también muy diferentes, pues el uso del NAT se desalienta altamente en el IPv6 y el direccionamiento privado no más leveraged la manera que era en el IPv4 (después del RFC 1918). Una vez que se entienden estas diferencias y/o se resuelven los problemas L2/L3, el proceso de Troubleshooting en la capa 4 (L4) y arriba es esencialmente lo mismo que ése usado para el IPv4 porque funcionan el TCP/UDP y los protocolos de capa más altas esencialmente lo mismo (sin importar versión IP se utiliza que).

## Conectividad del Troubleshooting L2 (ND)

La mayoría del comando básico que se utiliza para resolver problemas la Conectividad L2 con el IPv6 es el comando **vecino del [nameif] del IPv6 de la demostración**, que es el equivalente de la **demostración arp** para el 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 esta salida, usted puede ver la resolución acertada para el direccionamiento del IPv6 de **fd02::1**, que pertenece al dispositivo con una dirección MAC de **c471.fe93.b516**.

> **Note**: Usted puede ser que note que la dirección MAC de la interfaz del mismo router aparece dos veces en la salida anterior porque el router también tiene una dirección local del link autoasignada para esta interfaz. La dirección local del link es un direccionamiento dispositivo-específico que se puede utilizar solamente para la comunicación sobre la red con conexión directa. El Routers no remite los paquetes vía las direcciones locales del link, sino que él está bastante solamente para la comunicación sobre el segmento de la red con conexión directa. Muchos Routing Protocol del IPv6 (tales como OSPFv3) utilizan a las direcciones locales del link para compartir la información del Routing Protocol sobre el segmento L2.

Para borrar el caché ND, ingrese el **comando neighbors claro del IPv6**. Si el ND falla para un host determinado, usted puede ingresar el comando **nd del IPv6 del debug**, así como realiza a las capturas de paquetes y verifica los Syslog, para determinar el que ocurra en el nivel L2. Recuerde que el IPv6 ND utiliza los mensajes ICMPv6 para resolver las direcciones MAC para los direccionamientos del IPv6.

## IPv4 ARP contra el IPv6 ND

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

| IPv4 ARP | IPv6 ND |
|---|---|
| PEDIDO ARP (quién tiene 10.10.10.1?) | Solicitud de vecino |
| RESPUESTA ARP (10.10.10.1 está en dead.dead.dead) | Anuncio de vecino |

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

## Debugs ND

Aquí está la salida del comando **nd del IPv6 del debug**:

```
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 esta salida de los debugs, *aparece* que los anuncios de vecino de **fd02::2** nunca están recibidos. Usted puede marcar a las capturas de paquetes para confirmar si éste es realmente el caso.

## Capturas de paquetes ND

> **Note**: A partir de la versión ASA 9.4(1), las listas de acceso todavía se requieren para las capturas de paquetes del IPv6. Un pedido de mejora se ha clasifiado para seguir esto con el Id. de bug Cisco CSCtn09836.

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

```
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
```

Inicie un ping a **fd02::1 del** 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]
```

Tal y como se muestra en de las capturas de paquetes, los anuncios de vecino de **fd02::1** se reciben. Sin embargo, los anuncios no se procesan por alguna razón, tal y como se muestra en de las salidas de los debugs. Para el examen adicional, usted puede ver los Syslog.

## Syslog ND

Aquí están algunos Syslog del ejemplo 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 Syslog, usted puede ver que los paquetes del anuncio de vecino ND del ISR en **fd02::1** son caído debido al Identificador único extendido modificado fallado (EUI) 64 controles del

formato (EUI-64 modificado).

> **Tip**: Refiera a la sección *modificada de la codificación del direccionamiento EUI-64 de* este documento para más información sobre este problema específico. Esta lógica del troubleshooting se puede aplicar a toda clase de razones del descenso también, por ejemplo cuando los ACL no permiten el ICMPv6 en una interfaz específica o cuando ocurren los errores del control del Unicast Reverse Path Forwarding (uRPF), que pueden causar los problemas de conectividad L2 con el IPv6.

## El rutear básico del IPv6 del Troubleshooting

Los procedimientos deTroubleshooting para los Routing Protocol cuando se utiliza el IPv6 son esencialmente lo mismo que ésos cuando se utiliza el IPv4. El uso de los **comandos debug and show**, así como de las capturas de paquetes, es útil con las tentativas de comprobar la razón que un Routing Protocol no se comporta como se esperaba.

### Debugs del Routing Protocol para el IPv6

Esta sección proporciona los comandos debug útiles para el IPv6.

#### *IPv6 global que rutea los debugs*

Usted puede utilizar el **IPv6 del debug que rutea el** debug para resolver problemas todos los cambios de la tabla de ruteo del 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
```

### *Debugs OSPFv3*

Usted puede utilizar el **comando ospf del IPv6 del debug** para resolver problemas los problemas 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
```

Aquí está una salida de ejemplo para todos los debugs se habiliten que después de que se recomience 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
```

### *Enhanced Interior Gateway Routing Protocol (EIGRP)*

El EIGRP en el ASA no soporta el uso del IPv6. Refiera a las guías de consulta para la sección del EIGRP del *libro 1 CLI: Guía de configuración CLI de los funcionamientos generales de la serie de Cisco ASA, 9.4* para más información.

### *Border Gateway Protocol (BGP)*

Este **comando debug** puede ser utilizado para resolver problemas el BGP cuando se utiliza el 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 el IPv6

Usted puede utilizar estos **comandos show** para resolver problemas los problemas del IPv6:

- **show ipv6 route**
- **show ipv6 interface brief**
- **muestre el OSPF del IPv6 <process ID>**
- **muestre el tráfico del IPv6**
- **muestre al vecino del IPv6**
- **muestre el ICMP del IPv6**

## Trazalíneas del paquete con el IPv6

Usted puede utilizar las funciones incorporadas del trazalíneas del paquete con el IPv6 en el ASA igual que con el IPv4. Aquí está un ejemplo donde las funciones del paquete-trazalíneas se utilizan para simular el host interior en **fd03::2**, que intenta conectar con un servidor Web en **5555::1** que esté situado en Internet con la ruta predeterminado que es docta de la interfaz **881** vía el 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#
```

Note que la dirección MAC de la salida es la dirección local del link de la interfaz 881. Según lo mencionado previamente, para muchos Dynamic Routing Protocol, el IPv6 del local de la conexión del uso del Routers dirige para establecer las adyacencias.

## Lista completa de debugs relacionados a IPv6 ASA

Aquí están los debugs que se pueden utilizar para resolver problemas los problemas del 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 relacionados a IPv6 comunes

Esta sección describe cómo resolver problemas los problemas relacionados a IPv6 mas comunes.

### Subredes incorrectamente configuradas

Muchos casos TAC del IPv6 son generado debido a una falta general de conocimiento sobre cómo funciona el IPv6, o debido al administrador intenta implementar el IPv6 con el uso de los procesos IPv4-specific.

Por ejemplo, TAC ha visto los casos donde un Proveedor de servicios de Internet (ISP) ha

asignado un administrador un bloque \56 de los direccionamientos del IPv6. El administrador después asigna un direccionamiento y la subred completa \56 a la interfaz exterior ASA y elige un cierto rango interno para utilizar para los servidores interiores. Sin embargo, con el IPv6, todos los host internos deben también utilizar los direccionamientos del IPv6 del routable, y el bloqueo de dirección del IPv6 se debe analizar en subredes más pequeñas según las necesidades. En este escenario, usted puede crear muchas subredes \64 mientras que una parte del bloque \56 se ha afectado un aparato que.

> **Tip**: Refiera al RFC 4291 para la información adicional.

### Codificación modificada EUI 64

El ASA se puede configurar para requerir los direccionamientos modificados del IPv6 EUI-64-encoded. El EUI, según el RFC 4291, permite que un host se asigne un identificador 64-bit único de la interfaz del IPv6 (EUI-64). Esta característica es una ventaja sobre el IPv4, pues quita el requisito de utilizar el DHCP para la asignación de dirección del IPv6.

Si el ASA se configura para requerir esta mejora vía el **comando nameif del IPv6 enforce-eui64**, después caerá probablemente muchas solicitaciones y anuncios de la detección de vecino de otros host en la subred local.

> **Tip**: Para más información, refiera comprensión del documento de la comunidad del soporte de Cisco de la dirección de bit del IPv6 EUI-64.

### Los clientes utilizan los direccionamientos temporales del IPv6 por abandono

Por abandono, muchos sistemas operativos del cliente (OS), por ejemplo las versiones 7 y 8 de Microsoft Windows, Macintosh OS-X, y los sistemas Linux-basados, utilizan los direccionamientos *temporales* autoasignados del IPv6 para la aislamiento extendida vía la configuración automática de dirección apátrida del IPv6 (SLAAC).

El TAC de Cisco ha visto algunos casos donde éste causó los problemas inesperados en los entornos porque los host generan el tráfico del direccionamiento temporal y no del direccionamiento estático-asignado. Como consecuencia, los ACL y las rutas basadas en el host pudieron causar el tráfico a se caídos o se ruteados incorrectamente, que hace la comunicación del host fallar.

Hay dos métodos que se utilizan para dirigir esta situación. El comportamiento se puede inhabilitar individualmente en los sistemas del cliente, o usted puede inhabilitar este comportamiento en el ASA y el Routers del ® del Cisco IOS. En el ASA o el lado del router, usted debe modificar el indicador del mensaje del aviso del router (RA) que acciona este comportamiento.

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

#### *Microsoft Windows*

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

1. En Microsoft Windows, abra un comando prompt elevado (funcionamiento como administrador).

2. Ingrese este comando para inhabilitar la característica al azar de la generación del IP Address, y entonces el Presione ENTER:

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

3. Ingrese este comando para forzar 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 una terminal, ingrese este comando para inhabilitar el IPv6 SLAAC en el host hasta la reinicialización siguiente:

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

Para hacer la permanente de la configuración, ingrese este comando:

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

### *Linux*

En un shell terminal, ingrese este comando:

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

### *Inhabilite SLAAC global del ASA*

El segundo método que se utiliza para dirigir este comportamiento es modificar el mensaje RA que se envía del ASA a los clientes, que acciona el uso de SLAAC. Para modificar el mensaje RA, ingrese este comando del *modo de 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 es enviado por el ASA para no fijar el indicador del Un dígito binario, y los clientes no generan un direccionamiento temporal del IPv6.

> **Tip**: Refiera al RFC 4941 para la información adicional.

## IPv6 FAQ

Esta sección describe algunas preguntas frecuentes con respecto al uso del IPv6.

## ¿Puedo pasar el tráfico para ambo IPv4 y el IPv6 en lo mismo interfaz, al mismo tiempo?

Yes. Usted debe habilitar simplemente el IPv6 en la interfaz y asignar un IPv4 y un direccionamiento del IPv6 a la interfaz, y maneja ambos tipos de tráfico simultáneamente.

## ¿Puedo aplicar el IPv6 y el IPv4 ACL lo mismo interconecta?

Usted puede hacer esto en las Versiones de ASA anterior que la versión 9.0(1). A partir de la Versión de ASA 9.0(1), todos los ACL en el ASA *se unifican*, así que significa que un ACL soporta una mezcla de entradas del IPv4 y del IPv6 en el mismo ACL.

En las Versiones de ASA se combina junto 9.0(1) y posterior, los ACL simplemente y el ACL solo, unificado se aplica a la interfaz vía el **comando access-group**.

## ¿El ASA soporta QoS para el IPv6?

Yes. El ASA soporta el policing y la cola prioritaria para el IPv6 de la misma manera que hace con el IPv4.

A partir de la Versión de ASA 9.0(1), todos los ACL en el ASA *se unifican*, así que significa que un ACL soporta una mezcla de entradas del IPv4 y del IPv6 en el mismo ACL. Como consecuencia, cualquier comando qos que se decrete en un clase-mapa que haga juego un ACL toma medidas en el tráfico del IPv4 y del IPv6.

## ¿Debo utilizar el NAT con el IPv6?

Aunque el NAT se pueda configurar para el IPv6 en el ASA, el uso del NAT en el IPv6 es desalentado altamente e innecesario, dado la cantidad infinita cercana de disponible, los direccionamientos del IPv6 del global-routable.

Si el NAT se requiere en un escenario del IPv6, usted puede encontrar más información sobre cómo configurarla en la sección de las guías de consulta del IPv6 NAT del *libro 2 CLI: Guía de configuración CLI del Firewall de la serie de Cisco ASA, 9.4*.

> **Note**: Hay algunas guías de consulta y limitaciones que deben ser consideradas cuando usted implementa el NAT con el IPv6.

## ¿Por qué veo los direccionamientos del IPv6 del local de la conexión en la salida del *comando show failover*?

En el IPv6, el ND utiliza a las direcciones locales del link para realizar el address resolution L2. Por este motivo, los direccionamientos del IPv6 para las interfaces monitoreadas en la salida del **comando show failover** muestran la dirección local del link y no el direccionamiento global del IPv6 que se configura en la interfaz. Debe ocurrir lo siguiente.

## Advertencias conocidas/pedidos de mejora

Aquí están algunas advertencias conocidas con respecto al uso del IPv6:

- *La cláusula de la “coincidencia” de la captura del  ASA 8.x del*  Â del âÂ del Id. de bug Cisco CSCtn09836 *no coge el tráfico del IPv6*
- *ENH del*  Â del âÂ del Id. de bug Cisco CSCuq85949*: Soporte del IPv6 ASA para el WCCP*
- *La encaminamiento del IPv6 ECMP del  ASA del*  Â del âÂ del Id. de bug Cisco CSCut78380 *no carga el tráfico de la balanza*

## Información Relacionada

- Protocolo de Internet del  del  Â del âÂ del RFC 2460, especificación de la versión 6 (IPv6)
- Arquitectura de direccionamiento del IP versión 6 del  del  Â del âÂ del RFC 4291
- Detección de vecino del  del  Â del âÂ del RFC 4861 para el IP versión 6 (IPv6)
- Libro 1 CLI: Guía de configuración CLI de los funcionamientos generales de la serie de Cisco ASA, 9.4 IPv6s del  del  Â del âÂ
- AnyConnect SSL sobre IPv4+IPv6 a la configuración ASA
- Cisco Systems del  Â del âÂ del Soporte técnico y de la documentación