

Rastreador de paquetes: descubrimiento de vecinos IPv6

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección/prefijo IPv6	Gateway predeterminado
RTA	G0/0/0	2001:db8:acad:1::1/64	No corresponde
	G0/0/1	2001:db8:acad:1::1/64	No corresponde
PCA1	NIC	2001:db8:acad:1::A/64	fe80::1
PCA2	NIC	2001:db8:acad:1::B/64	fe80::1
PCB1	NIC	2001:db8:acad:2::A/64	fe80::1

Objetivos

Parte 1: Red local de detección de vecinos IPv6

Parte 2: Red remota de detección de vecinos IPv6

Aspectos básicos

Para que un dispositivo se comunice con otro dispositivo, se debe conocer la dirección MAC del destino. Con IPv6, un proceso denominado Neighbor Discovery que utiliza el protocolo NDP o ND es responsable de determinar la dirección MAC de destino. Recopilará información de PDU en modo de simulación para comprender mejor el proceso. No hay puntuación de Packet Tracer para esta actividad.

Instrucciones

Parte 1: Red local de descubrimiento de vecinos IPv6

En la Parte 1 de esta actividad, obtendrá la dirección MAC de un dispositivo de destino en la misma red.

Paso 1: Compruebe el router para ver si hay algún vecino que haya descubierto.

- Haga clic en el Router RTA. Seleccione la pestaña CLI y ejecute el comando **show ipv6 neighbors** desde el modo ejecutivo privilegiado. Si se muestran entradas, elimínelas con el comando **clear ipv6 neighbors**.
- Haga clic en **PCA1**, seleccione la pestaña Escritorio y haga clic en el icono **Símbolo del sistema**.

Paso 2: Cambie al modo de simulación para capturar eventos.

- Haga clic en el botón de **Simulación** en la esquina inferior derecha de la ventana Topología de Packet Tracer.
- Haga clic en el botón de **Mostrar todo/Ninguno** en la parte inferior izquierda del panel de Simulación. Hacer ciertos **Filtros de lista de eventos - Eventos visibles** muestran **Ningunos**.
- Desde el símbolo del sistema en **PCA1**, ejecute el comando **ping -n 1 2001:db8:acad:1::b**. Esto iniciará el proceso de hacer ping **PCA2**.

- f. Haga clic en el botón **Reproducir captura hacia delante**, que se muestra como una flecha que apunta a la derecha con una barra vertical dentro del cuadro Controles de reproducción. La barra de estado sobre los controles de reproducción debería leer Capturada a 150. (El número exacto puede variar).
- g. Haga clic en el botón **Editar filtros**. Seleccione la pestaña IPv6 en la parte superior y marque las casillas para **ICMPv6** y **NDP**. Haga clic en la X roja en la parte superior derecha de la ventana Editar filtros ACL. Los eventos capturados ahora deberían estar listados. Debe tener aproximadamente 12 entradas en la ventana.

¿Por qué están presentes PDU ND?

- h. Haga clic en el cuadrado de la columna Tipo para el primer evento, que debería ser **ICMPv6**.

Debido a que el mensaje comienza con este evento, solo hay una PDU de salida. Debajo de la pestaña Modelo OSI, ¿cuál es el tipo de mensaje listado para ICMPv6?

Observe que no hay direccionamiento de capa 2. Haga clic en el botón **Next Layer >>** para obtener una explicación sobre el proceso ND (Neighbor Discovery).

- i. Haga clic en el cuadrado situado junto al siguiente evento en el Panel de simulación. Debe estar en el dispositivo PCA1 y el tipo debe ser NDP.

¿Qué cambió en el direccionamiento de Capa 3?

¿Qué direcciones de capa 2 se muestran?

Cuando un host no conoce la dirección MAC del destino, la detección de vecinos IPv6 utiliza una dirección MAC de multidifusión especial como la dirección de destino de la capa 2.

- j. Seleccione el primer evento **NDP** en el SwitchA.

¿Hay alguna diferencia entre las capas de entrada y salida para la capa 2?

- k. Seleccione el primer evento **NDP** en **PCA2**. Haga clic en la ficha de Detalles de la PDU saliente.

¿Qué direcciones se muestran para lo siguiente?

Nota: Las direcciones en los campos pueden estar ajustadas, ajuste el tamaño de la ventana de la PDU para que la información de la dirección sea más fácil de leer.

Ethernet II DEST ADDR:

Ethernet II SRC ADDR:

IPv6 SRC IP:

IP de horario de verano de IPv6:

- l. Seleccione el primer evento **NDP** en **RTA**. ¿Por qué no hay capas de salida?

- m. Haga clic en el botón **Next Layer >>** (siguiente capa) hasta el final y lea los pasos del 4 hasta el 7 para obtener más información.
- n. Haga clic en el siguiente evento **ICMPv6** en **PCA1** .
¿PCA1 ahora tiene toda la información necesaria para comunicarse con PCA2?
- o. Haga clic en el último evento **ICMPv6** en **PCA1** . Observe que esta es la última comunicación listada.
¿Cuál es el tipo de mensaje de eco ICMPv6?
- p. Haga clic en **Reset Simulation** (Restablecer simulación) en el panel de simulación. Desde el símbolo del sistema de PCA1, repita el **ping** a PCA2. (Sugerencia: debería poder presionar la flecha hacia arriba para devolver el comando anterior.)
- q. Haga clic en el botón **Capture Forward** 5 veces para completar el proceso de ping.
¿Por qué no hubo ningún evento de NDP?

Parte 2: Red remota de Detección de Vecinos IPv6

En la Parte 2 de esta actividad, realizará pasos similares a los de la Parte 1, excepto en este caso, el host de destino está en otra LAN. Observe cómo el proceso de Detección de Vecinos difiere del proceso observado en la Parte 1. Preste mucha atención a algunos de los pasos de direccionamiento adicionales que tienen lugar cuando un dispositivo se comunica con un dispositivo que está en una red diferente.

Asegúrese de hacer clic en el botón **Reset Simulation** (Restablecer simulación) para borrar los eventos anteriores.

Paso 1: Capturar eventos para comunicación remota.

- a. Mostrar y borrar las entradas de la tabla de dispositivos vecinos IPv6 como se hizo en la parte I.
- b. Cambiar al modo de simulación. Haga clic en el botón de **Show All/None** (Mostrar todo/Ninguno) en la parte inferior izquierda del panel de Simulación. Asegúrese de que **Filtros de lista de eventos — Eventos visibles** muestra **Ninguno**.
- c. Desde el símbolo del sistema en PCA1, ejecute el comando **ping —n 1 2001:db8:acad:2::a** para hacer ping al host PCB1.
- d. Haga clic en el botón **Play Capture Forward**, que se muestra como una flecha que apunta a la derecha con una barra vertical dentro del cuadro Controles de reproducción. La barra de estado sobre los controles de reproducción debería leer Capturada a 150. (El número exacto puede variar).
- e. Haga clic en el botón **Edit Filters** (Editar filtros). Seleccione la pestaña IPv6 en la parte superior y marque las casillas para **ICMPv6** y **NDP** . Haga clic en la X roja en la parte superior derecha de la ventana Editar filtros ACL. Todos los eventos anteriores deben aparecer ahora en la lista. Debe notar que hay muchas más entradas listadas esta vez.
- f. Haga clic en el cuadrado de la columna "Tipo" para el primer evento, que debería ser **ICMPv6**. Dado que el mensaje comienza con este evento, sólo hay una PDU saliente. Observe que le falta la información de Capa 2 como en el escenario anterior.
- g. Haga clic en el primer evento **NDP** en el dispositivo **PCA1** .
¿Qué dirección se utiliza para la IP Src en la PDU entrante?

La detección de vecinos IPv6 determinará el próximo destino para reenviar el mensaje ICMPv6.

- h. Haga clic en el segundo evento ICMPv6 para **PCA1**. PCA1 ahora tiene suficiente información para crear una solicitud de eco ICMPv6.

¿Qué dirección MAC se utiliza para el MAC de destino?

- i. Haga clic en el siguiente evento ICMPv6 en el dispositivo **RTA**. Observe que la PDU saliente de RTA carece de la dirección de capa 2 de destino. Esto significa que RTA tiene que realizar de nuevo una detección de vecinos para la interfaz que tiene la red 2001:db8:acad:2:: porque no conoce las direcciones MAC de los dispositivos en la LAN G0/0/1.

- j. Vaya al primer evento ICMPv6 para el dispositivo **PCB1**.

¿Qué falta en la información saliente de Capa 2?

- k. Los siguientes eventos **NDP** están asociando las direcciones IPv6 restantes hacia las direcciones MAC. Los eventos NDP anteriores asociaron direcciones MAC con direcciones locales de enlace.

- l. Vaya al último conjunto de eventos ICMPv6 y observe que todas las direcciones han sido aprendidas. Ahora se conoce la información requerida, por lo que PCB1 puede enviar mensajes de respuesta de eco a PCA1.

- m. Haga clic en el botón Reset Simulation (Restablecer simulación) en el Panel de simulación. Desde el símbolo del sistema de PCA1, repita el comando para hacer ping a PCB1.

- n. Haga clic en el botón Capture Forward nueve veces para completar el proceso de ping.

¿Hubo algún evento de NDP?

- o. Haga clic en el único evento **PCB1** en la nueva lista.

¿A qué corresponde la dirección MAC de destino?

¿Por qué PCB1 utiliza la dirección MAC de la interfaz del router para crear sus PDU ICMP?

Paso 2: Examine las salidas del router.

- a. Vuelva al modo **Realtime**.
- b. Haga clic en **RTA** y seleccione la pestaña CLI. En la consola del router, ingrese el comando **show ipv6 neighbors**.

¿Cuántas direcciones aparecen en la lista?

¿Con qué dispositivos están asociadas estas direcciones?

¿Hay alguna entrada para PCA2 en la lista (por qué o por qué no)?

- c. Ping **PCA2** desde el router.

d. Emita el comando **show ipv6 neighbors**.

¿Hay entradas para PCA2?

Preguntas de reflexión

1. ¿Cuándo un dispositivo requiere el proceso de detección de vecinos IPv6?
2. ¿Cómo ayuda un router a minimizar la cantidad de tráfico de detección de vecinos IPv6 en una red?
3. ¿Cómo minimiza IPv6 el impacto del proceso ND en los hosts de red?
4. ¿En qué difiere el proceso de detección de vecinos cuando un host de destino está en la misma LAN y cuando está en una LAN remota?