Montano, George Jose

Packet Tracer - IPv6 Neighbor Discovery

Addressing Table

Device	Interface	IPv6 Address / Prefix	Default Gateway
RTA	G0/0/0	2001:db8:acad:1::1/64	N/A
RTA	G0/0/1	2001:db8:acad:1::1/64	N/A
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

Blank Line, No additional information

Objectives

Part 1: IPv6 Neighbor Discovery Local Network

Part 2: IPv6 Neighbor Discovery Remote Network

Background

For a device to communicate with another device, the MAC address of the destination must be known. With IPv6, a process called Neighbor Discovery using NDP or ND protocol is responsible for determining the destination MAC address. You will gather PDU information in simulation mode to better understand the process. There is no Packet Tracer scoring for this activity.

Instructions

Part 1: IPv6 Neighbor Discovery Local Network

In this part, you will obtain the MAC address of a destination device on the same network.

Step 1: Check the router for any neighbors that it discovered.

a. Click the RTA Router. Select the CLI tab and issue the command **show ipv6 neighbors** from the privileged EXEC mode. If there are any entries displayed, remove them using the command **clear ipv6 neighbors**.

b. Click **PCA1**, select the Desktop tab and click the **Command Prompt** icon.

Step 2: Switch to Simulation Mode to capture events.

a. Click the **Simulation** button in the lower right corner of the Packet Tracer Topology window.

b. Click the **Show All/None** button in the Simulation Panel until **Event List Filters – Visible Events** displays **None**.

c. Click **Edit Filters**. Select the IPv6 tab at the top and check the boxes for **ICMPv6** and **NDP**. Close the Edit ACL Filters window. Now the Event List Filters displays ICMPv6 and NDP.

d. From the command prompt on **PCA1**, issue the command **ping –n 1 2001:db8:acad:1::b**. This will start the process of pinging **PCA2**.

e. Click **Play (Hands Free)** in the PLAY CONTROLS outside the Simulation Panel. If prompted, click **View Previous Events** in the Buffer Full - Packet Tracer window. You should have approximately 12 entries in the window.

Question:
Why are ND PDUs present?

➔ ***If PCA 1 wants to send the ICMPv6 to PCA 2 then it will need the MAC address of that end device. The ND PDU will request for this information.***

f. Click the square in the Type column for the first event, which should be **ICMPv6**.

Question:
Because the message starts with this event there is only an Outbound PDU. Under the OSI Model tab, what is the Message Type listed for ICMPv6?

➔ ***ICMPv6 Echo Message Type: 128.***

Notice there is no Layer 2 addressing. Click the **Next Layer >>** button to get an explanation about the ND (Neighbor Discovery) process.

g. Click the square next to the next event in the Simulation Panel. It should be at device PCA1 and the type should be NDP.

Questions:
What changed in the Layer 3 addressing?

➔ ***The destination IP has changed into FF02::1:FF00:B***

What Layer 2 addresses are shown?

➔ ***Source address: PCA1 MAC – 0001.427E.E8ED***

➔ ***Destination MAC address: 3333.FF00.000B***

When a host does not know the MAC address of the destination, a special multicast MAC address is used by IPv6 Neighbor Discovery as the Layer 2 destination address.

h. Navigate back to the Event List. Select the first **NDP** event at SwitchA.

Question:
Is there any difference between the In Layers and Out Layers for Layer 2?

➔ ***There is no difference between the two.***

i. Select the first **NDP** event at **PCA2**. Click the Outbound PDU Details.

Question:
What addresses are displayed for the following?

Note: The addresses in the fields may be wrapped, adjust the size of the PDU window to make address information easier to read.

Ethernet II DEST ADDR:

➔ ***0001.427E.E8ED***

Ethernet II SRC ADDR:

➔ ***0040.0B02:.243E***

IPv6 SRC IP:

➔ ***2001:db8:acad:1::b***

IPv6 DST IP:

➔ ***2001:db8:acad:1::a***

Question:
j. Select the first **NDP** event at **RTA**. Why are there no Out Layers?

➔ ***The neighbor solicitation target IPv6 address does not match the router's port address and therefore drops the package.***

k. Click through the **Next Layer >>** button until the end and read steps 4 through 7 for further explanation.

l. Click the next **ICMPv6** event at **PCA1**.

Question:
Does PCA1 now have all the necessary information to communicate with PCA2?

➔ ***Yes PCA 1 now has all necessary information to communicate with PCA 2.***

m. Click the last **ICMPv6** event at **PCA1**. Notice this is the last communication listed.

Question:
What is the ICMPv6 Echo Message Type?

➔ ***ICMPv6 Echo Message Type: 129. Echo reply message.***

n. Click the **Reset Simulation** button in the Simulation Panel. From the command prompt of PCA1, repeat the **ping** to PCA2. (Hint: you should be able to press the up arrow to bring the previous command back.)

o. Click **Play (Hands Free)** to complete the ping process. Click **View Previous Events** if prompted.

Question:
Why were there no NDP events?

➔ ***Because PCA 1 already knows the MAC address of PCA 2.***

Part 2: IPv6 Neighbor Discovery Remote Network

In Part 2 of this activity, you will perform steps that are similar to those in the previous part, except in this case, the destination host is on another LAN. Observe how the Neighbor Discovery process differs from the process you observed in the previous part. Pay close attention to some of the additional addressing steps that take place when a device communicates with a device that is on a different network.

Step 1: Capture events for remote communication.

a. Click the **Reset Simulation** button to clear out the previous events. Display and clear any entries in the IPv6 neighbor device table as was done in the previous part.

b. Verify only **ICMPv6** and **NDP** are listed in the Event List Filters - Visible Events.

c. From the command prompt on PCA1, issue the command **ping –n 1 2001:db8:acad:2::a** to ping host PCB1.

d. Click **Play (Hands Free)** in the PLAY CONTROLS outside the Simulation Panel. If prompted, click **View Previous Events** in the Buffer Full -- Packet Tracer window.

e. When the pinging process is done, click the square in the Type Column for the first event, which should be **ICMPv6**. Because the message starts with this event, there is only an Outbound PDU. Notice that it is missing the Layer 2 information as it did in the previous scenario.

f. Click the first **NDP** event At Device **PCA1**.

Question:
What address is being used for the Src IP in the inbound PDU?

➔ ***fe80::201:42ff:fe7e:e8ed which is the link local address for PCA 1.***

IPv6 Neighbor Discovery will determine the next destination to forward the ICMPv6 message.

g. Click the second ICMPv6 event for **PCA1**. PCA1 now has enough information to create an ICMPv6 echo request.

Question:
What MAC address is being used for the destination MAC?

➔ ***0001.961d.6301 which is the MAC address of the router at the port of Gigabit 0/0/0.***

h. Click the next ICMPv6 event at device **RTA**. Notice that the outbound PDU from RTA lacks the destination Layer 2 address, This means that RTA once again has to perform a Neighbor Discovery for the interface that has the 2001:db8:acad:2:: network because it does not know the MAC addresses of the devices on the G0/0/1 LAN.

i. Skip down to the first ICMPv6 event for device **PCB1**.

Question:
What is missing in the outbound Layer 2 information?

➔ ***The destination MAC address which is required for the IPv6 destination address.***

j. The next few **NDP** events are associating the remaining IPv6 addresses to MAC addresses. The previous NDP events associated MAC addresses with Link Local addresses.

k. Skip to the last set of ICMPv6 events and notice that all the addresses have been learned. The required information is now known, so PCB1 can send echo reply to messages to PCA1.

l. Click the Reset Simulation button in the Simulation Panel. From the command prompt of PCA1 repeat the command to ping PCB1.

m. Click **Play (Hands Free)** to complete the ping process. Click **View Previous Events** if prompted in the Buffer Full window.

Question:
Were there any NDP events?

➔ ***There are no NDP events.***

n. Click the only **PCB1** event in the new list.

Questions:
What does the destination MAC address correspond to?

➔ ***The router at Gigabit 0/0/1 port interface.***

Why is PCB1 using the router interface MAC address to make its ICMP PDUs?

➔ ***The destination end device is located on another network. The PDU is addressed to the default gateway by PCB 1 and the router will determine how to send it to its destination.***

Step 2: Examine router outputs.

a. Return to **Realtime** mode.

b. Click **RTA** and select the CLI tab. At the router prompt enter the command **show ipv6 neighbors**.

Questions:
How many addresses are listed?

➔ ***There are 4 addresses listed. IPv6 and MAC address of PCA 1 and PCB 1.***

What devices are these addresses associated with?

➔ ***PCA 1 and PCB 1***

Are there any entries for PCA2 listed? Explain.

➔ ***None. PCA 2 has not communicated yet with the network.***

c. Ping **PCA2** from the router.

d. Issue the **show ipv6 neighbors** command.

Question:
Are there entries for PCA2?

➔ ***Yes. PCA 2's MAC address and IPv6 address.***

Reflection Questions

1. When does a device require the IPv6 Neighbor Discovery process?

➔ ***This is useful when the destination MAC address is unknown which is similar to IPv4's ARP.***

2. How does a router help to minimize the amount of IPv6 Neighbor Discovery traffic on a network?

➔ ***The router uses its neighbors tables which keeps track of MAC addresses of its neighbors so that it does not need to use Neighbor Discovery every time for a destination host.***

3. How does IPv6 minimize the impact of the ND process on network hosts?

   ➔ ***IPv6 uses multicast address to limit the addresses that would receive the Neighbor Discovery messages. IPv6 creates a multicast destination MAC address which include a portion of the node address.***

4. How does the Neighbor Discovery process differ when a destination host is on the same LAN and when it is on a remote LAN?

   ➔ ***The device that matches the IPv6 address on the same LAN will respond while the others will drop the packet. On a remote host, the router or another default gateway device will determine to which interface on the local interface the destination MAC address is given and then searches the remote network for the MAC address. The corresponding IPv6 and MAC address pair that respond are recorded in the Neighbor table by the router.***

End of document