 **BRANDON CLASPILL – PT 9.3.4 RESPONSE QUESTIONS**

**Packet Tracer – IPv6 Neighbor Discovery**

# Addressing Table

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

# Objectives

**Part 1: IPv6 Neighbor Discovery Local Network**

**Part 2: IPv6 Neighbor Discovery Remote Network**

# Background

In order 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 Part 1 of this activity, 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.**

1. 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**.
2. Click **PCA1**, select the Desktop tab and click the **Command Prompt** icon.

**Step 2: Switch to Simulation Mode to capture events.**

1. Click the **Simulation** button in the lower right corner of the Packet Tracer Topology window.
2. Click the **Show All/None** button in the lower left part of the Simulation Panel. Make certain **Event List Filters – Visible Events** displays **None**.
3. 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**.
4. Click the **Play Capture Forward** button, which is displayed as an arrow pointing to the right with a vertical bar within the Play Controls box. The status bar above the Play Controls should read Captured to 150.

(The exact number may vary.)

1. Click the **Edit Filters** button. Select the IPv6 tab at the top and check the boxes for **ICMPv6** and **NDP**. Click the red X in the upper right of the Edit ACL Filters window. The captured events should now be listed. You should have approximately 12 entries in the window.

Question:

Why are ND PDUs present?

**There are ND PDU’s present, because as stated above a MAC Address destination must be known for devices to communicate. So, this is showing how the IPv6 ND appears, in order to get the MAC Address information of its destination. In this scenario, the ND would be starting the process of accessing PCA2’s MAC Address in order to start the communication of the ping I requested.**

***Type your answers here.***

1. 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?

**Message Type - 128**

***Type your answers here.***

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

1. 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 Dest. IP changed to FF02::1:FF00:B and also the ICMPv6 Neighbor Message Type change from 128 to a Neighbor Message Type of 135.**

***Type your answers here.***

What Layer 2 addresses are shown?

**Addresses showing in Layer 2 are the Source Address 0001.427E.E8ED and Destination Address 3333.FF00.000B.**

***Type your answers here.***

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.

1. Select the first **NDP** event at SwitchA.

Question:

Is there any difference between the In Layers and Out Layers for Layer 2? **NO**

***Type your answers here.***

1. 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*e your answers here.***

Question:

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

* **The Neighbor Solicitation's target IPv6 address does not match the receiving port's IPv6 address.**
* **The NDP process drops the packet.**

***Type your answers here.***

1. Click through the **Next Layer >>** button until the end and read steps 4 through 7 for further explanation. n. Click the next **ICMPv6** event at **PCA1**.

Question:

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

**Yes there Is now the Destination IPv6 Address and the Destination MAC Address of PCA2 listed in Layer 2. So, there is enough information for PCA1 to communicate with PCA2 at this point.**

***Type your answers here.***

1. 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 is 129, an echo reply message.**

***Type your answers here.***

1. 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.)
2. Click the **Capture Forward** button 5 times to complete the ping process.

Question:

Why weren’t there any NDP events?

**This is now the second ping communicated to the same device, PCA1 to PCA2 so PCA1 now already knows the MAC Address for PCA2. Which means there is no need for Neighbor Discovery to be utilized in this scenario.**

***Type your answers here.***

# Part 2: IPv6 Neighbor Discovery Remote Network

In Part 2 of this activity, you will perform steps that are similar to those in Part 1, except in this case, the destination host is on another LAN. Observe how the Neighbor Discovery process differs from the process you observed in Part 1. 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.

Make sure to click the **Reset Simulation** button to clear out the previous events.

**Step 1: Capture events for remote communication.**

1. Display and clear any entries in the IPv6 neighbor device table as was done in Part I.
2. Switch to simulation mode. Click the **Show All/None** button in the lower left part of the Simulation Panel. Make certain the **Event List Filters – Visible Events** displays **None.**
3. From the command prompt on PCA1 issue the command **ping –n 1 2001:db8:acad:2::a** to ping host PCB1.
4. Click the **Play Capture Forward** button which is displayed as an arrow pointing to the right with a vertical bar within the Play Controls box. The status bar above the Play Controls should read Captured to 150. (The exact number may vary.)
5. Click the **Edit Filters** button. Select the IPv6 tab at the top and check the boxes for **ICMPv6** and **NDP**. Click the red X in the upper right of the Edit ACL Filters window. All of the previous events should now be listed. You should notice there are considerably more entries listed this time.
6. 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.
7. Click the first **NDP** event At Device **PCA1**.

Question:

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

**The Link Layer address for PCA1 – FE80::201:42FF:FE7E:E8ED**

***Type your answers here.***

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

1. 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?

**The MAC Address being used is the Routers (RTA) and is - 0001.961d.6301**

***Type your answers here.***

1. 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 doesn’t know the MAC addresses of the devices on the G0/0/1 LAN.
2. Skip down to the first ICMPv6 event for device **PCB1**.

Question:

What is missing in the outbound Layer 2 information?

**Once again the Layer 2 Destination MAC Address is unknown, so there is no information in this layer at this point. The IPv6 Destination Address needs to be associated with the Destination MAC Address.**

***Type your answers here.***

1. 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.
2. Skip to the last set of ICMPv6 events and notice that all of the addresses have been learned. The required information is now known, so PCB1 can send echo reply messages to PCA1.
3. Click the Reset Simulation button in the Simulation Panel. From the command prompt of PCA1 repeat the command to ping PCB1.
4. Click the Capture Forward button nine times to complete the ping process.

Question:

Were there any NDP events?

**No, because they have communicated before, so the Destination MAC Address is known.**

***Type your answers here.***

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

Questions:

What does the destination MAC address correspond to?

**The Destination MAC Address corresponds to (RTA) which is the Routers G0/0/1 Interface.**

***Type your answers here.***

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

**PCB1 is using the RTA MAC Address because the Destination is not inside its local network. Which means it is outside the network and the Router needs to come into the equation. The PCB1 address the Router, and then the Router determines the next path to take outside the network. *your answers here.***

**Step 2: Examine router outputs.**

1. Return to **Realtime** mode.
2. 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 now 4 addresses listed in the RTA table.**

***Type your answers here.***

What devices are these addresses associated with?

**These addresses are associated with the most recent device communication and correspond to PCA1 and PCB1 devices.**

***Type your answers here.***

Are there any entries for PCA2 listed (why or why not)?

**No there is not a current entry listed for device PCA2 yet because there hasn’t been any communication with the device.**

***Type your answers here.***

Ping **PCA2** from the router.

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

Question:

Are there entries for PCA2? **Yes, the MAC and IPv6 Address of PCA2 are now in the RTA table.**

***Type your answers here.***

## Reflection Questions

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

**When the DESTINATION MAC Address is not recognized.**

***Type your answers here.***

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

**By keeping a log of entries, the router minimizes the need for ND and increase traffic on a network. The known addresses are stored in the routers table so it can quickly reference it when known devices are trying to communicate. Which reduces the need for ND to be utilized therefor decreasing traffic over the network.**

***Type your answers here.***

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

**By using a multicast address it significantly reduces the impact of ND because a lot fewer addresses are actively listening to the Neighbor Discovery messages. Also, hosts do not have to go through as many protocols and can easily determine if they are the intended target. So, it makes the hosts not have to work as hard to analyze and verify if they are the target.**

***Type your answers here.***

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

**When the device is local, the host responds and there then can be direct communication. In remote networks there is additional steps of the source host sending the packet to the router, then the router locates the destination hosts router, and they communicate. Then finally the destination host can be located by the router in that network and then relay its MAC Address back. So basically the main difference is that when a frame is sent to another device on the same local network, the device sending the frame will use the MAC address of the destination device. When sending a frame to another device on a remote network, the device sending the frame will use the MAC address of the local router interface, which is the default gateway.**