Rymbayeva Anelya, FIT, 2nd course, Lab5 – IT Infrastructure and Computer Networks

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
	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.

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.

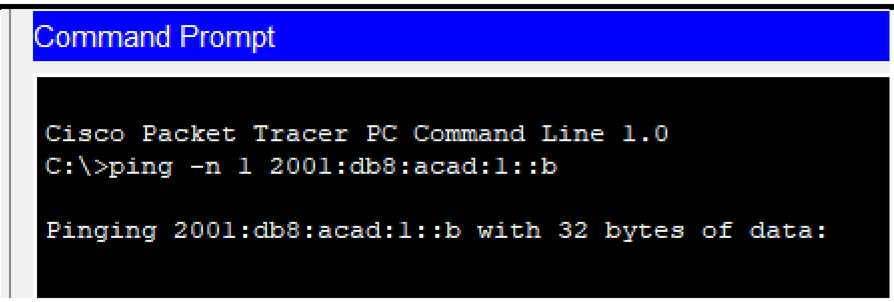
Step 2: Switch to Simulation Mode to capture events.

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

d. Click the **Show All/None** button in the lower left part of the Simulation Panel. Make certain **Event List Filters – Visible Events** displays **None**.

e. 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**.

© 2019 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -n 1 2001:db8:acad:1::b

Pinging 2001:db8:acad:1::b with 32 bytes of data:
```

f. 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.)

g. 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.

Why are ND PDUs present?

In order to send ICMPv6 ping packets to PCA2, PCA1 needs to know the MAC address of the destination. IPv6 ND requests this information on the network.

h. 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. Under the OSI Model tab, what is the Message Type listed for ICMPv6?

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

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

What changed in the Layer 3 addressing? The destination address is now an IPv6

What Layer 2 addresses are shown? The source address is PCA1 MAC – 001.427E.E8ED and the destination MAC address is 333.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.

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

Is there any difference between the In Layers and Out Layers for Layer 2? No, the switch does not change Layer 2, it only forwards the frame.

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

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

l. Select the first **NDP** event at **RTA**. Why are there no Out Layers?
The IPv6 address does not match the router's address so it drops the packet.

m. 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**.

Does PCA1 now have all of the necessary information to communicate with PCA2?
Yes, it now knows both the destination IPv6 address as well as the destination MAC address of PCA2.

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

What is the ICMPv6 Echo Message Type?

The ICMPv6 Echo Message Type is 129, an echo reply.

p. 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.)

q. Click the **Capture Forward** button 5 times to complete the ping process.

Why weren't there any NDP events?

PCA1 already knows the MAC address of PCA2 so it doesn't need to use Neighbor Discovery.

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.

a. Display and clear any entries in the IPv6 neighbor device table as was done in Part I.

b. 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.**

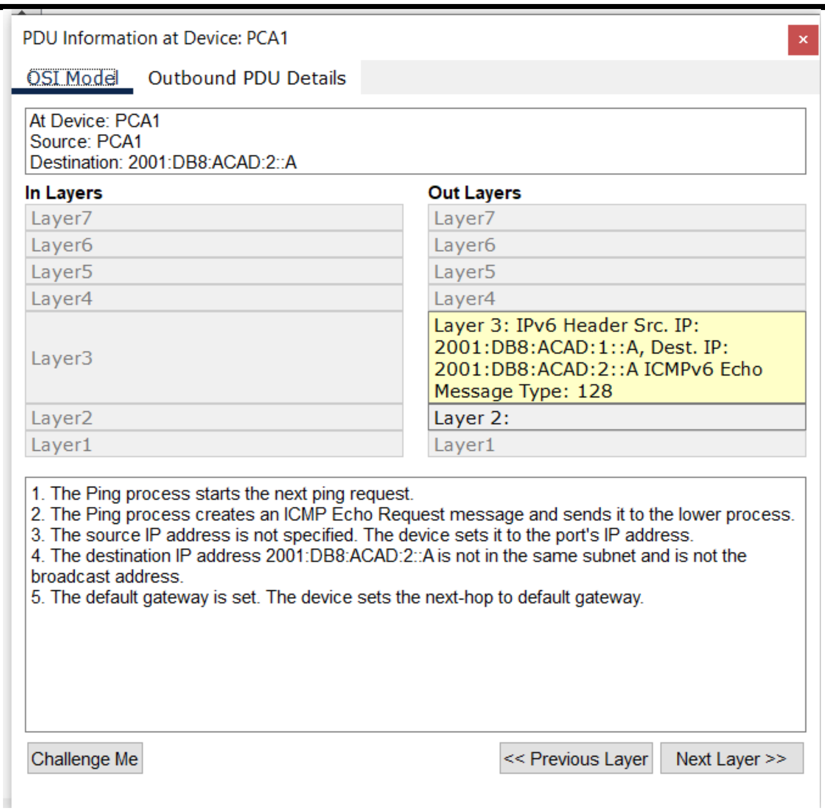
c. From the command prompt on PCA1 issue the command **ping –n 1 2001:db8:acad:2::a** to ping host PCB1.

d. 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.)

e. 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.

f. 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.

© 2019 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public



At Device: PCA1
Source: PCA1
Destination: 2001:DB8:ACAD:2::A

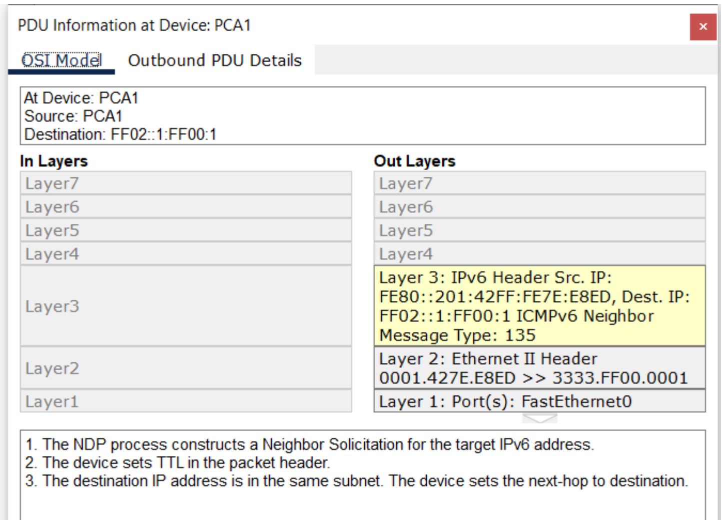
Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:2::A ICMPv6 Echo Message Type: 128

Layer 2:

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address 2001:DB8:ACAD:2::A is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

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

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



At Device: PCA1
Source: PCA1
Destination: FF02::1:FF00:1

Layer 3: IPv6 Header Src. IP: FE80::201:42FF:FE7E:E8ED, Dest. IP: FF02::1:FF00:1 ICMPv6 Neighbor Message Type: 135

Layer 2: Ethernet II Header 0001.427E.E8ED >> 3333.FF00.0001

Layer 1: Port(s): FastEthernet0

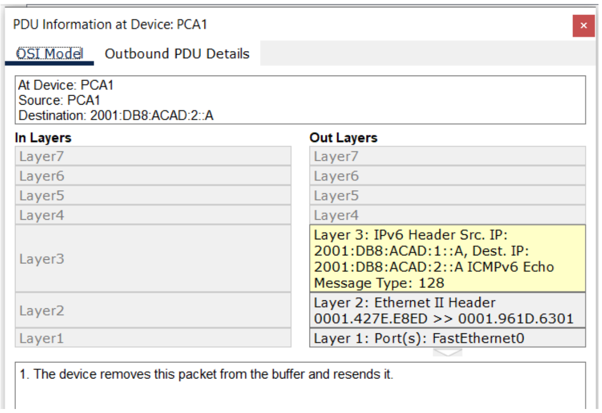
1. The NDP process constructs a Neighbor Solicitation for the target IPv6 address.
2. The device sets TTL in the packet header.
3. The destination IP address is in the same subnet. The device sets the next-hop to destination.

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

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

© 2019 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

What MAC address is being used for the destination MAC?



At Device: PCA1
Source: PCA1
Destination: 2001:DB8:ACAD:2::A

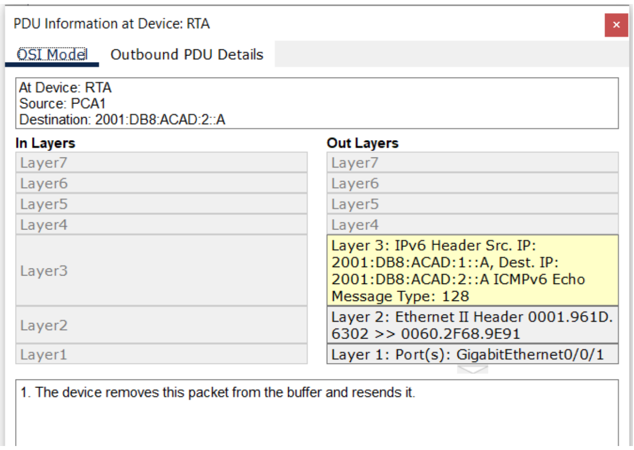
Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:2::A ICMPv6 Echo Message Type: 128

Layer 2: Ethernet II Header 0001.427E.E8ED >> 0001.961D.6301

Layer 1: Port(s): FastEthernet0

1. The device removes this packet from the buffer and resends it.

i. 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.



At Device: RTA
Source: PCA1
Destination: 2001:DB8:ACAD:2::A

Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:2::A ICMPv6 Echo Message Type: 128

Layer 2: Ethernet II Header 0001.961D.6302 >> 0060.2F68.9E91

Layer 1: Port(s): GigabitEthernet0/0/1

1. The device removes this packet from the buffer and resends it.

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

What is missing in the outbound Layer 2 information?

The destination MAC address must be determined

for the IPv6 destination address.

k. 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.

l. 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.

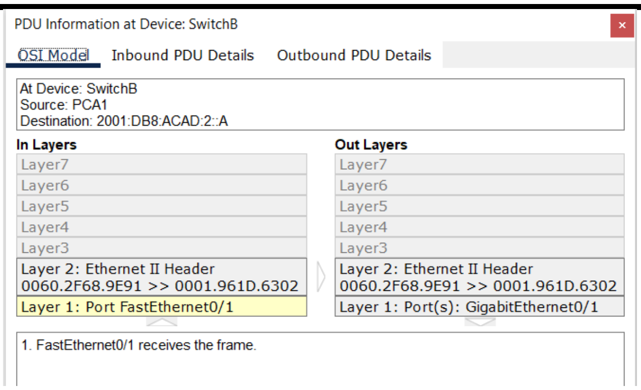
m. Click the Reset Simulation button in the Simulation Panel. From the command prompt of PCA1 repeat the command to ping PCB1.

n. Click the Capture Forward button nine times to complete the ping process.

Were there any NDP events? No

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

What does the destination MAC address correspond to?



At Device: SwitchB
Source: PCA1
Destination: 2001:DB8:ACAD:2::A

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0060.2F68.9E91 >> 0001.961D.6302	Layer 2: Ethernet II Header 0060.2F68.9E91 >> 0001.961D.6302
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): GigabitEthernet0/1

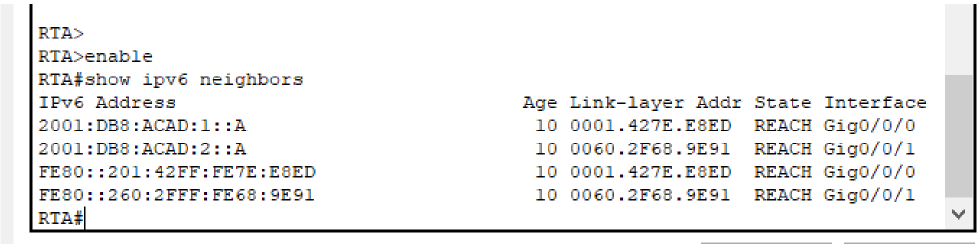
1. FastEthernet0/1 receives the frame.

Why is PCB1 using the router interface MAC address to make its ICMP PDUs?
Because the destination device is on another network, PCB1 addresses the PDU to the default gateway interface MAC. RTA will determine how to address the PDU at Layer 2 to send it towards 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**.



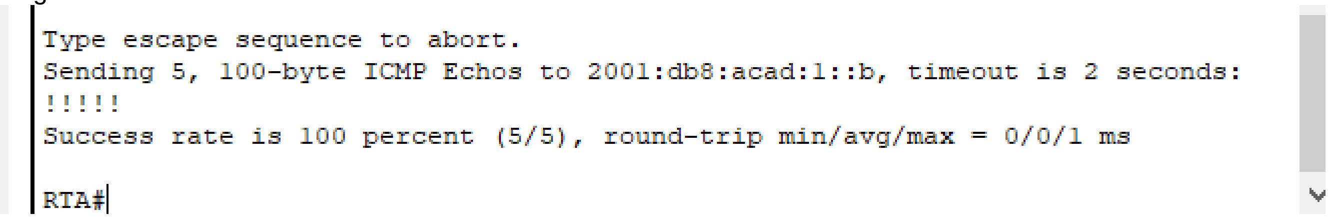
```
RTA>
RTA>enable
RTA#show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
2001:DB8:ACAD:1::A                         10 0001.427E.E8ED  REACH Gig0/0/0
2001:DB8:ACAD:2::A                         10 0060.2F68.9E91  REACH Gig0/0/1
FE80::201:42FF:FE7E:E8ED                   10 0001.427E.E8ED  REACH Gig0/0/0
FE80::260:2FFF:FE68:9E91                   10 0060.2F68.9E91  REACH Gig0/0/1
RTA#
```

How many addresses are listed? 4

What devices are these addresses associated with? PCA1, PCB1

Are there any entries for PCA2 listed (why or why not)? PCA2 has not the connection across the network yet.

Ping **PCA2** from the router.



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::b, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

RTA#
```

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

Are there entries for PCA2? Yes, the IPv6

address and MAC address for PCA2.

Reflection Questions

1. When does a device require the IPv6 Neighbor Discovery process?
   When the destination MAC address is not known. This process is similar to ARP with IPv6.

2. How does a router help to minimize the amount of IPv6 Neighbor Discovery traffic on a network?
   The router keeps neighbor tables so that it doesn't need to initiate ND for every destination host.

   How does IPv6 minimize the impact of the ND process on network hosts?
   It uses a multicast address so that only a handful of addresses would be listening to be Neighbor Discovery messages. IPv6 creates a specially crafted multicast destination MAC address which includes a portion of the node address.

3. 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 a destination host is on the same LAN segment only the device that matches the IPv6 address responds and other devices drop the packet. When the device is remote the gateway device (usually a router) provides the MAC address of the interface on the local interface for the destination MAC and then searches for the MAC address on the remote network. The router will then place the responding IPv6/MAC address pair in the IPv6 Neighbor table. (similar to an ARP table in IPv4)

© 2019 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public