

## Addressing Table

Device	Interface	AIIPv6 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.

## 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.

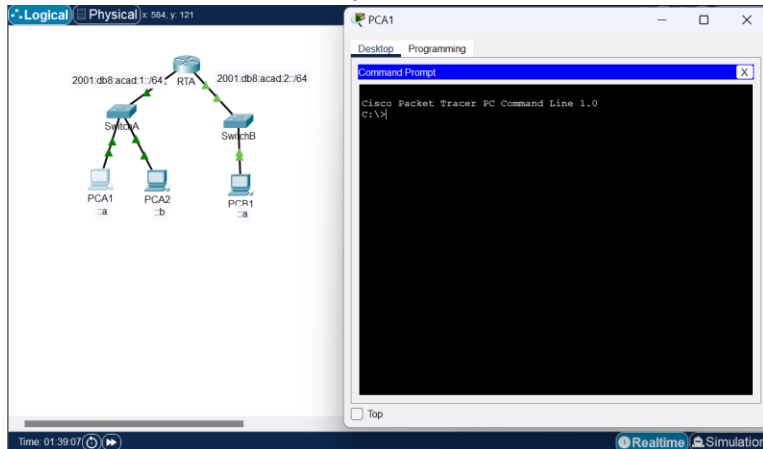
- Click the RTA Router. Select the CLI tab and issue the command **show ipv6 neighbors** from the privileged exec mode. If there are any entries displayed, remove them using the command **clear ipv6 neighbors**.

The screenshot displays the Packet Tracer interface. On the left, a network diagram shows a central router (RTA) connected to two switches, SwitchA and SwitchB. SwitchA is connected to two PCs, PCA1 and PCA2. SwitchB is connected to a PC, PCB1. The router RTA has two interfaces, G0/0/0 and G0/0/1, both with IPv6 addresses 2001:db8:acad:1::1/64. SwitchA has an IPv6 address 2001:db8:acad:1::1/64. SwitchB has an IPv6 address 2001:db8:acad:2::1/64. On the right, the RTA router's CLI is open, showing the following output:

```
RTA>enable
RTA#show ipv6 neighbors
RTA#
```

The CLI output shows the router's configuration details, including the processor, memory, and interfaces. The command **show ipv6 neighbors** has been entered, and the output is displayed in a red box.

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

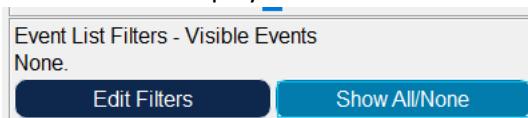


## Step 2: Switch to Simulation Mode to capture events.

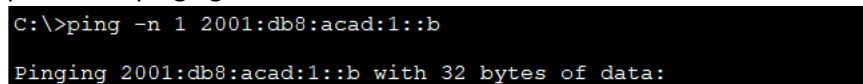
- c. Click the **Simulation** button in the lower right corner of the Packet Tracer Topology window.



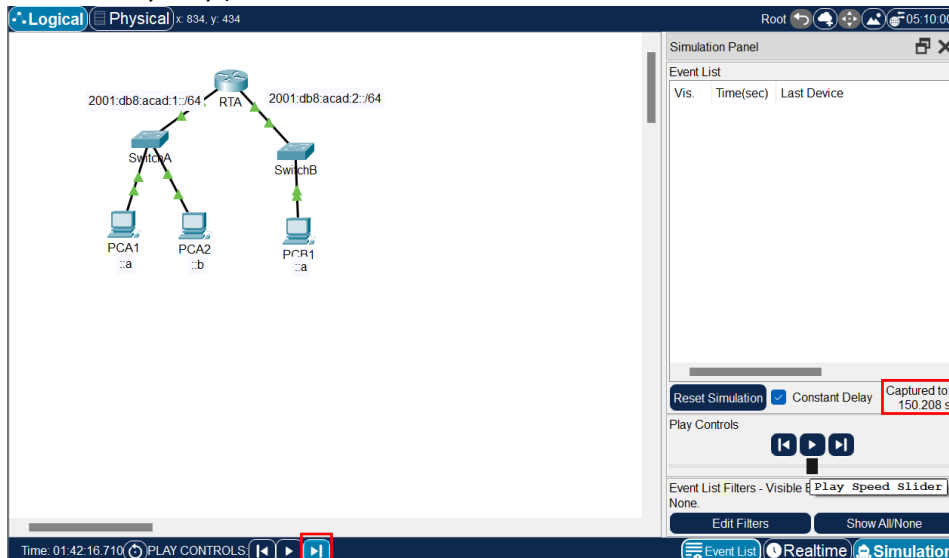
- d. Click the **Show All/None** button in the lower left part of the Simulation Panel. Make certain **Event List Filters – Visible Events** displays **None**.



- 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**.



- 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.

The screenshot shows the Cisco Packet Tracer interface. On the left, the 'Event List Filters - Visible Events' window is open, showing 'None' under 'Visible Events' and buttons for 'Edit Filters' and 'Show All/None'. On the right, the 'Cisco Packet Tracer' window has the 'IPv6' tab selected, with checkboxes for 'ICMPv6' and 'NDP' checked. The main simulation area shows a network topology with a central router (RTA) connected to two switches (SwitchA and SwitchB), which are connected to three PCs (PCA1, PCA2, PCA3). The 'Simulation Panel' on the right shows an 'Event List' with 12 entries, including ICMPv6 and NDP events. The 'Event List Filters - Visible Events' window is also open in the bottom right, showing 'ICMPv6, NDP' under 'Visible Events'.

### Why are ND PDUs present?

If PCA1 wants to send ICMPv6 ping packets to PCA2, then it needs to know the MAC address of PCA2. (IPv6 ND requests this information on the network.)

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

The screenshot shows the 'Simulation Panel' with the 'Event List' table. The first event is at time 0.000, from PCA1, and its type is 'ICMPv6'. Below the table, the 'PDU Information at Device: PCA1' window is open, showing the 'OSI Model' and 'Outbound PDU Details' tabs. The 'Out Layers' section shows the details of the ICMPv6 Echo message, including the source and destination IP addresses and the message type (128).

Time(sec)	Last Device	At Device	Type
0.000	--	PCA1	ICMPv6

**PDU Information at Device: PCA1**

**OSI Model** | **Outbound PDU Details**

At Device: PCA1  
Source: PCA1  
Destination: 2001:DB8:ACAD:1::B

**In Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

**Out Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:1::B ICMPv6 Echo
- Layer2:
- Layer1

**Message Type: 128**

- The Ping process starts the next ping request.
- The Ping process creates an ICMP Echo Request message and sends it to the lower process.
- The source IP address is not specified. The device sets it to the port's IP address.
- The destination IP address is in the same subnet. The device sets the next-hop to destination.

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.

PDU Information at Device: PCA1

At Device: PCA1  
Source: PCA1  
Destination: 2001:DB8:ACAD:1::B

**In Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

**Out Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:1::B ICMPv6 Echo Message Type: 128
- Layer 2:
- Layer1

1. The next-hop IP address is unicast address. The ND Process looks it up in the neighbor table.  
2. The next-hop IP address is not in the neighbor table. The NDP process sends a neighbor solicitation for that IP address and buffers this packet.

Challenge Me << Previous Layer Next Layer >>

- 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.

Simulation Panel

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
	0.002	SwitchA	RTA	NDP
	0.003	PCA2	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	PCA2	ICMPv6
	0.007	PCA2	SwitchA	ICMPv6
	0.008	SwitchA	PCA1	ICMPv6
	6.959	--	RTA	NDP
	6.960	RTA	SwitchB	NDP
	6.961	SwitchB	PCB1	NDP

Reset Simulation Constant Delay Captured to: 150.208 s

Play Controls

Event List Filters - Visible Events  
ICMPv6, NDP

Edit Filters Show All/None

PDU Information at Device: PCA1

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

**In Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

**Out Layers**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: FF02::1:FF00:B ICMPv6 Neighbor Message Type: 135
- Layer 2: Ethernet II Header 0001.427E.E8ED >> 3333.FF00.000B
- 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.

Challenge Me << Previous Layer Next Layer >>

What changed in the Layer 3 addressing?

The destination IP address is changed. It is now FF02::1:FF00:B, an IPv6 multicast address. (In the previous event, it was 2001:DB8:ACAD::B.)

What Layer 2 addresses are shown?

Source MAC address: 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.

**NOTE:** The special multicast MAC address used by IPv6 Neighbor Discovery as the Layer 2 destination address is 3333.FF00.000B.

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

The screenshot shows the Packet Tracer simulation interface. On the left, the 'Event List' panel displays a list of events. The first NDP event at SwitchA is selected, showing a time of 0.001 seconds. The event details show the source as PCA1 and the destination as FF02::1:FF00:B. On the right, the 'PDU Information at Device: SwitchA' panel shows the OSI Model, Inbound PDU Details, and Outbound PDU Details. The In Layers section shows Layer 2: Ethernet II Header with source and destination MAC addresses. The Out Layers section shows Layer 2: Ethernet II Header with the same source and destination MAC addresses. The Layer 1 section shows Port FastEthernet0/1.

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

No. (The switch does not alter Layer 2 information, it only forwards the frame.)

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

The screenshot shows the Packet Tracer simulation interface. On the left, the 'Event List' panel displays a list of events. The first NDP event at PCA2 is selected, showing a time of 0.002 seconds. On the right, the 'PDU Information at Device: PCA2' panel shows the Outbound PDU Details. The PDU Formats section shows the Ethernet II header with the following fields: PREAMBLE: 101010\_10, SFD, DEST ADDR: 0001.427E.E8ED, SRC ADDR: 0040.0BD2.243E, TYPE: 0x86dd, DATA (VARIABLE LENGTH), and FCS: 0x00000000. The IPv6 header shows the following fields: VER: 6, TRFC, FLOW LABEL, PL: 28, NEXT: 0x3a, HOP LIMIT: 255, SRC IP: 2001:DB8:ACAD:1::B, and DST IP: 2001:DB8:ACAD:1::A.

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: 0040.0BD2.243E

IPv6 SRC IP: 2001:DB8:ACAD:1::B

IPv6 DST IP: 2001:DB8:ACAD:1::A

I. Select the first **NDP** event at **RTA**.

The screenshot shows the Packet Tracer interface. On the left, the 'Simulation Panel' displays an 'Event List' with the following data:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
👁	0.002	SwitchA	RTA	NDP
	0.003	PCA2	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	PCA2	ICMPv6
	0.007	PCA2	SwitchA	ICMPv6
	0.008	SwitchA	PCA1	ICMPv6
	6.959	--	RTA	NDP
	6.960	RTA	SwitchB	NDP
	6.961	SwitchB	PCB1	NDP

The event at 0.002 seconds, where SwitchA sends an NDP to RTA, is selected. The 'PDU Information at Device: RTA' window on the right shows the following details:

- At Device:** RTA
- Source:** PCA1
- Destination:** FF02::1:FF00:B
- In Layers:** Layer7, Layer6, Layer5, Layer4, Layer3 (IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: FF02::1:FF00:B ICMPv6 Neighbor Message Type: 135), Layer2 (Ethernet II Header 0001.427E.E8ED >> 3333.FF00.000B), Layer1 (Port GigabitEthernet0/0/0)
- Out Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
- Description:** 1. GigabitEthernet0/0/0 receives the frame.

At the bottom, the 'Event List Filters' are set to 'Visible Events: ICMPv6, NDP'.

**Why are there no Out Layers?**

There are no out layers because the IPv6 address does not match the router's address. The packet ends up being dropped.

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

The screenshot shows the 'PDU Information at Device: RTA' window with the 'OSI Model' tab selected. The 'In Layers' and 'Out Layers' sections are visible. The 'In Layers' section shows the following details:

- Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: FF02::1:FF00:B ICMPv6 Neighbor Message Type: 135
- Layer 2: Ethernet II Header 0001.427E.E8ED >> 3333.FF00.000B
- Layer 1: Port GigabitEthernet0/0/0

The 'Out Layers' section is empty. Below the layers, a list of steps is provided:

1. The packet is coming from an outside network. The device looks up its NAT table for necessary translations.
2. The destination IP address is a broadcast or multicast address. The device dispatches the packet to the upper layer.
3. The packet is an ICMP packet. The ICMP process processes it.
4. The packet is an NDP packet. The device processes the packet.
5. The ND packet is a Neighbor Solicitation.
6. The Neighbor Solicitation's target IPv6 address does not match the receiving port's IPv6 address.
7. The NDP process drops the packet.

At the bottom, the 'Challenge Me' button is visible, along with '<< Previous Layer' and 'Next Layer >>' buttons.

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

The screenshot shows the Packet Tracer interface. On the left, the 'Simulation Panel' displays an 'Event List' with the following data:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
👁	0.002	SwitchA	RTA	NDP
	0.003	PCA2	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	PCA2	ICMPv6
	0.007	PCA2	SwitchA	ICMPv6
	0.008	SwitchA	PCA1	ICMPv6
	6.959	--	RTA	NDP
	6.960	RTA	SwitchB	NDP
	6.961	SwitchB	PCB1	NDP

The event at 0.004 seconds, where PCA1 sends an ICMPv6 event, is selected. The 'PDU Information at Device: PCA1' window on the right shows the following details:

- At Device:** PCA1
- Source:** PCA1
- Destination:** 2001:DB8:ACAD:1::B
- In Layers:** Layer7, Layer6, Layer5, Layer4, Layer3, Layer2, Layer1
- Out Layers:** Layer7, Layer6, Layer5, Layer4, Layer3 (IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:1::B ICMPv6 Echo Message Type: 128), Layer2 (Ethernet II Header 0001.427E.E8ED >> 0040.0BD2.243E), Layer1 (Port(s): FastEthernet0)
- Description:** 1. The device removes this packet from the buffer and resends it.

At the bottom, the 'Event List Filters' are set to 'Visible Events: ICMPv6, NDP'.

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

Yes, since it has information on both the source and destination IPv6 addresses, as well as the destination MAC addresses of PCA2.

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

The screenshot shows the Packet Tracer Simulation Panel and the PDU Information window for device PCA1.

**Simulation Panel:**

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
	0.002	SwitchA	RTA	NDP
	0.003	PCA2	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	PCA2	ICMPv6
	0.007	PCA2	SwitchA	ICMPv6
	0.008	SwitchA	PCA1	ICMPv6
	6.959	--	RTA	NDP
	6.960	RTA	SwitchB	NDP
	6.961	SwitchB	PCB1	NDP

Reset Simulation ☒ Constant Delay Captured to: 150.208 s

Play Controls: [Previous] [Play] [Next]

Event List Filters - Visible Events: ICMPv6, NDP

Edit Filters Show All/None

**PDU Information at Device: PCA1**

OSI Model Inbound PDU Details

At Device: PCA1  
Source: PCA1  
Destination: 2001:DB8:ACAD:1::B

**In Layers**

- Layer 7
- Layer 6
- Layer 5
- Layer 4
- Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::B, Dest. IP: 2001:DB8:ACAD:1::A ICMPv6 Echo Message Type: 129
- Layer 2: Ethernet II Header 0040.0BD2.243E >> 0001.427E.E8ED
- Layer 1: Port FastEthernet0

**Out Layers**

- Layer 7
- Layer 6
- Layer 5
- Layer 4
- Layer 3
- Layer 2
- Layer 1

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.  
2. The packet is an ICMP packet. The ICMP process processes it.  
3. The ICMP process received an Echo Reply message.  
4. The Ping process received an Echo Reply message.

Challenge Me << Previous Layer Next Layer >>

What is the ICMPv6 Echo Message Type?

ICMPv6 Echo Message Type: 129

- p. Click the **Reset Simulation** button in the Simulation Panel.

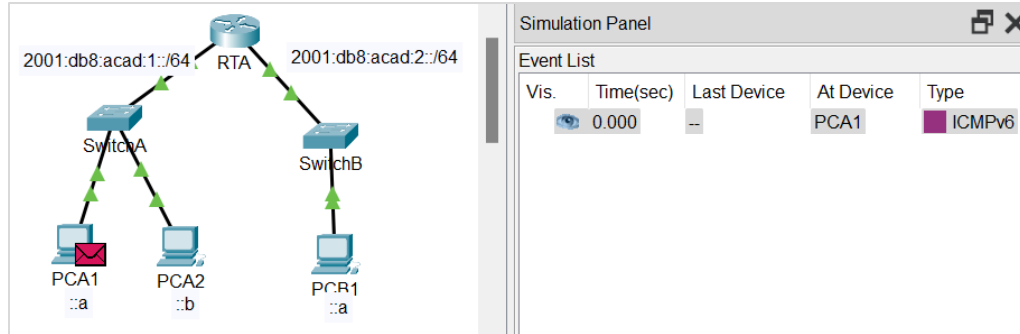
The screenshot shows the Packet Tracer Simulation Panel. The **Reset Simulation** button is highlighted with a red box. The **Constant Delay** checkbox is checked. The **Captured to:** field shows "(no captures)". The **Play Controls** section includes buttons for [Previous], [Play], and [Next]. The **Event List Filters - Visible Events** section shows "ICMPv6, NDP". The **Edit Filters** and **Show All/None** buttons are visible at the bottom.

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.)

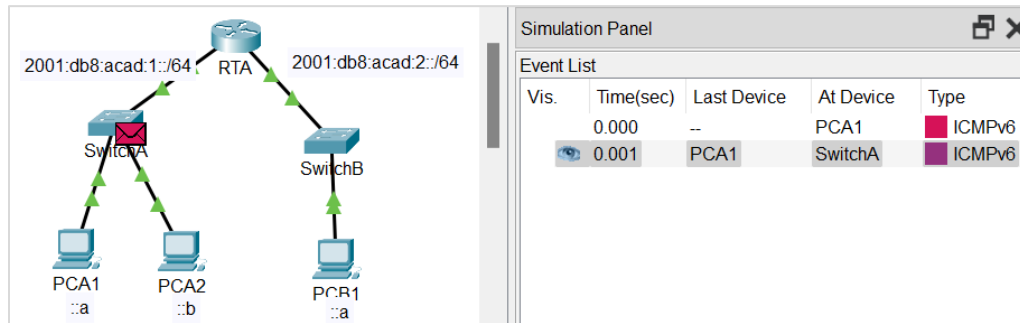
```
Pinging 2001:db8:acad:1::b with 32 bytes of data:
```

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

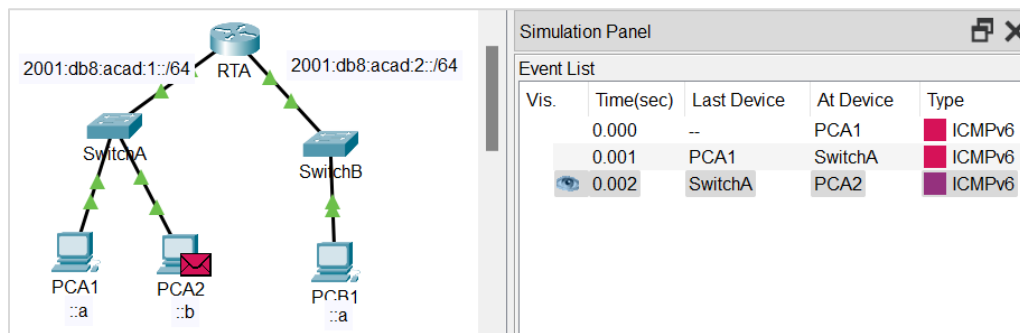
**1 (Current):**



**2:**



**3:**

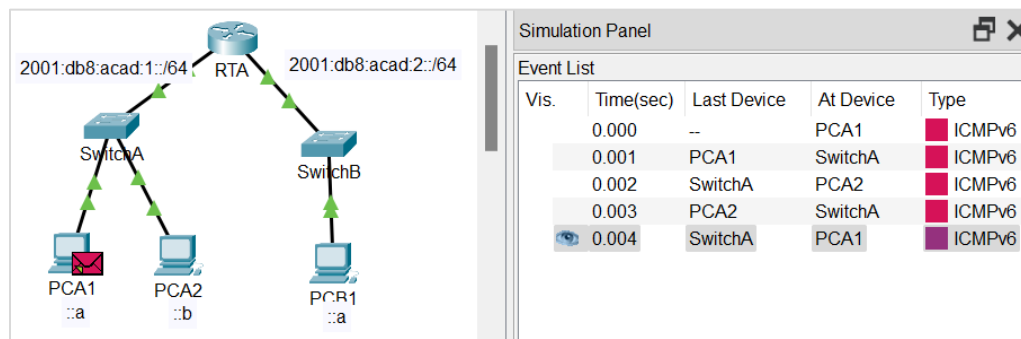


**4:**





5:



Why weren't there any NDP events?

Because PCA1 already knows the MAC address of PCA2, it does not need to use Neighbor Discovery.

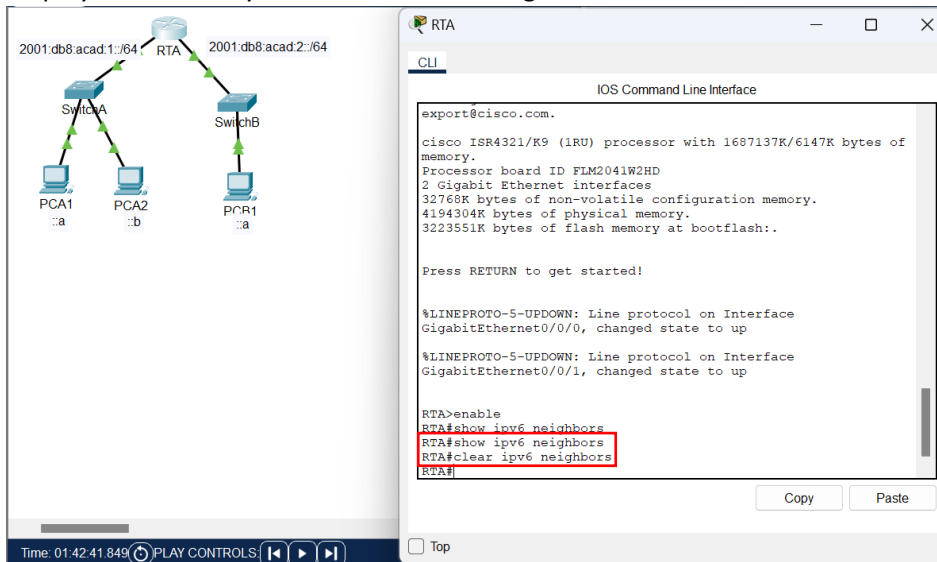
## Part 2: IPv6 Neighbor Discovery Remote Network

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.

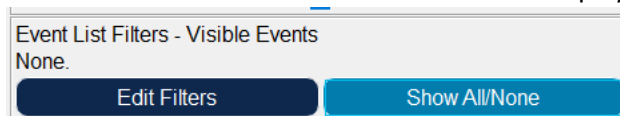
Make sure to click the Reset Simulation button to clear out the previous events.

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

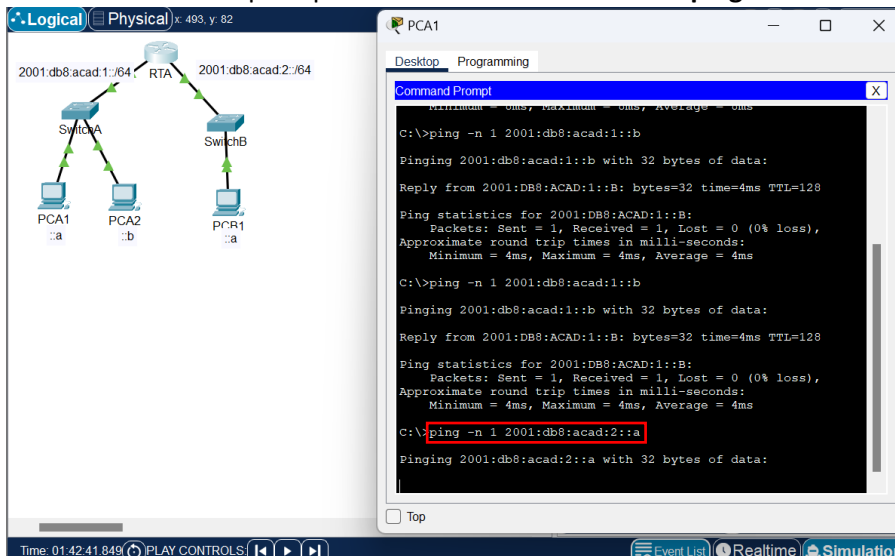
- Display and clear any entries in the IPv6 neighbor device table as was done in Part 1.



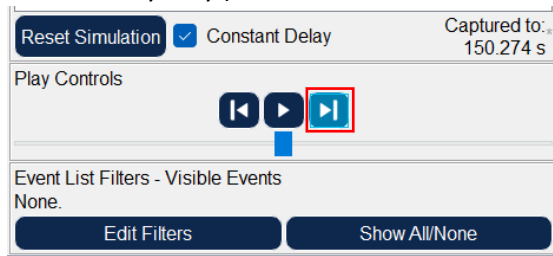
- Switch to simulation mode. Click the **Show All/None** button in the lower left part of the Simulation Panel. Make certain the **Event List Filters – Visible Events** displays **None**.



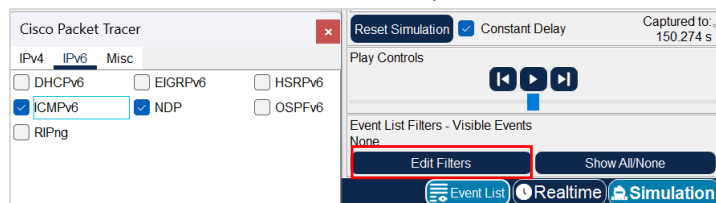
- From the command prompt on PCA1 issue the command **ping -n 1 2001:db8:acad:2::a** to ping host PCB1.



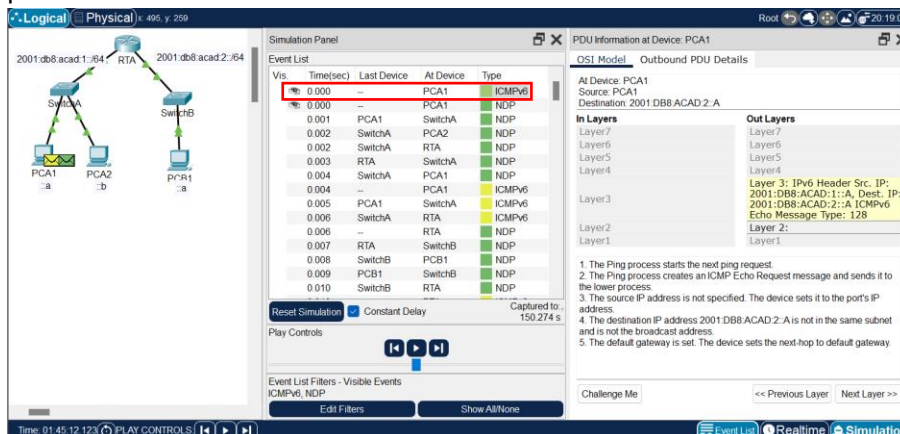
- d. Click the **Play Capture Forward** button which is displayed as an arrow pointing to the right with a vertical bar within the Play Controls box. The status bar above the Play Controls should read Captured to 150. (The exact number may vary.)



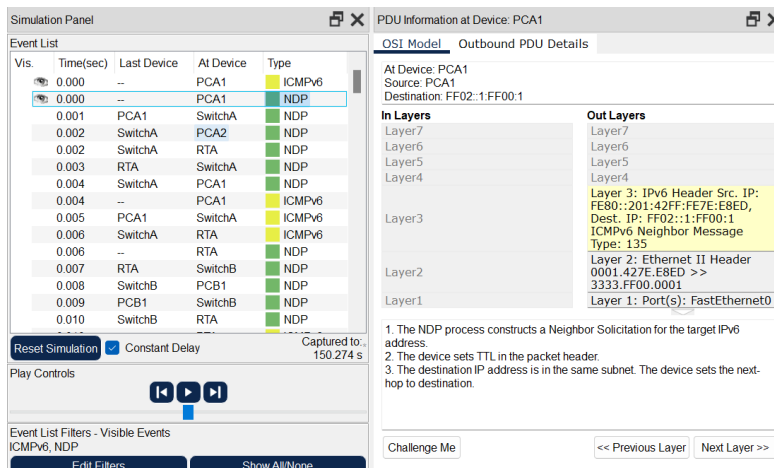
- e. Click the **Edit Filters** button. Select the IPv6 tab at the top and check the boxes for **ICMPv6** and **NDP**. Click the red X in the upper right of the Edit ACL Filters window. All of the previous events should now be listed. You should notice there are considerably more entries listed this 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.



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



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

There isn't a Src IP in the inbound PDU. However, the Src IP in the *outbound* PDU is FE80::201:42FF:F373:E8ED.

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.

The screenshot shows the Packet Tracer interface. On the left, the 'Event List' panel displays a table of events. The second ICMPv6 event for PCA1 is selected. On the right, the 'PDU Information at Device: PCA1' panel shows the 'Outbound PDU Details' tab. The 'In Layers' section lists Layer 7 through Layer 1. The 'Out Layers' section lists Layer 7 through Layer 1. The 'Layer 3: IPv6 Header' section shows the source IP as 2001:DB8:ACAD:1::A and the destination IP as 2001:DB8:ACAD:2::A. The 'Layer 2: Ethernet II Header' section shows the source MAC as 0001.427E.E8ED and the destination MAC as 0001.961D.6301. The 'Layer 1: Port(s)' section shows FastEthernet0.

Vis	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
	0.002	SwitchA	RTA	NDP
	0.003	RTA	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	RTA	ICMPv6
	0.006	--	RTA	NDP
	0.007	RTA	SwitchB	NDP
	0.008	SwitchB	PCB1	NDP
	0.009	PCB1	SwitchB	NDP
	0.010	SwitchB	RTA	NDP

### What MAC address is being used for the destination MAC?

0001.961D.6301. This MAC address belongs to our RTA device (router) through Gig0/0/0.

- 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.

The screenshot shows the Packet Tracer interface. On the left, the 'Event List' panel displays a table of events. The second ICMPv6 event for RTA is selected. On the right, the 'PDU Information at Device: RTA' panel shows the 'Inbound PDU Details' tab. The 'In Layers' section lists Layer 7 through Layer 1. The 'Out Layers' section lists Layer 7 through Layer 1. The 'Layer 3: IPv6 Header' section shows the source IP as 2001:DB8:ACAD:1::A and the destination IP as 2001:DB8:ACAD:2::A. The 'Layer 2: Ethernet II Header' section shows the source MAC as 0001.427E.E8ED and the destination MAC as 0001.961D.6301. The 'Layer 1: Port' section shows GigabitEthernet0/0/0.

Vis	Time(sec)	Last Device	At Device	Type
	0.000	--	PCA1	ICMPv6
	0.000	--	PCA1	NDP
	0.001	PCA1	SwitchA	NDP
	0.002	SwitchA	PCA2	NDP
	0.002	SwitchA	RTA	NDP
	0.003	RTA	SwitchA	NDP
	0.004	SwitchA	PCA1	NDP
	0.004	--	PCA1	ICMPv6
	0.005	PCA1	SwitchA	ICMPv6
	0.006	SwitchA	RTA	ICMPv6
	0.006	--	RTA	NDP
	0.007	RTA	SwitchB	NDP
	0.008	SwitchB	PCB1	NDP
	0.009	PCB1	SwitchB	NDP
	0.010	SwitchB	RTA	NDP

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

**Simulation Panel**

Vis.	Time(sec)	Last Device	At Device	Type
0.004	SwitchA	PCA1	PCA1	NDP
0.004	--	PCA1	PCA1	ICMPv6
0.005	PCA1	SwitchA	RTA	ICMPv6
0.006	SwitchA	RTA	RTA	NDP
0.006	--	RTA	RTA	ICMPv6
0.007	RTA	SwitchB	PCB1	NDP
0.008	SwitchB	PCB1	PCB1	NDP
0.009	PCB1	SwitchB	RTA	ICMPv6
0.010	SwitchB	RTA	RTA	NDP
0.010	--	RTA	RTA	ICMPv6
0.011	RTA	SwitchB	PCB1	ICMPv6
0.012	SwitchB	PCB1	PCB1	ICMPv6
0.012	--	PCB1	PCB1	NDP
0.013	PCB1	SwitchB	RTA	ICMPv6
0.014	SwitchB	RTA	RTA	NDP

**PDU Information at Device: PCB1**

At Device: PCB1  
Source: PCA1  
Destination: 2001:DB8:ACAD:2::A

**In Layers**

Layer 7  
Layer 6  
Layer 5  
Layer 4  
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 FastEthernet0

**Out Layers**

Layer 7  
Layer 6  
Layer 5  
Layer 4  
Layer 3: IPv6 Header Src. IP: 2001:DB8:ACAD:2::A, Dest. IP: 2001:DB8:ACAD:1::A ICMPv6 Echo Message Type: 129  
Layer 2:  
Layer 1:

1. FastEthernet0 receives the frame.

Challenge Me << Previous Layer Next Layer >>

**What is missing in the outbound Layer 2 information?**

The destination MAC address. (It 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.

**Simulation Panel**

Reset Simulation ☒ Constant Delay Captured to: (no captures)

```
C:\>ping -n 1 2001:db8:acad:2::a
Pinging 2001:db8:acad:2::a with 32 bytes of data:
```

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

**Simulation Panel**

2001:db8:acad:1::/64 RTA 2001:db8:acad:2::/64

SwitchA SwitchB

PCA1 PCA2 PCB1

**Event List**

Vis.	Time(sec)	Last Device	At Device	Type
0.000	--	PCA1	PCA1	ICMPv6
0.001	PCA1	SwitchA	SwitchA	ICMPv6
0.002	SwitchA	RTA	RTA	ICMPv6
0.003	RTA	SwitchB	SwitchB	ICMPv6
0.004	SwitchB	PCB1	PCB1	ICMPv6
0.005	PCB1	SwitchB	RTA	ICMPv6
0.006	SwitchB	RTA	RTA	ICMPv6
0.007	RTA	SwitchA	SwitchA	ICMPv6
0.008	SwitchA	PCA1	PCA1	ICMPv6

**Were there any NDP events?**

No, they were all ICMPv6 events.

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

**Simulation Panel**

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	-	PCA1	ICMPv6
	0.001	PCA1	SwitchA	ICMPv6
	0.002	SwitchA	RTA	ICMPv6
	0.003	RTA	SwitchB	ICMPv6
	0.004	SwitchB	PCB1	ICMPv6
	0.005	PCB1	SwitchB	ICMPv6
	0.006	SwitchB	RTA	ICMPv6
	0.007	RTA	SwitchA	ICMPv6
	0.008	SwitchA	PCA1	ICMPv6

**PDU Information at Device: PCB1**

At Device: PCB1  
Source: PCA1  
Destination: 2001:DB8:ACAD:2::A

**In Layers**

Layer7  
Layer6  
Layer5  
Layer4  
Layer3: IPv6 Header Src. IP: 2001:DB8:ACAD:1::A, Dest. IP: 2001:DB8:ACAD:2::A ICMPv6 Echo Message Type: 128  
Layer2: Ethernet II Header 0001.961D.6302 >> 0060.2F68.9E91  
**Layer 1: Port FastEthernet0**

**Out Layers**

Layer7  
Layer6  
Layer5  
Layer4  
Layer3: IPv6 Header Src. IP: 2001:DB8:ACAD:2::A, Dest. IP: 2001:DB8:ACAD:1::A ICMPv6 Echo Message Type: 129  
Layer2: Ethernet II Header 0060.2F68.9E91 >> **0001.961D.6302**  
Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Time: 01:45:21.684 PLAY CONTROLS

What does the destination MAC address correspond to?

0001.961D.6302 is the MAC address for the RTA (router).

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#show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
2001:DB8:ACAD:1::A                         3 0001.427E.E8ED REACH Gig0/0/0
2001:DB8:ACAD:2::A                         3 0060.2F68.9E91 REACH Gig0/0/1
FE80::201:42FF:FE7E:E8ED                   3 0001.427E.E8ED REACH Gig0/0/0
FE80::260:2FFF:FE68:9E91                   3 0060.2F68.9E91 REACH Gig0/0/1
```

How many addresses are listed?

4 (IPv6 global unicast and link local addresses and MAC addresses for PCA1 and PCB1)

What devices are these addresses associated with?

PCA1 and PCB1.

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

None because PCA2 has not communicated across the network.

Ping **PCA2** from the router.

```
RTA#ping 2001:db8:acad:1::b
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
```

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

```
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:1::B                         0 0040.0BD2.243E 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
```

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 IPv4.

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

A router usually keeps neighbor tables so that it does not need to initiate Neighbor Discovery 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 the 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 packets. 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. (It's similar to ARP table in IPv4.)