

# Packet Tracer 4.0 Skill Building Activity: Using Packet Tracer

## Objective

Use Packet Tracer to complete the following skills

- To learn to use Packet Tracer
- To examine Ping and MAC tables on various devices using various methods

## Scenario

These topologies represent two networks, one using a hub and the other using a switch. These topologies are ideal for studying ARP and ICMP behavior.

## Required Files

To complete this lab, you will need the following Packet Tracer (.pkt) files.

- UsingHub.pkt
- UsingSwitch.pkt

## Plan

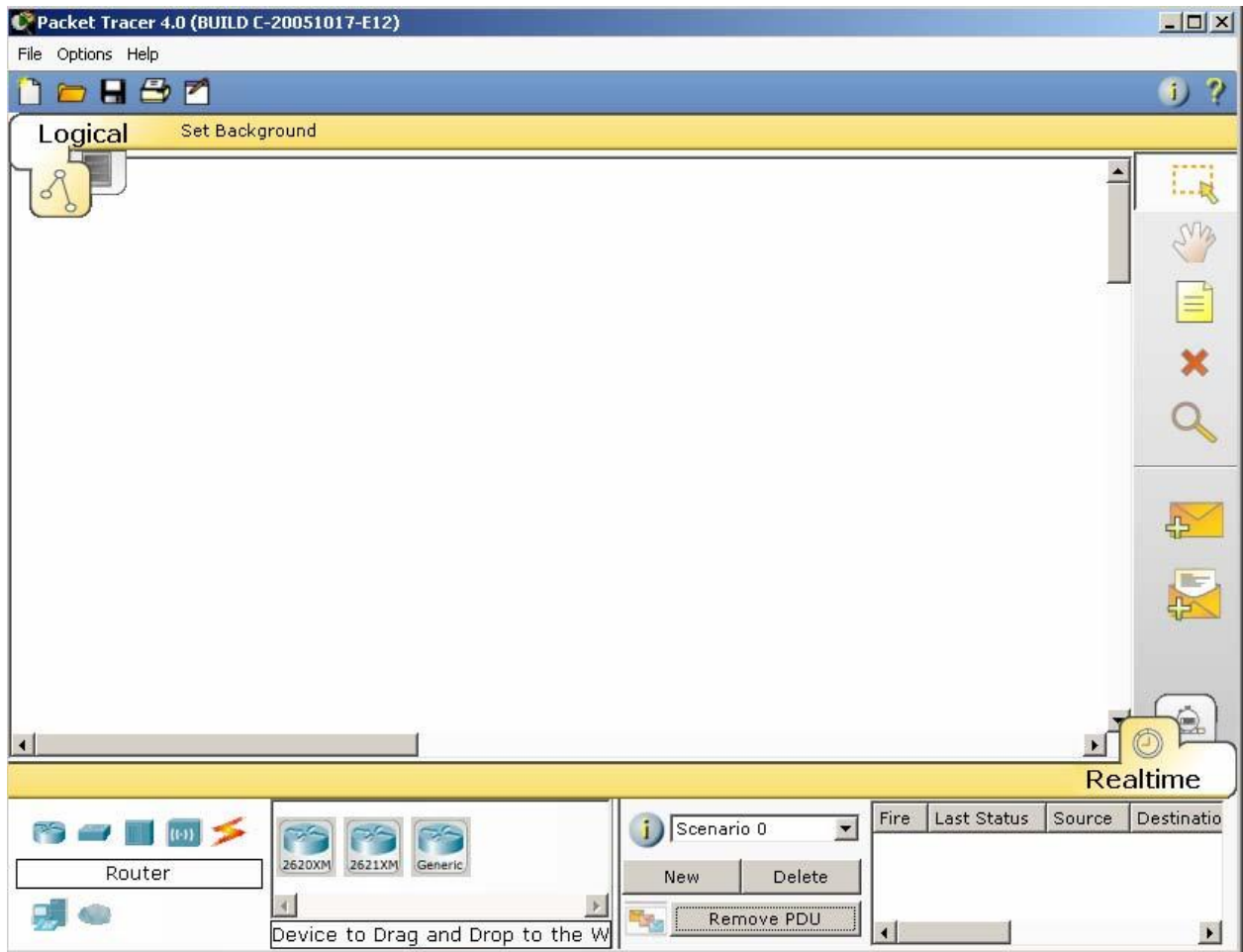
### To learn to use Packet Tracer.

**What is Packet Tracer?** Packet Tracer is a protocol simulator developed by Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced.

**Purpose:** The purpose of this activity is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own.

## Act 1 Introduction to the Packet Tracer Interface using a Hub Topology

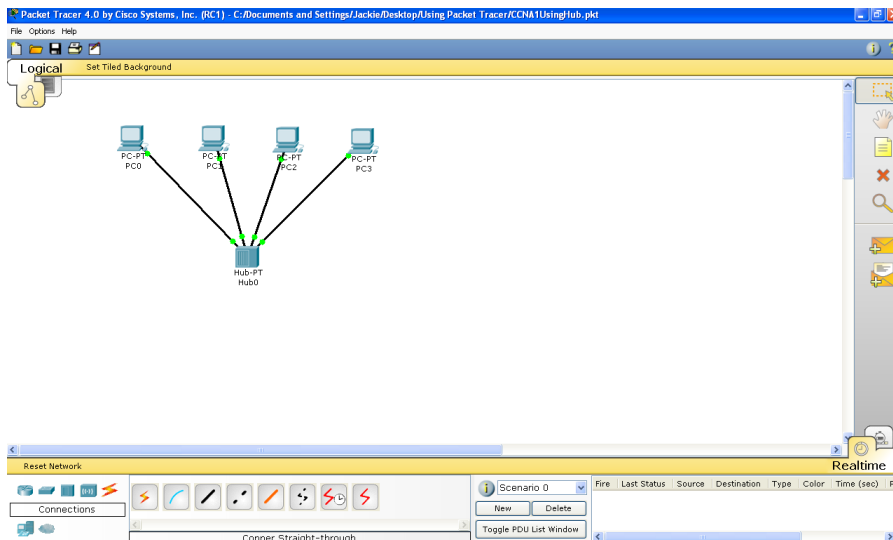
### Step 1 Start Packet Tracer and Entering Simulation Mode



## Step 2 Open an existing topology

Perform the following steps to open the **UsingHub.pkt** file.

- Open the file UsingHub.pkt.

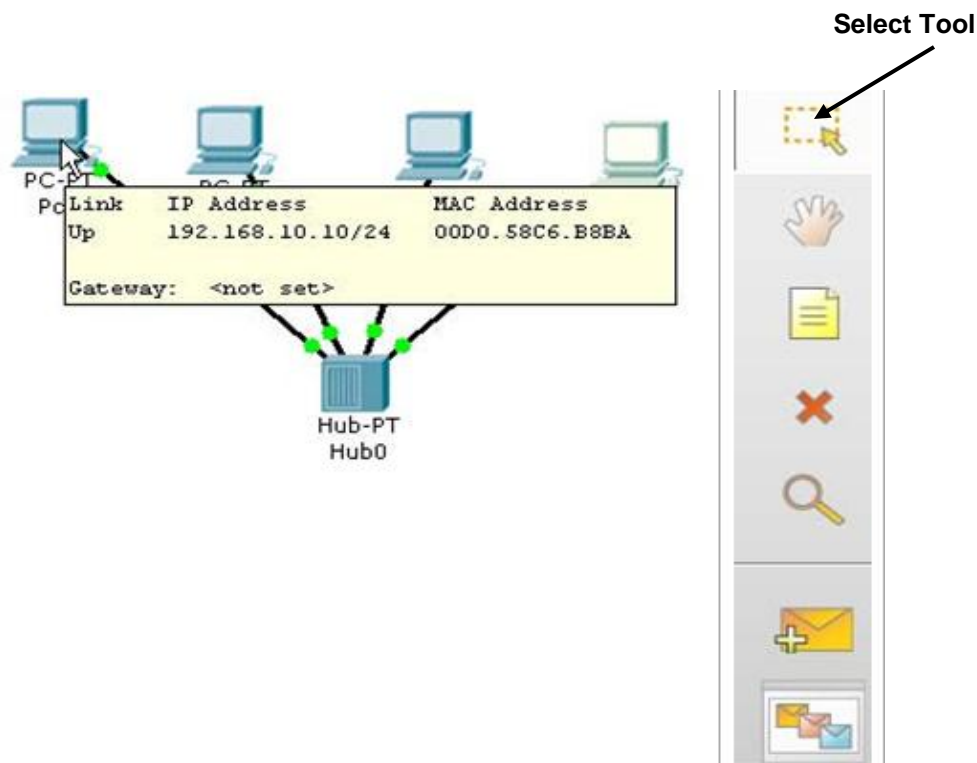


By default, the topology opens in **Realtime** mode. We will examine the difference between **Realtime** and **Simulation** modes in later steps.

**Simulation** mode allows you to view a sequence of events associated with the communications between two or more devices. **Realtime** mode performs the operation with all of the sequence of events happening at “real time”.

**Help** can be obtained by using the Help menu. Both online help and tutorials are available. Please take advantage of these facilities.

To view the IP address, subnet mask, default gateway, and MAC address of a host, move the cursor over that computer. Be sure the Select tool is selected.



### Step 3 Issue a ping from PC0 to PC1

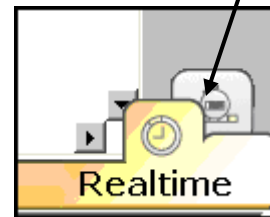
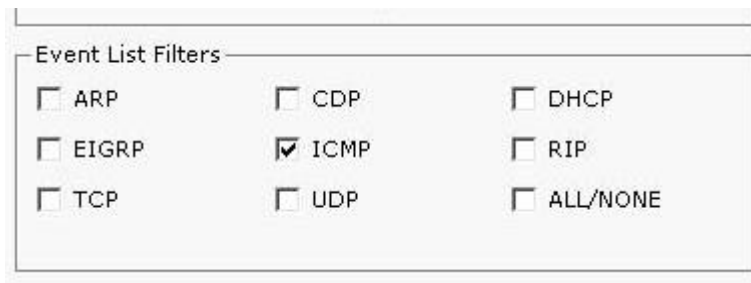
Pings and the ICMP protocol will be examined in much more detail in later steps. The ping program generates an IP packet with an encapsulated ICMP Echo Request message. It is a tool used to test basic layer 2 and layer 3 communications between two devices. When the user issues the ping command, most operating systems send multiple (four or five) ICMP Echo messages. When the destination device receives the ping, Echo Request, it issues an Echo Reply.

Command to be issued from PC0 is: **ping 192.168.10.37**

Packet Tracer allows you to either issue the command from the command prompt or to use the Add Simple PDU tool. Both methods will be used.

To enter Simulation Mode click the Simulation Mode tab in the lower right hand corner Of the interface.

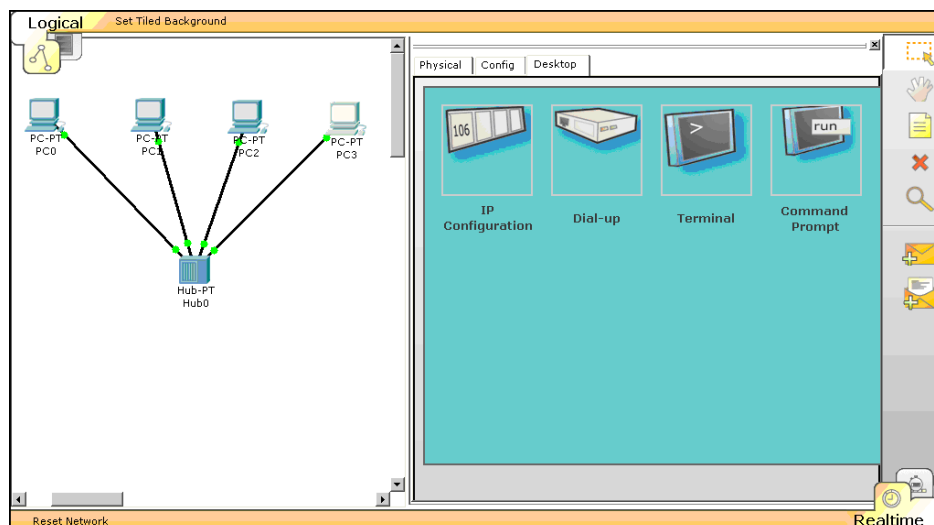
In order to view only the “pings”, in the **Event List**, click on **ALL/NONE** to clear all protocols, and then click on **ICMP** to select only that protocol.



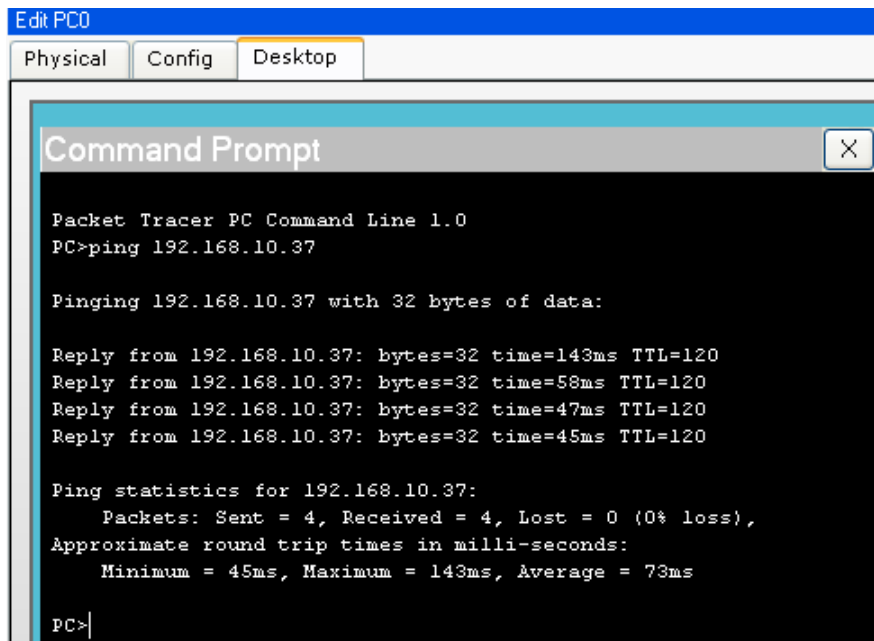
### Ping: Using the Command Prompt in Realtime Mode

Return to Realtime mode by clicking the Realtime tab in the lower right hand corner of the screen.

Single click on **PC0** with the left mouse button. 2. Click on the **Desktop** tab. 3. Click on the **Command Prompt**.



Click after **PC>** prompt and type the following ping command, **ping 192.168.10.37** and press the Enter key.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.37

Pinging 192.168.10.37 with 32 bytes of data:

Reply from 192.168.10.37: bytes=32 time=143ms TTL=120
Reply from 192.168.10.37: bytes=32 time=58ms TTL=120
Reply from 192.168.10.37: bytes=32 time=47ms TTL=120
Reply from 192.168.10.37: bytes=32 time=45ms TTL=120

Ping statistics for 192.168.10.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 143ms, Average = 73ms

PC>|
```

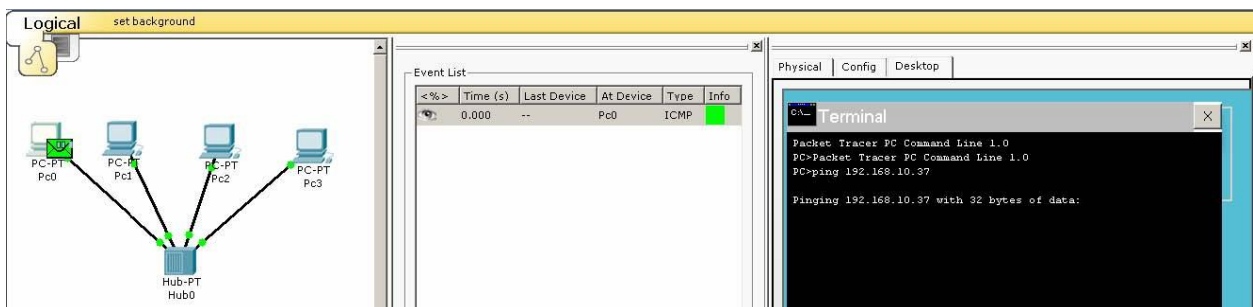
### Ping: Using the Simulation mode

Click on the **Simulation** tab located on the bottom right side of the Packet Tracer screen. The tab is located behind the **Realtime** mode tab.

If you cannot see the topology close the Event List window.

Reissue the ping command in the **Terminal** screen (Use the Up Arrow key to repeat the last command).

You will notice that an ICMP packet is now preparing to leave PC0 (left screen) and is also displayed in the **Event List** (middle screen).



Click on the **Capture / Forward** button in **Play Controls** (the yellow bar below the windows) to view a step-by-step process of the ping command.

As you click through the events, notice how the hub processes each frame (Ethernet frame, IP packet, and ICMP message). Notice that each event is listed in the Event List. Also, notice that the ping program displays the ICMP Echo Reply returned to PC0 from PC1.

The screenshot shows the Packet Tracer 4.0 interface. On the left, a network topology is displayed with four PCs (PC0, PC1, PC2, PC3) connected to a central hub (Hub0). The Event List window in the center shows a series of ICMP events. The Terminal window on the right shows the output of a ping command from PC0 to PC1.

| <%> | Time (s) | Last Device | At Device | Type | Info |
|-----|----------|-------------|-----------|------|------|
|     | 0.000    | --          | Pc0       | ICMP |      |
|     | 0.005    | --          | Pc0       | ICMP |      |
|     | 0.006    | Pc0         | Hub0      | ICMP |      |
|     | 0.007    | Hub0        | Pc1       | ICMP |      |
|     | 0.007    | Hub0        | Pc2       | ICMP |      |
|     | 0.007    | Hub0        | Pc3       | ICMP |      |
|     | 0.008    | Pc1         | Hub0      | ICMP |      |
|     | 0.009    | Hub0        | Pc0       | ICMP |      |
|     | 0.009    | Hub0        | Pc2       | ICMP |      |
|     | 0.009    | Hub0        | Pc3       | ICMP |      |

The Terminal window shows the following output:

```

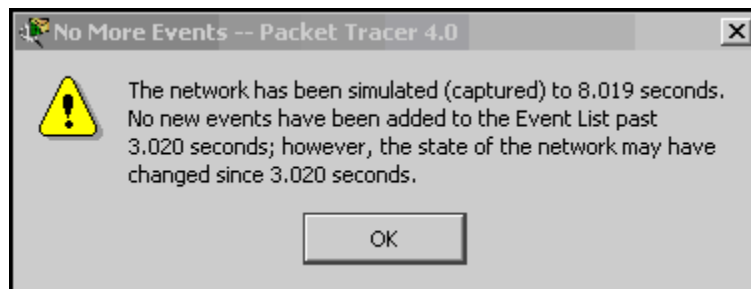
Packet Tracer PC Command Line 1.0
PC>Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.37

Pinging 192.168.10.37 with 32 bytes of data:

Reply from 192.168.10.37: bytes=32 time=9ms TTL=120
  
```

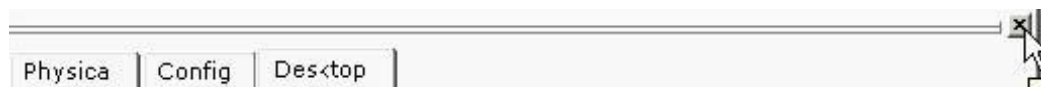
Continue clicking the Capture / Forward button until all frames have been sent. **Notice that the hub floods all of the frames out all ports except the port it came in on.**

When the ping program is finished sending four pings (ICMP Echo Requests) you will receive the following message:



### Using the Simple PDU Tool

Another method for pinging a device is the use of the **Simple PDU tool**. This tool performs the ping without having to issue the ping command. Before proceeding with this step, close the Desktop for PC0, click the "X" in the right-hand corner.

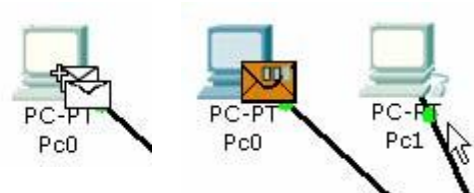


Restore the **Event List** if necessary by clicking Event List on the yellow bar to the left of Simulation and clicking the Reset Simulation button.

Choose the **Add Simple PDU** tool from the tool box:



Click once on PC0, the device issuing the ping (ICMP Echo Request) and then click once on PC1 (the destination of the ICMP Echo Request).

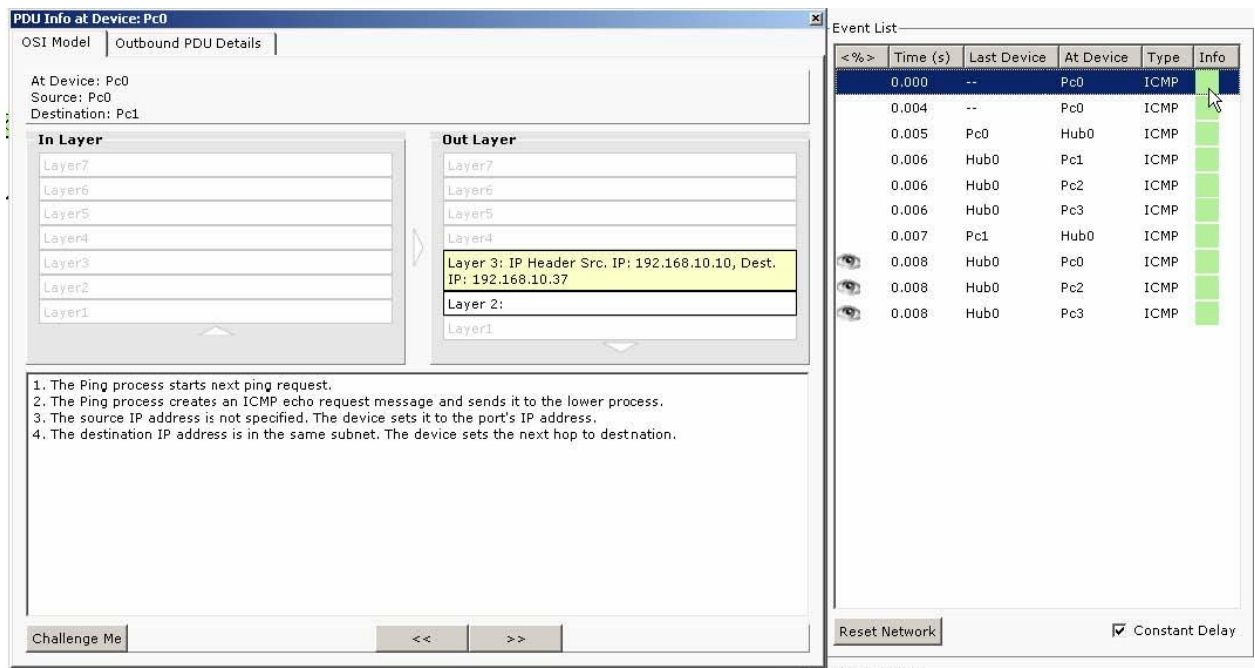


Click the Capture / Forward button and watch the ICMP Echo Requests and ICMP Echo Replies. **Notice that the hub floods all of the frames out all ports except the incoming port.**

**Note:** This tool only sends a single ICMP Echo Request instead of the four pings when using the command prompt.

#### Step 4 Viewing the frame using Protocol Analyzer

To examine the actual protocols being sent, click on the colored **Info** box in the **Event List**.



**PDU Info at Device: Pc0**

OSI Model | Outbound PDU Details

At Device: Pc0  
Source: Pc0  
Destination: Pc1

**In Layer**

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

**Out Layer**

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37
- Layer2:
- Layer1

1. The Ping process starts 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 is in the same subnet. The device sets the next hop to destination.

**Event List**

| <%> | Time (s) | Last Device | At Device | Type | Info |
|-----|----------|-------------|-----------|------|------|
|     | 0.000    | --          | Pc0       | ICMP |      |
|     | 0.004    | --          | Pc0       | ICMP |      |
|     | 0.005    | Pc0         | Hub0      | ICMP |      |
|     | 0.006    | Hub0        | Pc1       | ICMP |      |
|     | 0.006    | Hub0        | Pc2       | ICMP |      |
|     | 0.006    | Hub0        | Pc3       | ICMP |      |
|     | 0.007    | Pc1         | Hub0      | ICMP |      |
|     | 0.008    | Hub0        | Pc0       | ICMP |      |
|     | 0.008    | Hub0        | Pc2       | ICMP |      |
|     | 0.008    | Hub0        | Pc3       | ICMP |      |

Challenge Me << >> Reset Network ☒ Constant Delay



The default is a layer 3 **Outbound OSI Model** view with a brief description with what is occurring with this packet:

**PDU Info at Device: Pc0**

OSI Model | Outbound PDU Details

At Device: Pc0  
Source: Pc0  
Destination: Pc1

**In Layer**

Layer7

Layer6

Layer5

Layer4

Layer3

Layer2

Layer1

**Out Layer**

Layer7

Layer6

Layer5

Layer4

Layer3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37

Layer2:

Layer1

1. The Ping process starts 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 is in the same subnet. The device sets the next hop to destination.

Challenge Me << >>

Click on the **Outbound PDU Details** tab to see the layer 2 Ethernet frame, and the layer 3 IP packet and ICMP message.

**PDU Info at Device: Pc0**

OSI Model | Outbound PDU Details

PDU Formats

**Ethernet II**

| 0         |  | 4                      |  | 8              |  | 14 |  | 19             |  | Bytes |  |
|-----------|--|------------------------|--|----------------|--|----|--|----------------|--|-------|--|
| PREAMBLE: |  |                        |  | DEST MAC:      |  |    |  | SRC MAC:       |  |       |  |
| 1010 1010 |  |                        |  | 0002.16AB.5C50 |  |    |  | 00D0.58C6.B8BA |  |       |  |
| TYPE:     |  | DATA (VARIABLE LENGTH) |  |                |  |    |  | FCS:           |  |       |  |
| 0x800     |  |                        |  |                |  |    |  | 0x0            |  |       |  |

**IP**

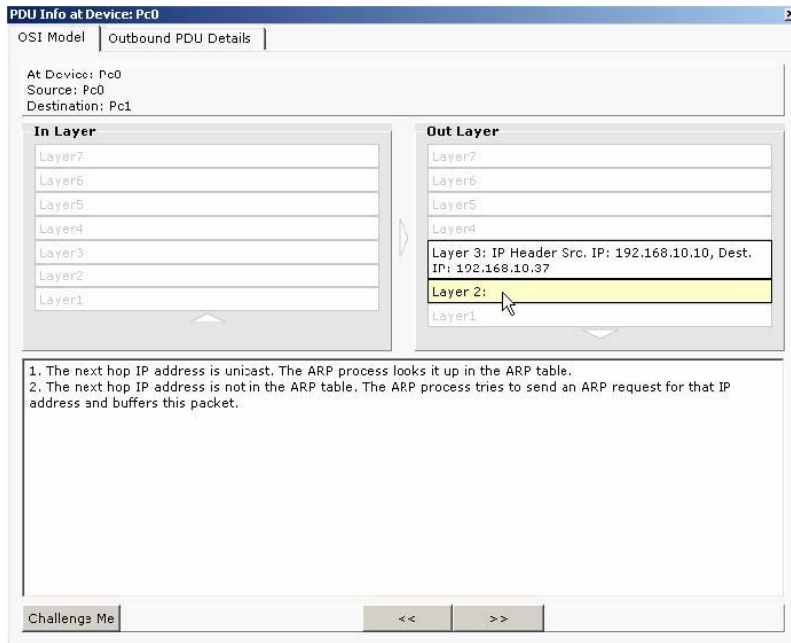
| 0                      |  | 4   |  | 8        |  | 16      |  | 19               |  | 31  |  | Bits |  |
|------------------------|--|-----|--|----------|--|---------|--|------------------|--|-----|--|------|--|
| 4                      |  | IHL |  | TOS: 0x0 |  | TL: 0x0 |  |                  |  |     |  |      |  |
| ID: 0x0                |  |     |  | 0x0      |  |         |  | FRAG OFFSET: 0x0 |  |     |  |      |  |
| TTL: 32                |  |     |  | PRO: 0x1 |  |         |  | CHKSUM: 0x0      |  |     |  |      |  |
| SRC IP: 192.168.10.10  |  |     |  |          |  |         |  |                  |  |     |  |      |  |
| DST IP: 192.168.10.37  |  |     |  |          |  |         |  |                  |  |     |  |      |  |
| OPT: 0x0               |  |     |  |          |  |         |  |                  |  | 0x0 |  |      |  |
| DATA (VARIABLE LENGTH) |  |     |  |          |  |         |  |                  |  |     |  |      |  |

**ICMP**

| 0         |  | 8         |  | 16            |  | 31 |  | Bits |  |
|-----------|--|-----------|--|---------------|--|----|--|------|--|
| TYPE: 0x8 |  | CODE: 0x0 |  | CHECKSUM: 0x0 |  |    |  |      |  |

Click on layer 2 of the **Outbound OSI Model** view with a brief description with what is occurring at layer 2:





## Act 2 Looking at the Switch Algorithm and Switch MAC Address Tables

### Step 1

Open the **UsingSwitch.pkt** file. Do not save the changes to the current network. Notice the similarity to the previous topology. The layer 1 hub has been replaced with a layer 2 switch.

Click on the **Simulation** icon to switch to simulation mode.

### Step 2 Viewing the Switch MAC Address Table

Use the **Select** tool to view IP address and MAC address information for the various hosts.

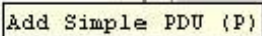


Use the **Inspect** tool to view the MAC Address Table of the switch.

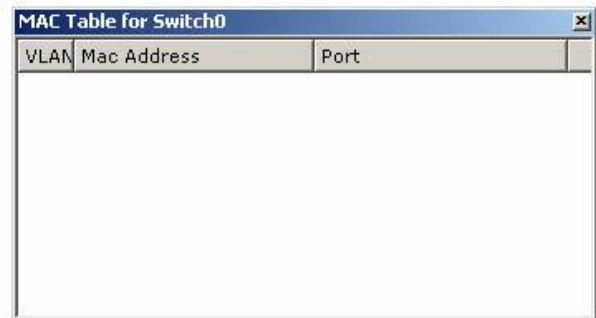


The MAC Address Table is empty as it has not learned any Source Ethernet MAC Addresses. Notice that there is also a VLAN column in this table. This will be discussed in future courses.



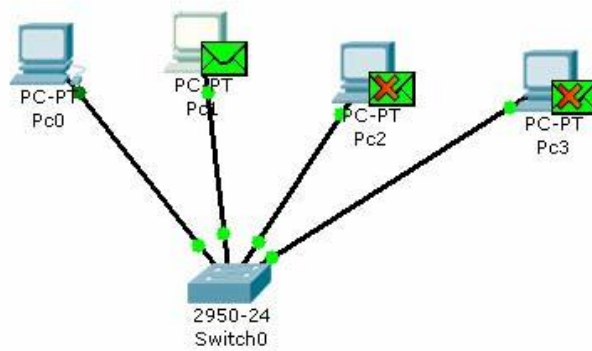


PC0 forwards the frame containing the ARP request to Switch0:



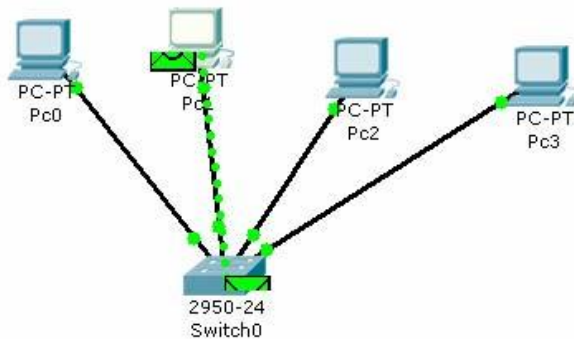
| VLAN | Mac Address    | Port            |
|------|----------------|-----------------|
| 1    | 0030.F274.8E79 | FastEthernet0/1 |

The packet is flooded out all ports because the Switch's MAC Address Table does not contain the Destination Address of the Ethernet frame. PC2 and PC3 disregard the frame:



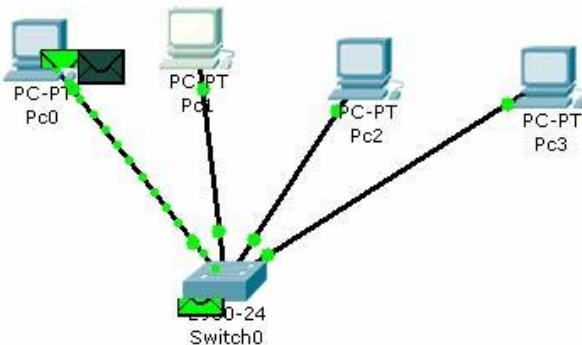
| MAC Table for Switch0 |                |                 |
|-----------------------|----------------|-----------------|
| VLAN                  | Mac Address    | Port            |
| 1                     | 0030.F274.8E79 | FastEthernet0/1 |

PC1 return the ARP reply. Switch0 learns the Source MAC Address of PC1:



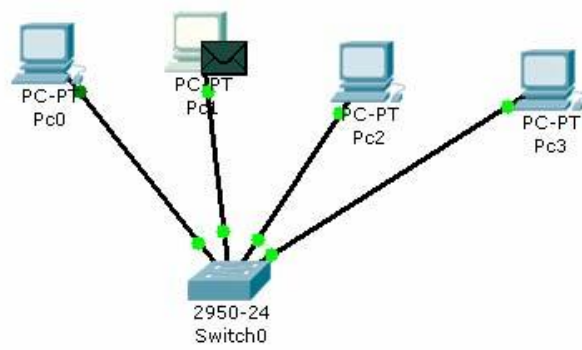
| MAC Table for Switch0 |                |                 |
|-----------------------|----------------|-----------------|
| VLAN                  | Mac Address    | Port            |
| 1                     | 0001.C798.4163 | FastEthernet0/2 |
| 1                     | 0030.F274.8E79 | FastEthernet0/1 |

Because the Source MAC Address of PC0 was learned previously, when examining the Destination MAC Address of the frame, Switch0 filters the frame by only sending it out FastEthernet port 0/1



| MAC Table for Switch0 |                |                 |
|-----------------------|----------------|-----------------|
| VLAN                  | Mac Address    | Port            |
| 1                     | 0001.C798.4163 | FastEthernet0/2 |
| 1                     | 0030.F274.8E79 | FastEthernet0/1 |

The rest of the pings, frames with IP packets containing ICMP Echo Requests from PC0 destined for PC1 and frames with IP packets containing ICMP Echo Replies from PC1 destined for PC0, are filtered by the switch and only sent out the appropriate interface (port).



| MAC Table for Switch0 |                |                 |
|-----------------------|----------------|-----------------|
| VLAN                  | Mac Address    | Port            |
| 1                     | 0001.C798.4163 | FastEthernet0/2 |
| 1                     | 0030.F274.8E79 | FastEthernet0/1 |

#### Step 4 Creating multiple scenarios

A technique used to learn new software is to experiment. Try different tools, look at various protocols using the Event List and the Info box, and use the Help and Tutorials. Have fun!