

Name : Arka Haldi
Date : 24/8/2020
UID : 2018130014

CEL 51, DCCN, Monsoon 2020

Lab 3: Learn usage of Packet Tracer

OBJECTIVES:

- Install Packet Tracer from <https://www.ciscopods.com/install-packet-tracer-ubuntu/>
- Develop an understanding of the basic functions of Packet Tracer.
- Create/model a simple Ethernet network using two hosts and a hub.
- Observe traffic behavior on the network.
- Observer data flow of ARP broadcasts and pings.

SETUP STEPS:

Step 1: Create a logical network diagram with two PCs and a hub

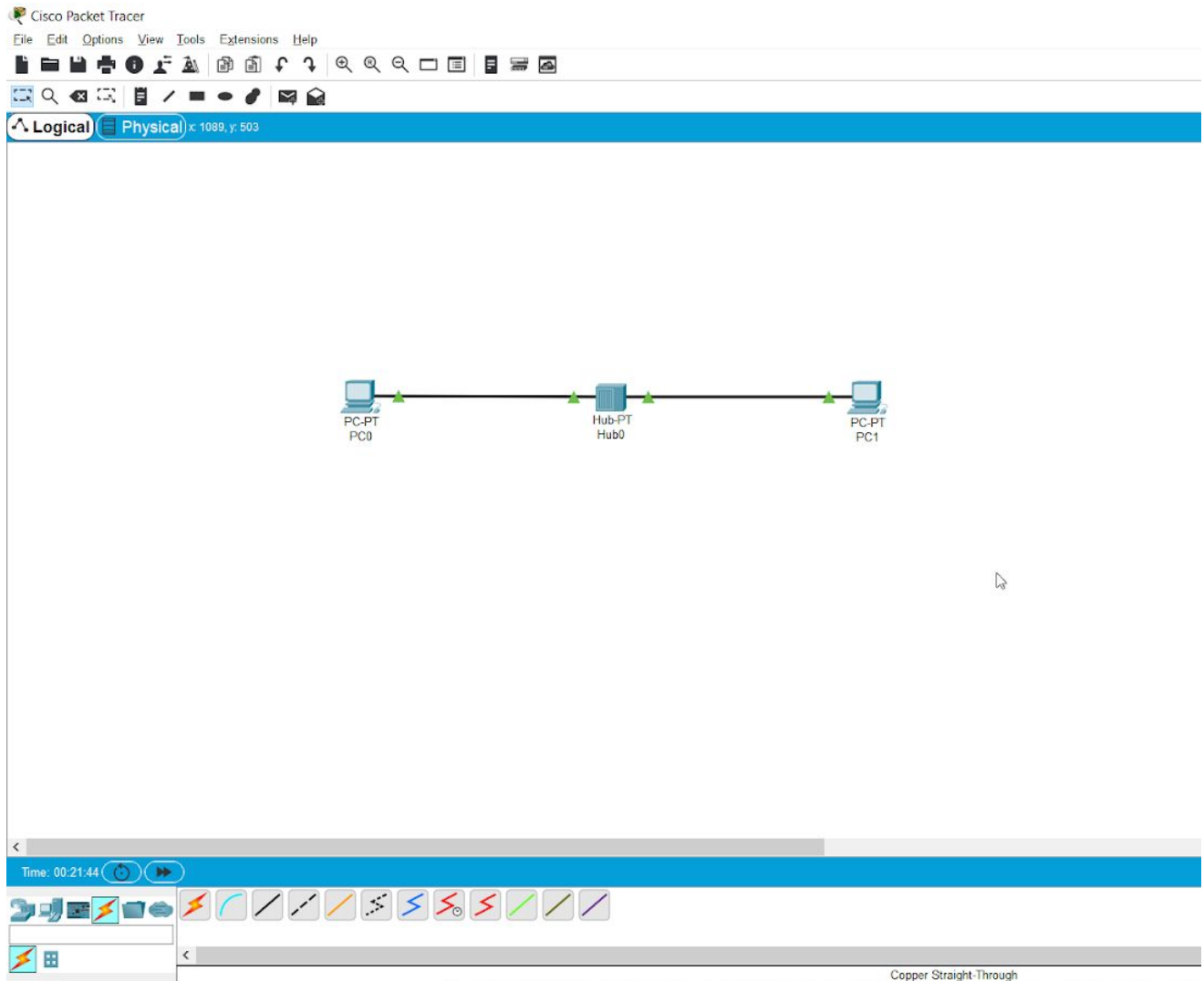
The bottom left-hand corner of the Packet Tracer screen displays eight icons that represent device categories or groups, such as Routers, Switches, or End Devices.

Moving the cursor over the device categories will show the name of the category in the box. To select a device, first select the device category. Once the device category is selected, the options within that category appear in the box next to the category listings. Select the device option that is required.

Observations

- a) Select **End Devices** from the options in the bottom left-hand corner. Drag and drop two generic PCs onto your design area.
- b) Select **Hubs** from the options in the bottom left-hand corner. Add a hub to the prototype network by dragging and dropping a generic hub onto the design area.
- c) Select **Connections** from the bottom left-hand corner. Choose a **Copper Straight-through** cable type. Click the first host, **PC0**, and assign the cable to the **FastEthernet** connector. Click the hub, **Hub0**, and select a connection port, **Port 0**, to connect to **PC0**.
- d) Repeat Step c for the second PC, **PC1**, to connect the PC to **Port 1** on the hub.

Snapshot:



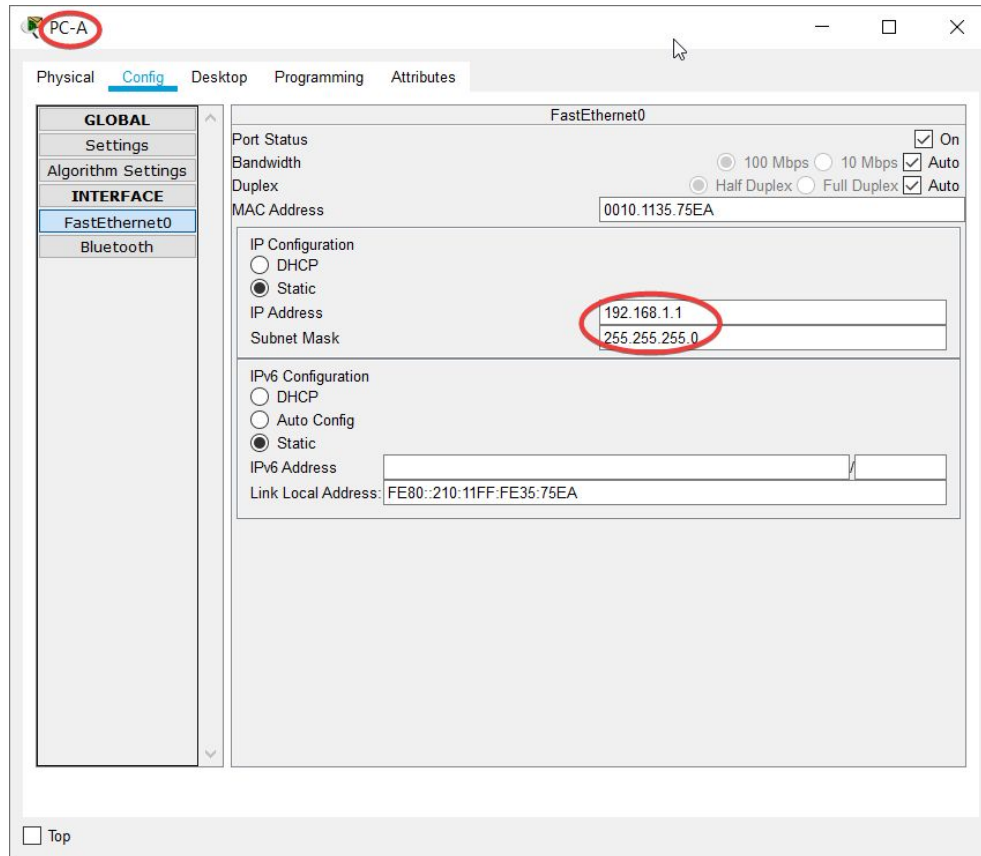
Description:

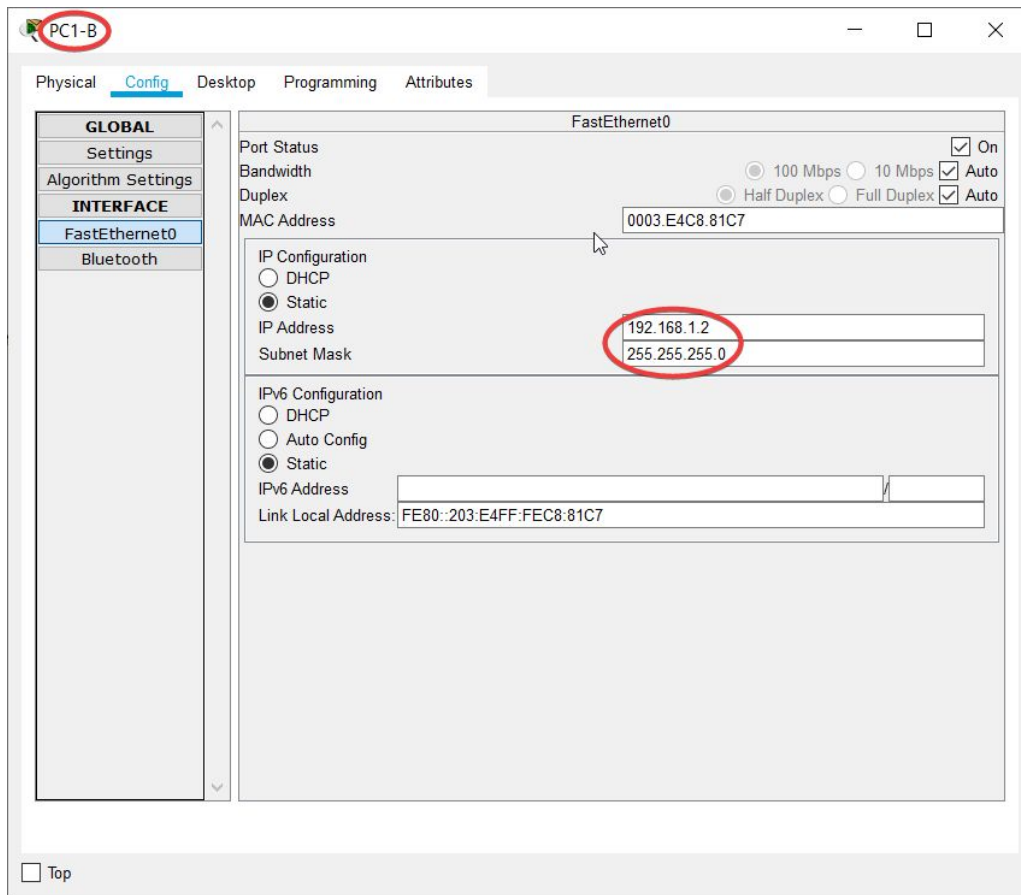
- Made the basic connections of the two PCs to the hub, renaming as necessary and observed the green arrows immediately after completing connection to the fast ethernet ports, indicating that the ports are on and working. [\[1\]](#)

Step 2: Configure host names and IP addresses on the PCs

- a) Click PC0. A PC0 window will appear.
- b) From the PC0 window, select the **Config** tab. Change the PC **Display Name** to **PC-A**. (An error message window will appear warning that changing the device name may affect scoring of the activity. Ignore this error message.) Select the **FastEthernet** tab on the left and add the IP address of **192.168.1.1** and subnet mask of **255.255.255.0**. Close the PC-A configuration window by selecting the **x** in the upper righthand corner.
- c) Click PC1.
- d) Select the **Config** tab. Change the PC **Display Name** to **PC-B**. Select the **FastEthernet** tab on the left and add the IP address of **192.168.1.2** and subnet mask of **255.255.255.0**. Close the PC-B configuration window.

Snapshot:



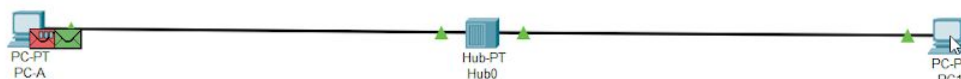


Description:

- Assigned unique two IP addresses to PC-A and PC-B to observe their interactions over the hub, everything is ready for a simulation at the end of this step. We act like Network service providers registering the devices to the new IP addresses.

Step 3: Observe the flow of data from PC-A to PC-B by creating network traffic

- Switch to **Simulation** mode by selecting the tab that is partially hidden behind the **Realtime** tab in the bottom right-hand corner. The tab has the icon of a stopwatch on it.
- Click the **Edit Filters** button in the **Edit List Filters** area. Clicking the **Edit Filters** button will create a pop-up window. In the pop-up window, click the **Show All/None** box to deselect every filter. Select just the **ARP** and **ICMP** filters.
- Select a **Simple PDU** by clicking the closed envelope on the right vertical toolbar. Move your cursor to the display area of your screen. Click **PC-A** to establish the source. Move your cursor to **PC-B** and click to establish the destination.



Description:

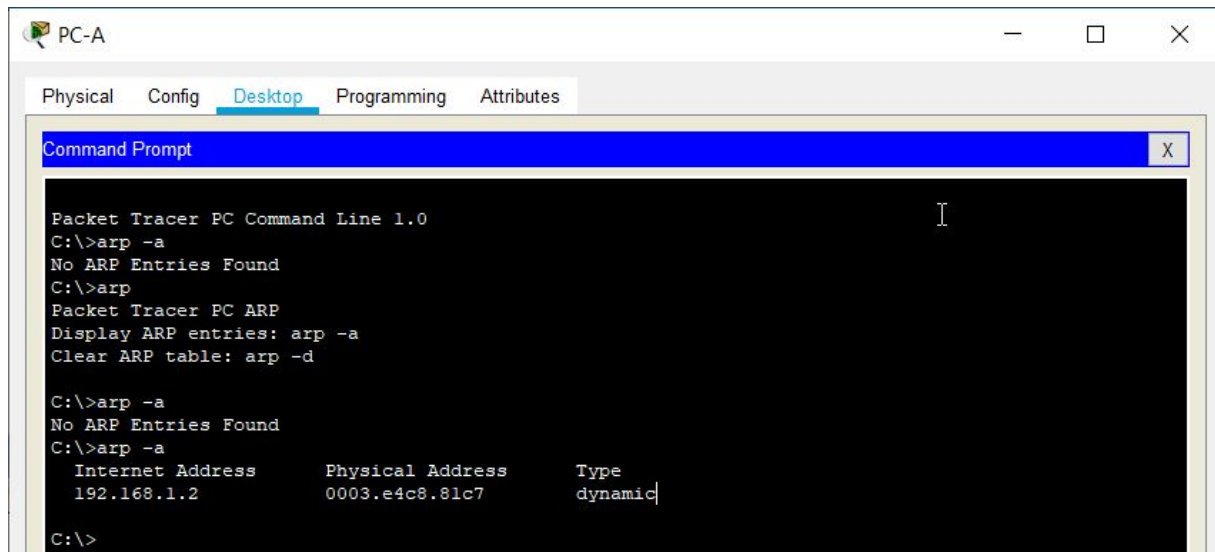
Two envelopes are positioned beside PC-A. Red envelope is ICMP, while the green is ARP.

- d) Select **Auto Capture / Play** from the **Play Controls** area of the Simulation Panel. Below the **Auto Capture / Play** button is a horizontal bar, with a vertical button that controls the speed of the simulation. Dragging the button to the right will speed up the simulation, while dragging is to the left will slow down the simulation.
- e) The animation will run until the message window *No More Events* appears. All requested events have been completed. Select OK to close the message box.
- f) Choose the **Reset Simulation** button in the Simulation Panel. Notice that the ARP envelope is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries. The ARP request is not necessary to complete the **ping** command because PC-A already has the MAC address in the ARP table.
- g) Choose the **Capture / Forward** button. The ICMP envelope will move from the source to the hub and stop. The **Capture / Forward** button allows you to run the simulation one step at a time. Continue selecting the **Capture / Forward** button until you complete the event.
- h) Choose the **Power Cycle Devices** button on the bottom left, above the device icons.
- i) An error message will appear asking you to confirm reset. Choose **Yes**. Now both the ICMP and ARP envelopes are present again. The **Reset Network** button will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.

Step 4: View ARP Tables on each PC

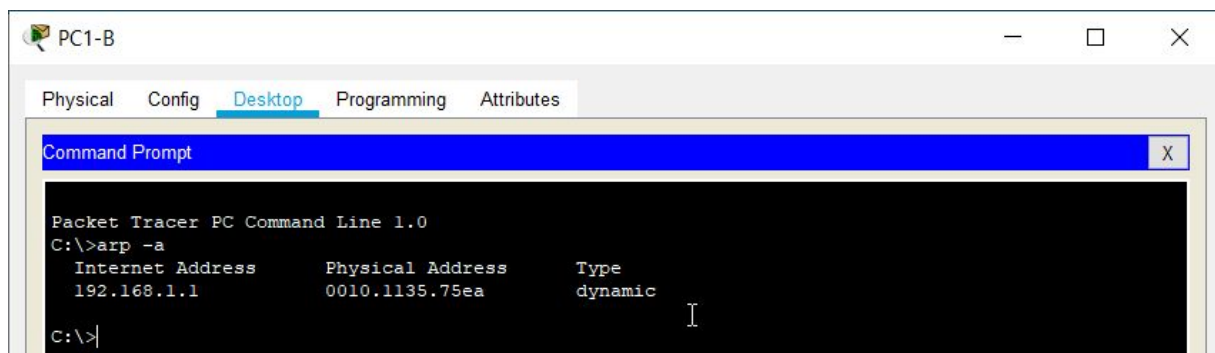
- a) Choose the **Auto Capture / Play** button to repopulate the ARP table on the PCs. Click **OK** when the *No More Events* message appears.
- b) Select the magnifying glass on the right vertical tool bar.
- c) Click **PC-A**. The ARP table for PC-A will appear. Notice that PC-A does have an ARP entry for PC-B. View the ARP tables for PC-B and PC-A as well. Close all ARP table windows.
- d) Click the **Select Tool** on the right vertical tool bar. (This is the first icon present in the toolbar.)
- e) Click **PC-A** and select the **Desktop** tab.
- f) Select the **Command Prompt** and type the command **arp -a** and press *enter* to view the ARP table from the desktop view. Close the PC-A configuration window.

- g) Examine the ARP table for **PC-B**.
- h) Close the PC-B configuration window.
- i) Click the **Check Results** button at the bottom of the instruction window to verify that the topology is correct.



```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d

C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.2           0003.e4c8.81c7       dynamic
C:\>
```



```
Packet Tracer PC Command Line 1.0
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.1           0010.1135.75ea       dynamic
C:\>
```

Description:

We notice that the PC-B is connected to the PC-A, as the IP address of A is shown to be present in the

THEORY:

Address Resolution Protocol (ARP) :

It is a Layer 2 Protocol, and uses Physical addresses (MAC addresses) for the communication. Here, ARP Protocol is used to convert a given IP address to the related hardware address (MAC Address) to provide this. This important duty makes this protocol a key protocol for Ethernet based networks.^[2]

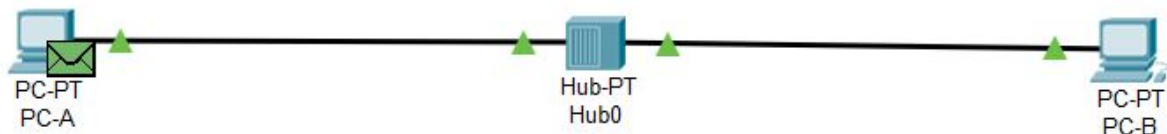
Protocol Data Unit (PDU):

It is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol-specific control information and user data. In the layered architectures of communication protocol stacks, each layer implements protocols tailored to the specific type or mode of data exchange^[3]

Internet Protocol Message Protocol (ICMP):

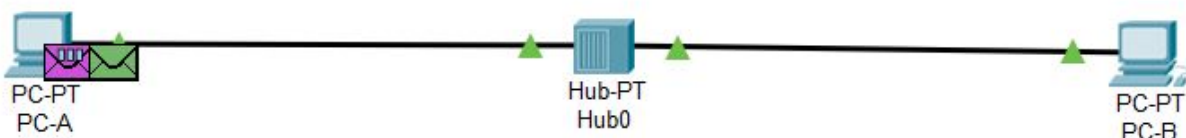
ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.^[4]

OBSERVATIONS:



1. When the ARP tables on both PC's are empty and PC-A pings PC-B

- The ping request is made using the ICMP protocol and starts at Layer-3 or network layer, as is evident by the following screenshot.
- The request gets forwarded to the underlying layer, which finds the IP address' MAC address in the ARP table. Since, it has no prior information on MAC, it schedules an ARP request, broadcasting the request for IP of PC-B, to send it's MAC address to add the MAC address to the ARP table, establish a dynamic connection, and send the ICMP request to PC-B.



- **purple envelope properties**

OSI Model Outbound PDU Details

At Device: PC-A Source: PC-A Destination: PC-B	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2 ICMP Message Type: 8
Layer2	Layer 2:
Layer1	Layer1

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 device sets TTL in the packet header.
5. The destination IP address is in the same subnet. The device sets the next-hop to destination.

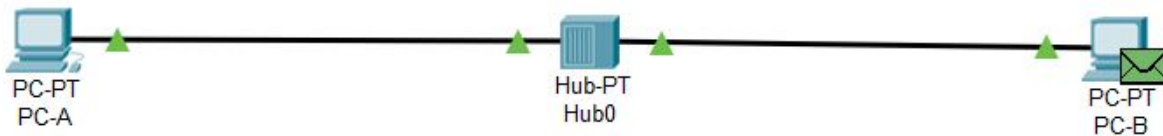
- **green envelope properties**

OSI Model Outbound PDU Details

At Device: PC-A Source: PC-A Destination: Broadcast	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 0004.9AA7.ADAE >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2
Layer1	Layer 1: Port(s): FastEthernet0

1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.

- We notice that the default MAC address reserved for a broadcast in the Data Link layer is FFFF.FFFF.FFFF
- We also note that the information of the Source and Destination IP addresses has also been moved to the Lower Layer, by the help of headers.
- Then the request is forwarded by the Hub to reach and be intercepted by the receiver port of PC-B which recognises the IP requested in the message belongs to itself.



OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: PC-A
Source: PC-B
Destination: Broadcast

In Layers

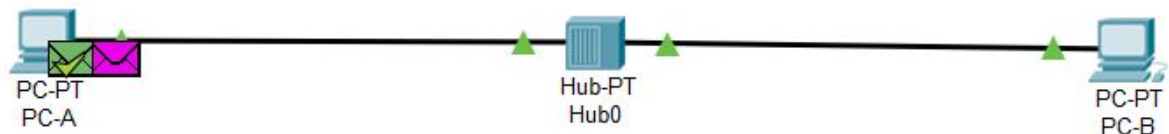
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0001.438B.98CE >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1
Layer 1: Port FastEthernet0

Out Layers

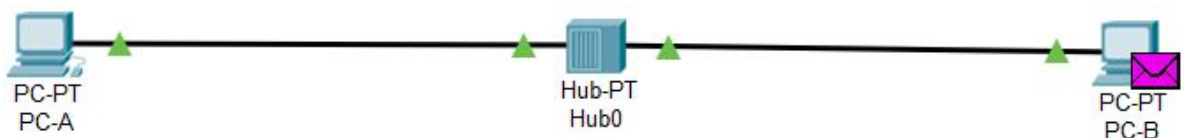
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0004.0AA7.ADAE >> 0001.438B.98CE ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2
Layer 1: Port(s): FastEthernet0

1. The ARP process replies to the request with the receiving port's MAC address.
2. The device encapsulates the PDU into an Ethernet frame.

- PC-B intercepts the ARP request at **level2**, registers the IP address in it's own ARP table and sends an ARP response with its own MAC address.
- PC-A receives the response and updates it's own ARP table, finishing the transaction, and prepares the ICMP packet to be sent, to ping PC-B.



- The ICMP request is sent via the Hub and received by PC-B, without any conflict as now they both know each other's MAC address.



PDU Information at Device: PC-B

[OSI Model](#)

[Inbound PDU Details](#)

[Outbound PDU Details](#)

At Device: PC-B
Source: PC-A
Destination: PC-B

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0004.9AA7.ADAE >> 0001.438B.98CE
Layer 1: Port FastEthernet0

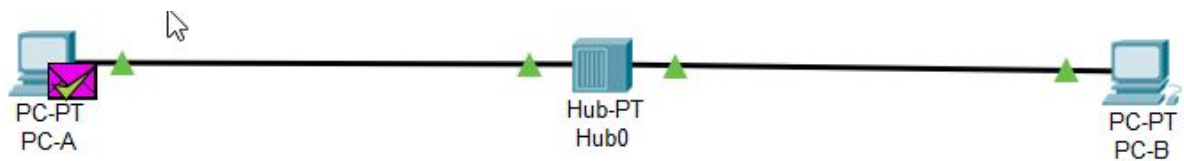
Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1 ICMP Message Type: 0
Layer 2: Ethernet II Header 0001.438B.98CE >> 0004.9AA7.ADAE
Layer 1: Port(s): FastEthernet0

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 Request message.

1. The ICMP process replies to the Echo Request by setting ICMP type to Echo Reply.
2. The ICMP process sends an Echo Reply.
3. The destination IP address is in the same subnet. The device sets the next-hop to destination.

- As we see above, the request is received by PC-B, recognises that the request is sent to its IP address, and decapsulates the packet to find an ICMP echo request message.
- It then responds to it with another echo message send using the ICMP protocol, and device sets the destination to the IP address that sent it the message.
- It is then received by PC-A, completing the transaction.



At Device: PC-A
Source: PC-A
Destination: PC-B

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1 ICMP Message Type: 0
Layer 2: Ethernet II Header 0001.438B. 98CE >> 0004.9AA7.ADAE
Layer 1: Port FastEthernet0

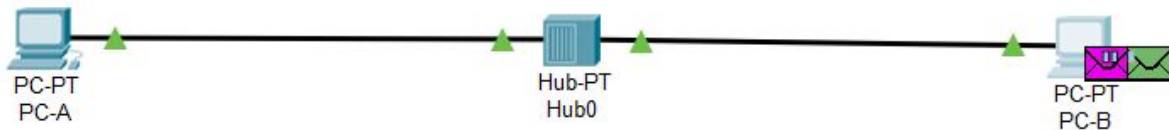
Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

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.

2. PC-A has ARP table, but PC-B has empty ARP table(PC-B lost power)

- The ICMP request is sent over to PC-B, but PC-B doesn't have a MAC address corresponding to PC-A, so even after PC-B detecting that echo request has been sent to it, It needs to update it's ARP table, so an extra ARP message is scheduled to update it's ARP



purple envelope

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: PC-B
Source: PC-A
Destination: PC-B

In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0004.9AA7.ADAE >> 0001.438B.98CE
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1 ICMP Message Type: 0
Layer 2:
Layer1

1. The ICMP process replies to the Echo Request by setting ICMP type to Echo Reply.
2. The ICMP process sends an Echo Reply.
3. The destination IP address is in the same subnet. The device sets the next-hop to destination.

• green envelope

OSI Model

Outbound PDU Details

At Device: PC-B
Source: PC-B
Destination: Broadcast

In Layers

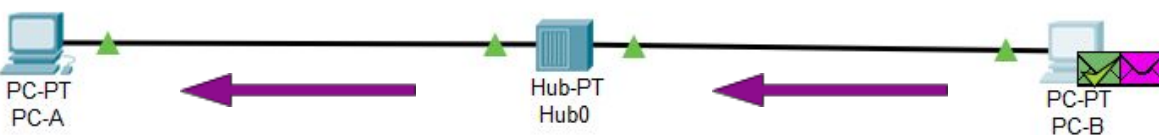
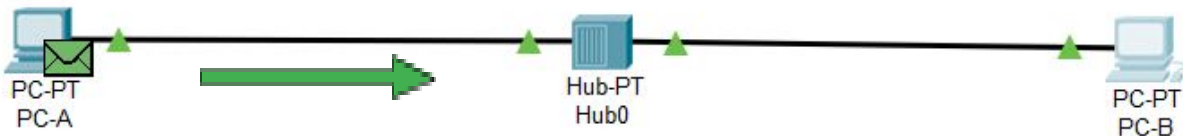
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

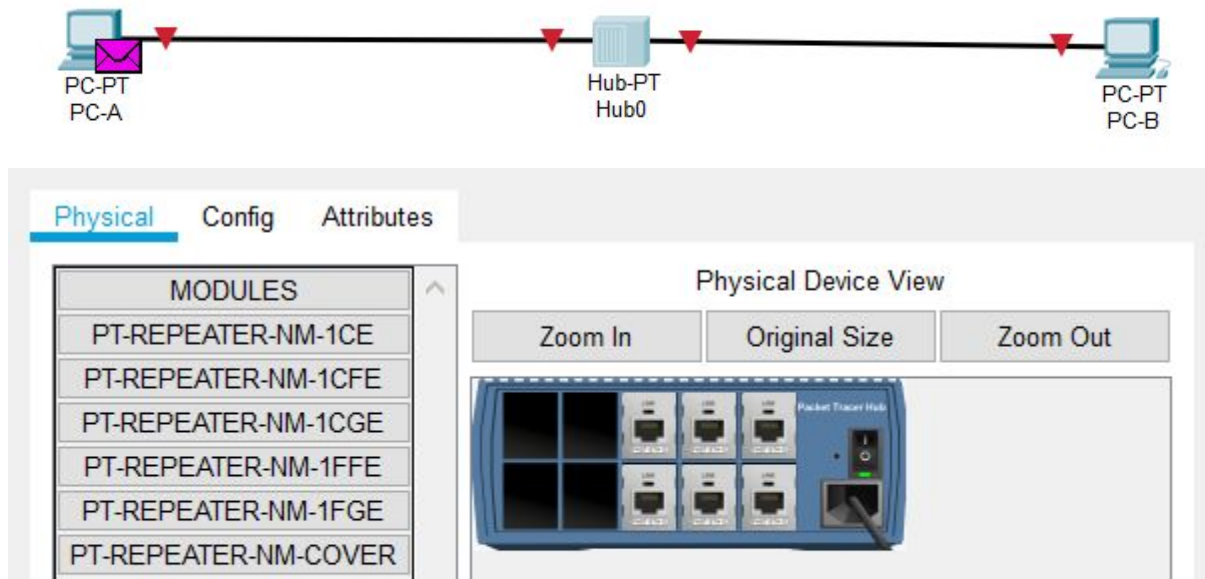
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0001.438B.98CE >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.2, Dest. IP: 192.168.1.1
Layer 1: Port(s): FastEthernet0

1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.

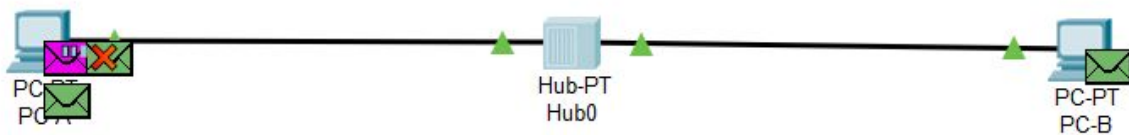
- The broadcast reaches PC-A, and it acknowledges by sending a response ARP message. PC-B updates it's ARP to the response sent by PC-A, and completes the ICMP echo by sending a response echo back to PC-A, using the entry for MAC in it's newly created ARP table.



3. PC-A and PC-B have full ARP tables, but Hub switches off by accident



- The picture above shows how to simulate such a scenario and also how the network looks when we switch off the hub.
- After starting the hub, we note that there are 3 envelopes in the PC-A side and one on the PC-B side.



Green striked envelope

At Device: PC-A
Source: PC-A
Destination: Broadcast

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2
Layer1

1. The sending port is down or it does not have an IP address.

- It rightly informs that the hub was down and the request sent by ICMP, was not met, as when checking in the ARP table, to send to PC-B, it discovered that the sending port is down and has no ARP entries anymore.
- To resolve the conflict in the table, it sends a Gratuitous ARP request to itself to resolve the ARP conflict

At Device: PC-A
Source: PC-A
Destination: GRATUITOUS ARP

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

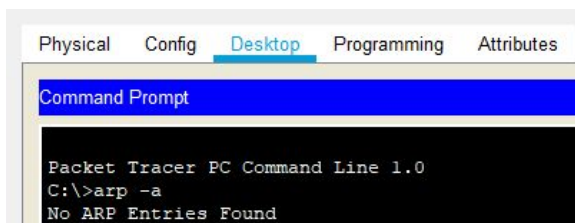
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0004.9AA7.ADAE >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.1, Dest. IP: 192.168.1.1
Layer 1: Port(s): FastEthernet0

1. The ARP frame is a gratuitous ARP Request to fix the LAN hosts' ARP cache due to a duplicate IP address conflict.
2. The device encapsulates the PDU into an Ethernet frame.

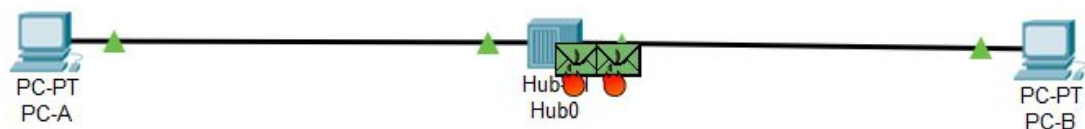
- PC-B also sends a Gratuitous ARP, to resolve the IP address conflict. Hence both broadcast ARP messages at the same time

At Device: PC-B Source: PC-B Destination: GRATUITOUS ARP	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 0001.438B.98CE >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.2, Dest. IP: 192.168.1.2
Layer1	Layer 1: Port(s): FastEthernet0

1. The ARP frame is a gratuitous ARP Request to fix the LAN hosts' ARP cache due to a duplicate IP address conflict.
2. The device encapsulates the PDU into an Ethernet frame.



- We see the above terminal for both the PC's



- We see that since in the simulation, both requests are sent simultaneously, they collide at the hub, and that the PC's receive collided frames which are then removed

At Device: Hub0
Source: PC-A
Destination: GRATUITOUS ARP

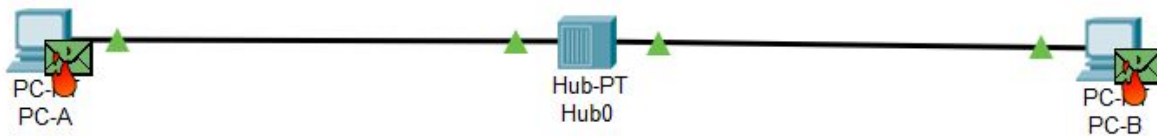
In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer 1: Port(s): FastEthernet0 FastEthernet2

1. FastEthernet0 receives the frame.
2. This frame collided with another frame at the device.



At Device: PC-A
Source: PC-A
Destination: GRATUITOUS ARP

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

1. FastEthernet0 receives the frame.
2. The port receives a collided frame. The device drops the frame.

- We then resolve the conflict by switching off PC-B and switching on again, which takes us back to the original scenario where both have empty ARP tables, and PC-A sends a fresh ARP message and completes the ICMP echo request, and PC-B responds, and so on...

CONCLUSION:

- We learnt how ICMP and ARP protocols are essential to setting up and debugging network configurations.

- We also learnt about how to resolve frame collision and to troubleshoot a network using ICMP protocol.