hDepartment of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4412: Data Communication and Networking Lab

Name : **Mirza Mohammad Azwad**

Student ID : **200042121**

Section : **BSc in SWE(Group A)**

Semester : **4th Semester**

Academic Year : **2022-23**

Date : **27/01/2023**

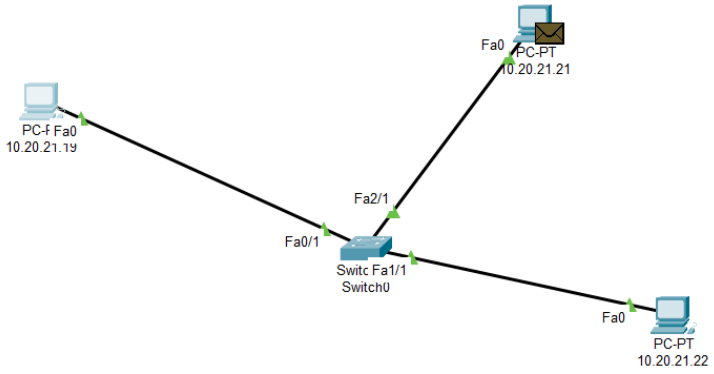
Lab No : **04**

Title: Observation of ARP events and lecture on Logical Addressing.

Objective:

1. Understand how the physical address of a node in the same network is found when the source only knows the logical address.
2. Understand the necessity of hierarchical addressing compared to flat addressing.
3. Understand classful addressing of IPv4 Addressing.
4. Understand the subnet mask.

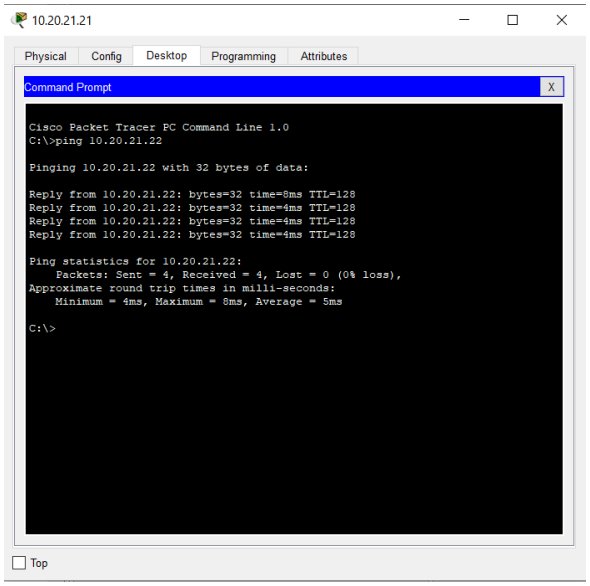
Diagram of the experiment:

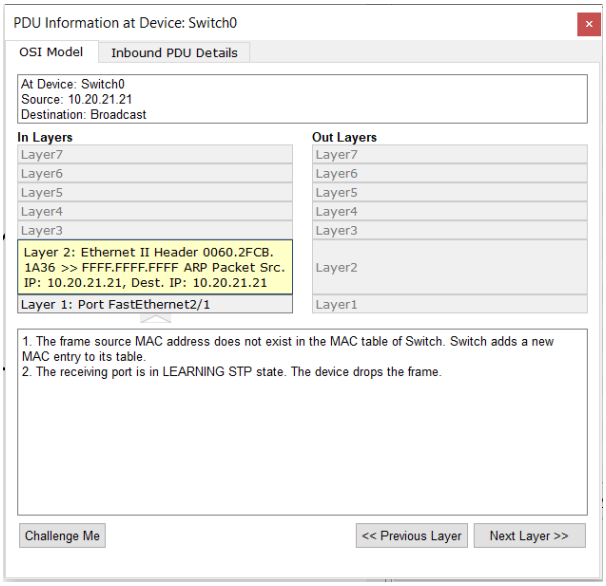


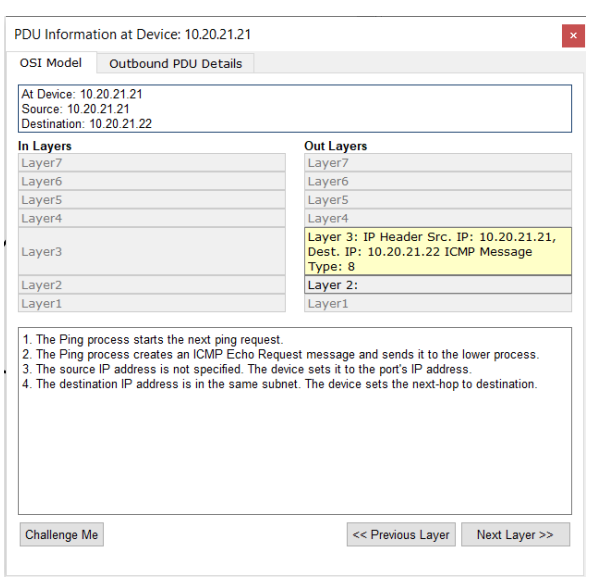
Simulation Panel

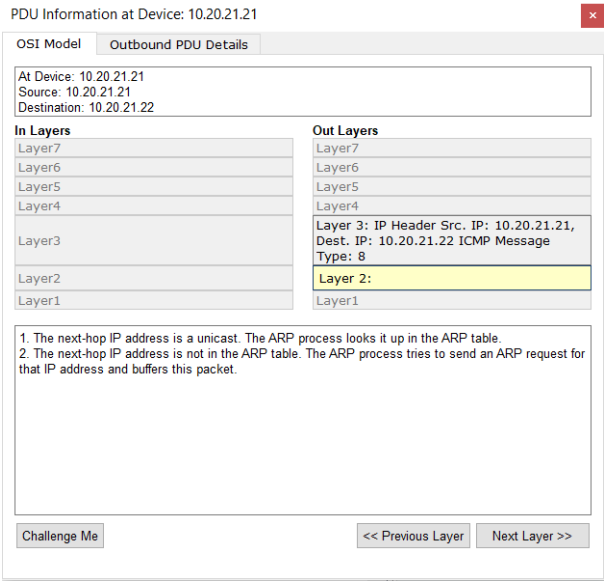
Event List

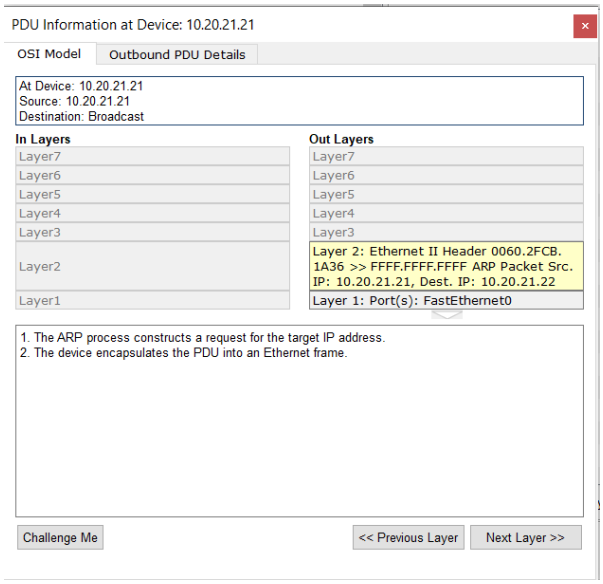
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	10.20.21.21	ARP
	0.001	10.20.21.21	Switch0	ARP
	751.386	--	10.20.21.21	ICMP
	751.386	--	10.20.21.21	ARP
	751.387	10.20.21.21	Switch0	ARP
	751.388	Switch0	10.20.21.19	ARP
	751.388	Switch0	10.20.21.22	ARP
	751.389	10.20.21.22	Switch0	ARP
	751.390	Switch0	10.20.21.21	ARP
	751.390	--	10.20.21.21	ICMP
	751.391	10.20.21.21	Switch0	ICMP
	751.392	Switch0	10.20.21.22	ICMP
	751.393	10.20.21.22	Switch0	ICMP
	751.394	Switch0	10.20.21.21	ICMP
	752.395	--	10.20.21.21	ICMP

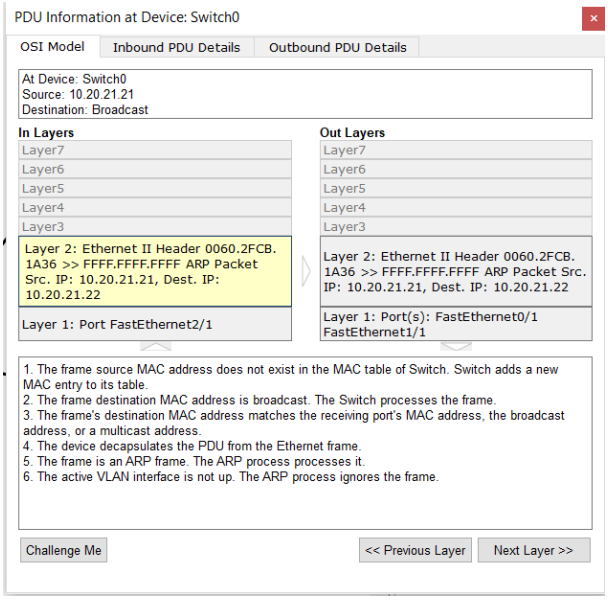

10.20.21.21
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.20.21.22
Pinging 10.20.21.22 with 32 bytes of data:
Reply from 10.20.21.22: bytes=32 time=8ms TTL=128
Reply from 10.20.21.22: bytes=32 time=4ms TTL=128
Reply from 10.20.21.22: bytes=32 time=4ms TTL=128
Reply from 10.20.21.22: bytes=32 time=4ms TTL=128
Ping statistics for 10.20.21.22:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 8ms, Average = 5ms
C:\>
Top

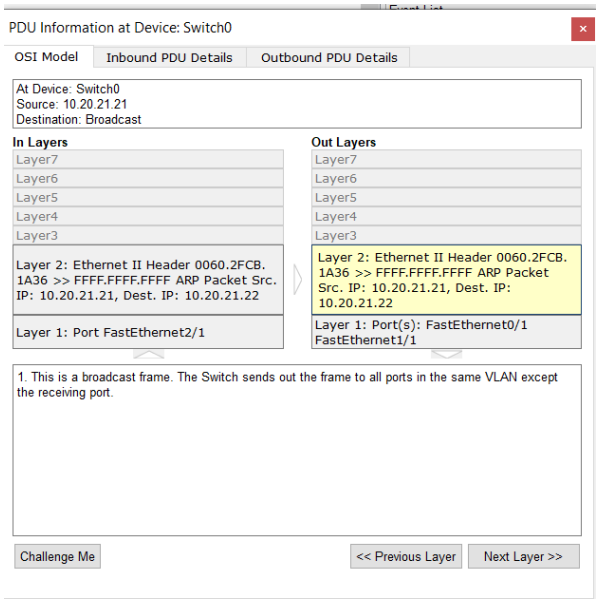

PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
At Device: Switch0
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.21
Layer2
Layer 1: Port FastEthernet2/1
Layer1
1. The frame source MAC address does not exist in the MAC table of Switch. Switch adds a new MAC entry to its table.
2. The receiving port is in LEARNING STP state. The device drops the frame.
Challenge Me
<< Previous Layer
Next Layer >>

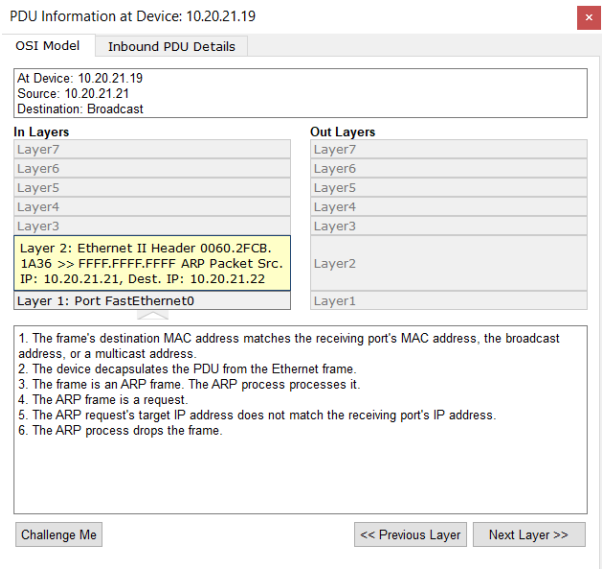

PDU Information at Device: 10.20.21.21
OSI Model
Outbound PDU Details
At Device: 10.20.21.21
Source: 10.20.21.21
Destination: 10.20.21.22
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 3: IP Header Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22 ICMP Message Type: 8
Layer2
Layer 2:
Layer1
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 destination IP address is in the same subnet. The device sets the next-hop to destination.
Challenge Me
<< Previous Layer
Next Layer >>

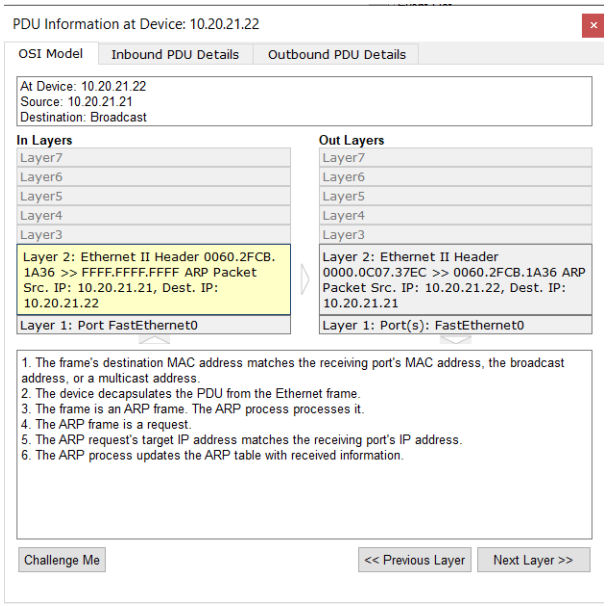

PDU Information at Device: 10.20.21.21
OSI Model
Outbound PDU Details
At Device: 10.20.21.21
Source: 10.20.21.21
Destination: 10.20.21.22
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 3: IP Header Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22 ICMP Message Type: 8
Layer2
Layer 2:
Layer1
1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is not in the ARP table. The ARP process tries to send an ARP request for that IP address and buffers this packet.
Challenge Me
<< Previous Layer
Next Layer >>

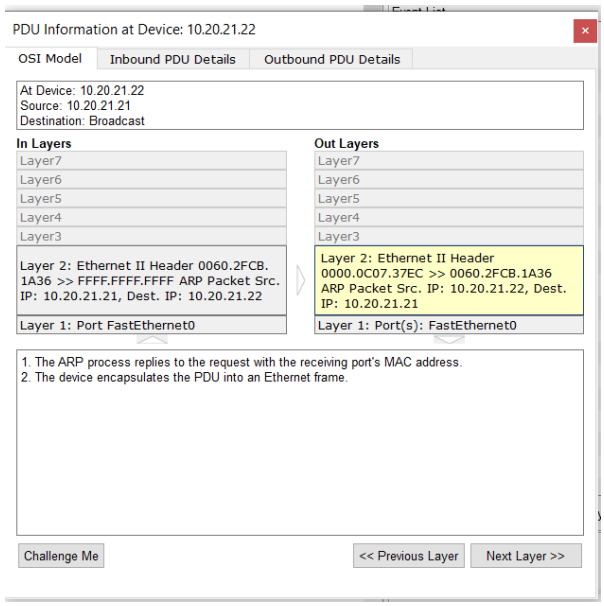

PDU Information at Device: 10.20.21.21
OSI Model
Outbound PDU Details
At Device: 10.20.21.21
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
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.
Challenge Me
<< Previous Layer
Next Layer >>

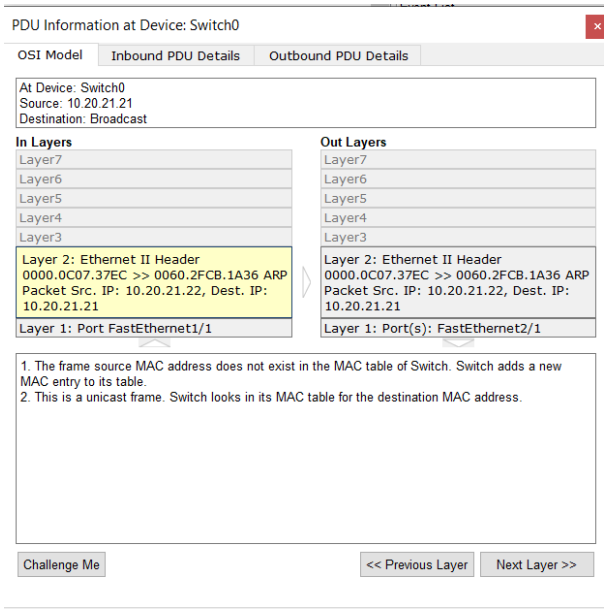

PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Switch0
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 1: Port FastEthernet2/1
Layer 1: Port(s): FastEthernet0/1 FastEthernet1/1
1. The frame source MAC address does not exist in the MAC table of Switch. Switch adds a new MAC entry to its table.
2. The frame destination MAC address is broadcast. The Switch processes the frame.
3. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
4. The device decapsulates the PDU from the Ethernet frame.
5. The frame is an ARP frame. The ARP process processes it.
6. The active VLAN interface is not up. The ARP process ignores the frame.
Challenge Me
<< Previous Layer
Next Layer >>

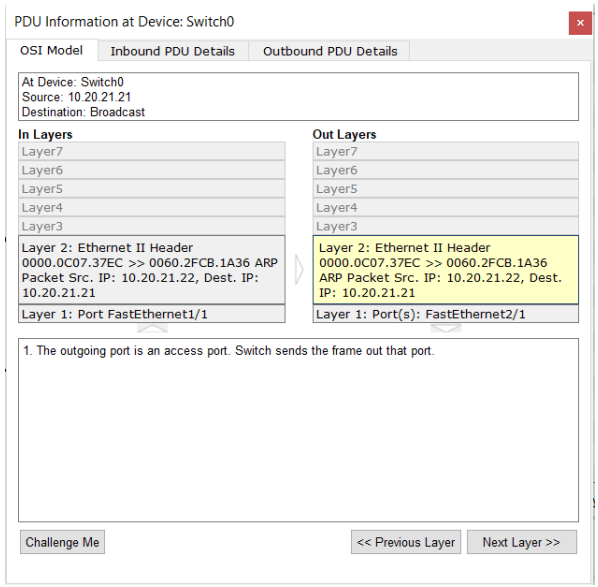

PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Switch0
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 1: Port FastEthernet2/1
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 1: Port(s): FastEthernet0/1 FastEthernet1/1
1. This is a broadcast frame. The Switch sends out the frame to all ports in the same VLAN except the receiving port.
Challenge Me
<< Previous Layer
Next Layer >>

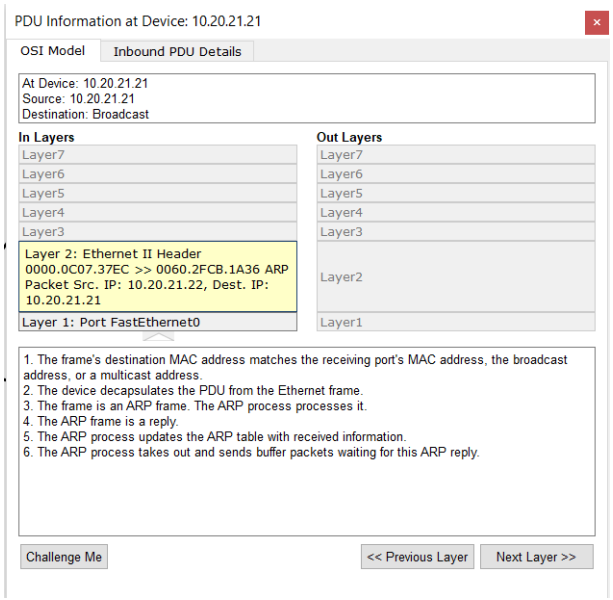

PDU Information at Device: 10.20.21.19
OSI Model
Inbound PDU Details
At Device: 10.20.21.19
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
Layer 2: Ethernet II Header 0060.2FCB. 1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 1: Port FastEthernet0
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a request.
5. The ARP request's target IP address does not match the receiving port's IP address.
6. The ARP process drops the frame.
Challenge Me
<< Previous Layer
Next Layer >>

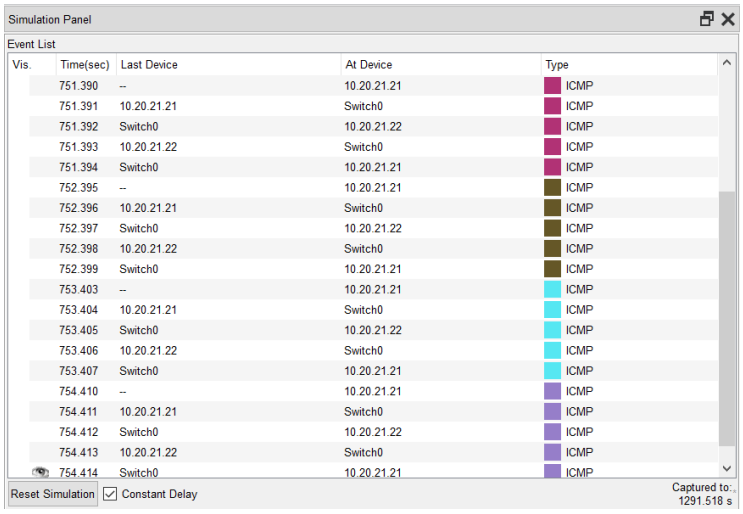

PDU Information at Device: 10.20.21.22
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: 10.20.21.22
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.2FCB.1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 1: Port FastEthernet0
Layer 1: Port(s): FastEthernet0
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a request.
5. The ARP request's target IP address matches the receiving port's IP address.
6. The ARP process updates the ARP table with received information.
Challenge Me
<< Previous Layer
Next Layer >>

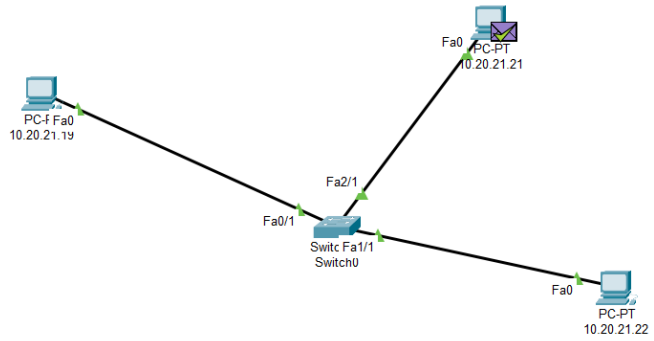

PDU Information at Device: 10.20.21.22
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: 10.20.21.22
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0060.2FCB.1A36 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 10.20.21.21, Dest. IP: 10.20.21.22
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 1: Port FastEthernet0
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.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Switch0
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 1: Port FastEthernet1/1
Layer 1: Port(s): FastEthernet2/1
1. The frame source MAC address does not exist in the MAC table of Switch. Switch adds a new MAC entry to its table.
2. This is a unicast frame. Switch looks in its MAC table for the destination MAC address.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: Switch0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Switch0
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 1: Port FastEthernet1/1
Layer 1: Port(s): FastEthernet2/1
1. The outgoing port is an access port. Switch sends the frame out that port.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: 10.20.21.21
OSI Model
Inbound PDU Details
At Device: 10.20.21.21
Source: 10.20.21.21
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0000.0C07.37EC >> 0060.2FCB.1A36 ARP Packet Src. IP: 10.20.21.22, Dest. IP: 10.20.21.21
Layer 1: Port FastEthernet0
Layer2
Layer1
1. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.
2. The device decapsulates the PDU from the Ethernet frame.
3. The frame is an ARP frame. The ARP process processes it.
4. The ARP frame is a reply.
5. The ARP process updates the ARP table with received information.
6. The ARP process takes out and sends buffer packets waiting for this ARP reply.
Challenge Me
<< Previous Layer
Next Layer >>


Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type
751.390 -- 10.20.21.21 ICMP
751.391 10.20.21.21 Switch0 ICMP
751.392 Switch0 10.20.21.22 ICMP
751.393 10.20.21.22 Switch0 ICMP
751.394 Switch0 10.20.21.21 ICMP
752.395 -- 10.20.21.21 ICMP
752.396 10.20.21.21 Switch0 ICMP
752.397 Switch0 10.20.21.22 ICMP
752.398 10.20.21.22 Switch0 ICMP
752.399 Switch0 10.20.21.21 ICMP
753.403 -- 10.20.21.21 ICMP
753.404 10.20.21.21 Switch0 ICMP
753.405 Switch0 10.20.21.22 ICMP
753.406 10.20.21.22 Switch0 ICMP
753.407 Switch0 10.20.21.21 ICMP
754.410 -- 10.20.21.21 ICMP
754.411 10.20.21.21 Switch0 ICMP
754.412 Switch0 10.20.21.22 ICMP
754.413 10.20.21.22 Switch0 ICMP
754.414 Switch0 10.20.21.21 ICMP
Reset Simulation
Constant Delay
Captured to: 1291.518 s


Fa0
PC-PT
10.20.21.21
PC-F Fa0
10.20.21.19
Fa2/1
Fa0/1
Switc Fa1/1
Switch0
Fa0
PC-PT
10.20.21.22

Experiment Set-Up Description:

The setup approach was 3 computed with static IP addresses 10.20.21.19 to 10.20.21.22 with a PT-Switch(Default switch in cisco pkm) connected between them with straight-through wiring. In the simulation mode, we filtered out the event list to only observe the ARP and ICMP events. We also observed the PDU details of every ARP event but for ICMP events I only showed the main event list image. To dispatch packets from one PC to another, I made use of the ping command.

Observation:

The first key observation was about how ARP events tend to work. We observed that initially besides just one ICMP event. All of the events are ARP events. ARP stands for Address Resolution Protocol. When a switch or router is first configured to a network with devices connected to it. It does not have the ARP table, a table that maps every IP address of the connected devices to the respective MAC addresses. This is to ensure that the packet reaches the destination it was meant for instead of other devices via the intelligent packet-switching technology provided by switches and routers. This routing mechanism is ensured via the ARP table which knows in which path the packet is to be dispatched. The first set of ARP events showed that when the table is not known, the switch or router tends to flood all the connections in an effort to identify and store their MAC address. The action of flooding is similar to that performed for hubs. The first ICMP event is just a response to the ping command, which I would mention in detail afterward.

Initially, the event suggests that the next hop IP address is unicast and is supposed to be directed to the PC with IP address 10.20.21.22 but unfortunately that IP address is not stored in the ARP table. Note that all ARP events are in reality layer 2 events or take place in the data link layer whereas ICMP events are layer 3 events that have their inception in the network layer. Since the IP address was not found it floods the connection including the sender. This process leads to the ARP table recognizing and adding new IP addresses and MAC addresses. Every time a MAC address is not found for a particular IP address, it follows this procedure of flooding the connections. This flooding of connections to all devices is typically known as broadcast. This is broadcasted to every single device. In each packet dispatch, as soon as a PC receives the packet, its IP address and MAC address are configured into the ARP table of the switch or router. Upon the ARP table is configured with all the respective connections. The next hop IP address can be unicast with the ARP table being configured allowing successful delivery of the packets.

Now comes the idea of ICMP or in other words Internet Control Message Protocol. The Ping process is used to check the connectivity between two devices on a network. It starts by sending a request for a connection test. This request is in the form of an ICMP Echo Request message. This message is sent to the lower layer for transmission. When sending this message, the source IP address is not specified, instead, the device uses the IP address that is assigned to the port

from which the request is being sent. When the destination IP address is in the same subnet, the device sets the next hop as the destination address and sends the message. This helps in verifying the communication between the two devices and if there are any issues, it helps in identifying and troubleshooting them. ICMP (Internet Control Message Protocol) is a network protocol used to send error messages and operational information about network conditions. It is typically used to troubleshoot network issues and can be used to test the reachability of a host on an Internet Protocol (IP) network. In Cisco Packet Tracer, there are 4 sets of ICMP events with different packets, these are

Echo Request: The ping command sends an Echo Request packet to a host to check for its reachability and to measure the round-trip time it takes for the packet to be sent and received by the host.
Echo Reply: The host sends an Echo Reply packet back to the source of the Echo Request packet in response to it.
Time Exceeded: This event is triggered when the time-to-live (TTL) value of a packet drops to zero while it is traversing the network. The router generates an ICMP Time Exceeded message and sends it back to the source.
Destination Unreachable: This event is triggered when a packet is unable to reach its destination. The router generates an ICMP Destination Unreachable message and sends it back to the source.
These different packets help in identifying the different error messages and conditions that may occur while transmitting data over a network.
In the simulation of the experiment discussed above, we observe that the ICMP events represent 4 different packets because ICMP is used for a variety of purposes, such as determining the reachability of a host or network, measuring round-trip time, and determining the maximum transmission unit (MTU) of a path. Each of these purposes requires a different type of ICMP packet to be sent.

For example, the ICMP Echo Request packet is used to test the reachability of a host and the ICMP Echo Reply packet is sent in response to an Echo Request packet. The ICMP Time Exceeded packet is used to indicate that a datagram has exceeded the time allowed for it to traverse a particular network, and the ICMP Destination Unreachable packet is used to indicate that the destination is unreachable for some reason.

Therefore, in Cisco Packet Tracer, we can filter out 4 different types of ICMP events, each representing a different packet with specific information. This allows us to better understand and analyze the network conditions and troubleshoot any issues that may arise.

Lastly in this lab, we also learned about how the ARP is reconfigured and what happens when the MAC address remains the same and the IP address changes for a device. We used the arp -a command to show all arp table information in the command prompt and arp -d to delete the ARP

table in the device. Upon deleting a new observation suggests that the entire broadcasting to find the IP address MAC address key-value pairs starts all over again. The objective of this experiment was to understand how the physical address of a node in the same network is found when the source only knows the logical address. The logical address mentioned is in this case the IP address while the physical address mentioned in this case is the MAC address. The physical address remains unique to a device and is not changed. Typically, this address is unique to every particular NIC(Network Interface Card). Upon further inspection, the MAC address can be seen as a 48-bit number, typically written via the use of hexadecimal. More discussion regarding the IP address is present in the answers section.

Challenges:

The most challenging aspect of the experiment was observing the event list, as my cisco packet tracer kept showing the event buffer list full and I had to clear the event buffer multiple times. Secondly, initially, the concept of broadcasting was a bit hard to grasp. I could not follow the lab to completion the last time although I tried my level best to cram through the notes before performing the experiments at home but I realized that not all aspect of the class was retained although I tried my best to mention all that I could remember.

Answer the Following Questions

1. What are flat addressing and hierarchical addressing? Why is IPv4 address hierarchical addressing?
2. What are the ranges of IP addresses in classes A, B, and C.
3. What is a subnet mask? How to determine a network's network address and broadcast address from an IP address and subnet mask? What is the default subnet mask of class A, B, and C networks?

What are flat addressing and hierarchical addressing? Why is IPv4 address hierarchical addressing?

Flat addressing and Hierarchical addressing are two ways of organizing network addresses. Flat addressing assigns unique addresses to all devices on a network without any structure or hierarchy, making it difficult to manage large networks. On the other hand, Hierarchical addressing organizes addresses in a hierarchical structure, where different levels of the hierarchy represent different levels of the network. This makes it easy to group and organize addresses based on their location in the network hierarchy, thus making it more manageable for large networks.

IPv4 addresses are an example of hierarchical addressing, where the 32-bit binary number is divided into four octets (or 8-bit groups) with the first octet identifying the network and the remaining three octets identifying the host. This structure allows for easy organization and management of large networks.

What are the ranges of IP addresses in classes A, B, and C? What is a subnet mask? How to determine a network's network address and broadcast address from an IP address and subnet mask? What is the default subnet mask of class A, B, and C networks?

In **class A**, IP address, the first bit of the first byte/octet will start with 0 so the network ID for the IP addresses will between 0 to 127 → 128 addresses for network ID with subnet mask 255.0.0.0 as the default subnet mask. Except for the first octet, the rest are ignored, allowing up to 2^{24} hosts.

In **class B**, the IP address of the first 2 bits will be 10 so the network ID for the IP addresses will be between 128 to 191 → 64 addresses for network ID with subnet mask 255.255.0.0 as the default subnet mask. Except for the first 2 octets, the rest are ignored, allowing up to 2^{16} hosts.

In **class C**, the IP address of the first 3 bits will be 110 so the network ID for the IP addresses will be between 192 to 223 → 32 addresses for the network ID with the default subnet mask as 255.255.255.0. Except for the first 3 octets, the rest are ignored, allowing up to 2^{8} hosts.

A **subnet mask** can uniquely identify devices within the same internal network. A subnet mask is a 32-bit string of numbers used to divide an IP address into two parts: the network address and the host address.

The subnet mask is used to determine which portion of the IP address belongs to the network and which portion potentially belongs to the host essentially the broadcast ID. It allows a network administrator to divide a larger network into smaller subnetworks, which can improve network security and organization. IP addresses and subnet masks are usually provided as the header for network layer packets that help regulate how the data in the packets are to be transmitted. I mentioned the default subnet mask when discussing class A, B and C addresses earlier. The idea of determining the network ID and the broadcast address is quite simple by the use of a bitwise AND operation between the subnet mask and the IP address. By bitwise AND with the subnet mask you can uniquely identify the network address. And the remaining values indicate the broadcast address or the potential host identifier. Usually, multiple devices are connected to a switch or a router. Upon determining the network ID. The packets can be routed to that particular switch or router connecting multiple devices as per the network ID obtained by the bitwise AND operation mentioned earlier. After arriving at the switch based on the ARP table of the switch or router, it can be directed to that particular device.