**Tutorial 5: Ethernet**

**Q1.**

1. In a Local Area Network, ARP request is a layer 2 broadcast message. All the devices in the LAN received the Address Resolution Protocol (ARP) request except the sending device.
2. What is the purpose of the ARP? (2 marks)

Purpose of ARP is to let the sending node *(e. g. Switch)* to find the Media Access Control (MAC) address of the destination for a Ethernet link

1. What is the action taken by a node if the node’s IP address matched the IP address in the ARP request? (2 marks)

The node that matches the IP address will respond to the ARP request and reply it’s MAC address

1. What happens if no device on the LAN responds to the ARP request? (2 marks)

If an ARP reply is not received, the packet will drop because the frame cannot be created. The IP address cannot be resolved to an Ethernet address. Without an Ethernet address, the packets cannot be transmitted.

1. Name and explain **ONE (1)** reason ARP can cause a problem in a network. (3 marks)

**ARP Spoofing**

* This can be caused by an attacker injecting the wrong MAC address into the network by issuing faking ARP requests. This cause the frame to send to wrong destination

**Overhead on the media**

* As a broadcast frame, an ARP request is received and processed by every device on the local network. If a large number of devices accessing the network services at the same time, it could cause delay and affect the performance

1. What is the ARP table used for? (4 marks)

* Used for finding the data link layer address that is mapped to the destination IPv4 address
* As a node receives frame from the media, it records the source IP address and MAC address to be mapped into ARP table

(b) Determine the correct sublayer for the following descriptions. (6 marks)

| **Descriptions** | **MAC or LLC?** |
| --- | --- |
| 1. Controls the network interface card through software drivers | **LLC** |
| 1. Works with the upper layers to add application information for delivery of data to higher level protocols | **LLC** |
| 1. Works with hardware to support bandwidth requirements and checks errors in the bits sent and received | **MAC** |
| 1. Controls access to the media through signaling and physical media standards requirements | **MAC** |
| 1. Supports Ethernet technology by using CSMA/CD or CSMA/CA | **MAC** |
| 1. Remain relatively independent of physical equipment | **MAC** |

**Q3**. (a) Inspect the following MAC addresses; is this a proper MAC address? If no, why?

(i) 77:EE:33:AA:DD (2 marks)

* No, MAC address is expressed as 12 hex digits (48 bits/ 6 bytes)
* The given example has only 10 hex digits

(ii) 01-34-45-7U-8B-P9 (2 marks)

* No, **7U** and **P9** were not a valid hexadecimal value

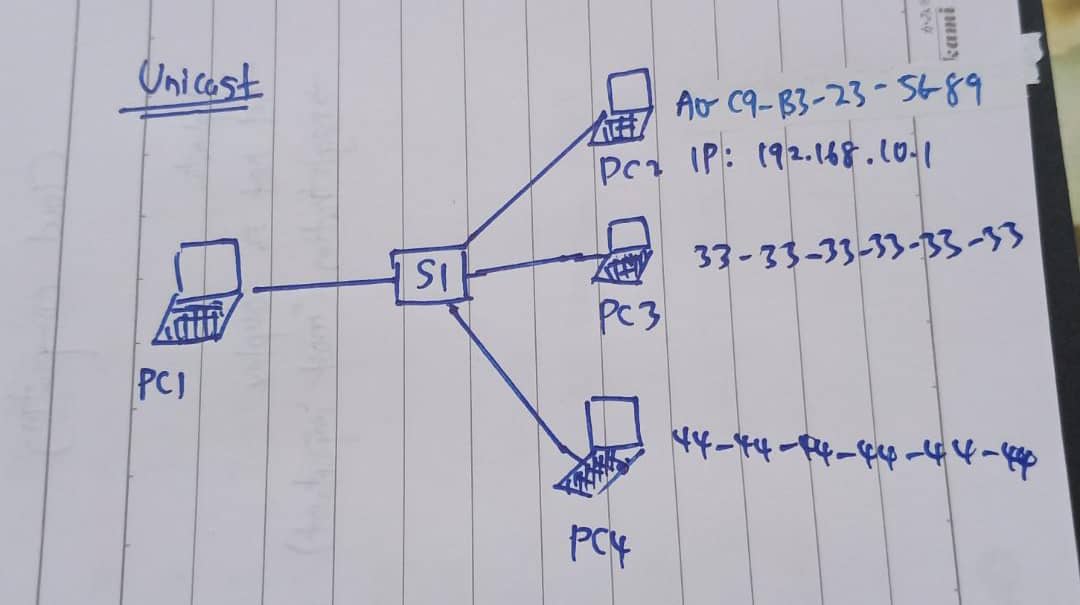
(iii) FI00:5678.910C (2 marks)

* No, MAC address was expressed is in hex format which I is not a valid hexadecimal value
* Besides that, mixture of period and colon is invalid in MAC addresses representation

(b) In Ethernet, different MAC addresses are used for unicast, multicast, and broadcast communications. Give relevant examples **(need to draw !)** of MAC used in unicast, multicast, and broadcast delivery. (6 marks)

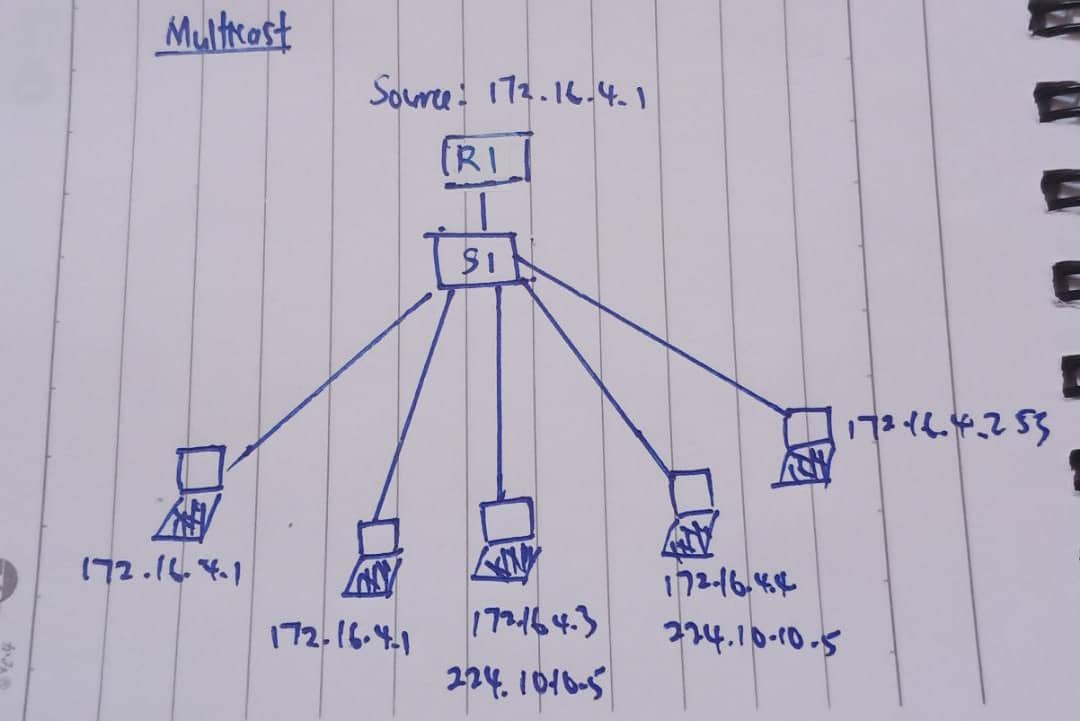
**Unicast**

* Unicast IP and MAC destination addresses will be sent to a specific destination device with a unique MAC address. *E.g. A0-C9-B3-23-56-89*



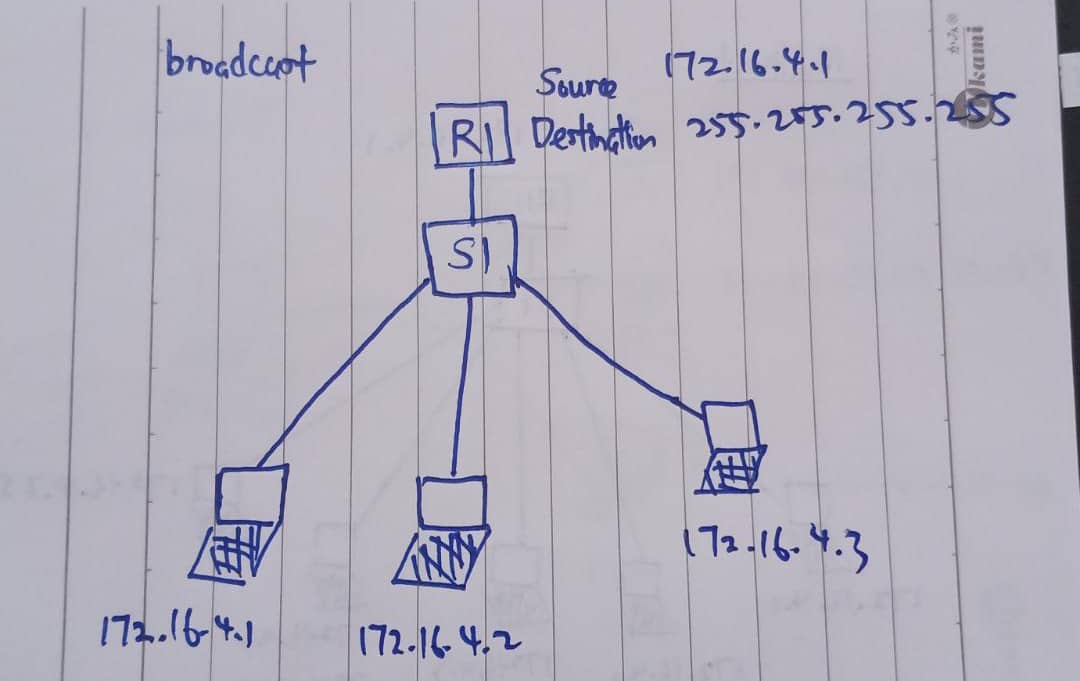
**Multicast**

* + Multicast IP and MAC destination addresses deliver frames to a group of destination devices.
  + Multicast MAC address is a special value that begins with 01-00-5E (*IPv6*) and IP address that range from 224.0.0.0 to 239.255.255.255 (*IPv4*)

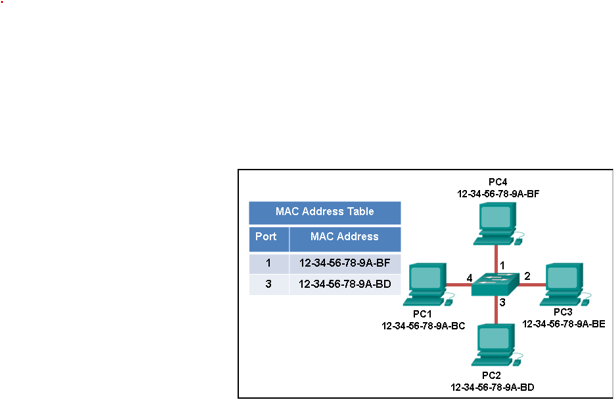


**Broadcast**

* Broadcast IP and MAC destination addresses deliver frames to all destination devices on the network.
* By default, the destination MAC address with value *FF-FF-FF-FF-FF-FF(IPv6)* or 255.255.255.255*(IPv4)* will be the broadcast MAC address.



(c) Refer to the exhibit. The exhibit(展览) shows a small switched network and the contents of the MAC address table of the switch. PC1 has sent a frame addressed to PC3. What will the switch do with the frame? (6 marks)



* The switch will forward the frame to all ports except port 4 (incoming port).
* This is because the MAC address of PC3 is not present in the MAC address table of the switch. The switch does not know where to forward the frame to it.
* Therefore, the switch will forward the frame to all the ports except for port 4 which is the incoming port. This is known as unknown unicast
* The switch will enter the sources MAC address of PC3 (12-34-56-78-9A-BE) and the port number of the switch port number (port2) into the MAC address table
* The switch can now forward frames between source and destination devices without flooding as it has entries in the MAC address table that identify the associated ports.

Answer2:

* Switch receive frame from PC1 on port 4
* The switch enters the source MAC address of PC1 and its port (Port 4) into the MAC Address table as it doesn’t exists in that table
* Next, the switch will forward the frame to all ports except the incoming port which is port 4 as the destination Mac Address of PC3 is not presented in the MAC Address table
* The corresponding destination device which is PC3 will reply to the broadcast with its MAC Address (12-34-56-78-8A-BE) to PC1
* The switch will enter the MAC address of PC3 and its port (Port 2) into the MAC Address table. The destination Mac Address (12-34-56-78-8A-BE) and port (Port 2) of the PC3 is now in the MAC address table.
* The switch now can forward the frame from PC1 to PC3 directly as it has entries in the address table that will identify the associated ports.

**Another situation: PC1 has sent a frame addressed to PC2 (4m)**

* PC1 want to send data to the PC2
* Destination MAC address of PC2 (12-34-56-78-8A-BF) can be found on MAC Address table of the switch
* In this case, the PC1 will directly send the frame to PC2, no ARP request and no ARP reply is required because the destination MAC address can be found on the MAC address table