CO223 : LABORATORY SESSION 3

GAMAGE C.T.N.

E/13/107

GROUP 05

SEMESTER 3

28/03/2016

**Layered Architectures: Addressing, Encapsulation, and Layers Working Together**

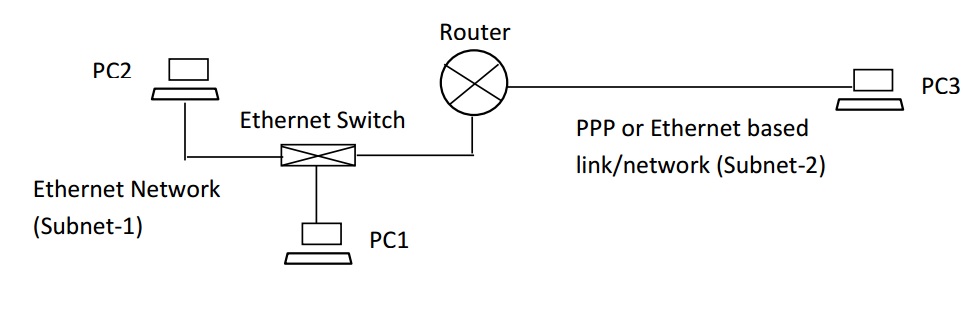
**Part-1: IP addresses and MAC addresses**

IP address

An IP address is an unique address assigned for a computer to differentiate from each other which are using internet protocol to communicate. It is a32 bit number separated by full stops consisting of the network id and the host id.

MAC address

MAC (Media Access Control) address is termed as the physical address also. It is a unique address assigned to network interfaces for communications on the physical network segment. The MAC address is a hardware address which is connected with the Network Interface Card of the machine.

The network setup which we built up in the lab is shown below.****

**a. Assigning IP addresses to Interfaces**

First we decided the IP addresses which can be assigned for the subnet-1 and subnet-2

In this lab session we decided to use 24 bits of the IP address as the network address and the rest 8 bits were allocated for the host ID.

Subnet -1: 200.100.1.0

Subnet-2: 200.100.2.0

Hence the subnet mask of the network we built up is 255.255.255.0

Accordingly the 3 PC’s and the routers interfaces were also assigned with the IP addresses as shown below.

PC1’s interface on subnet-1: 200.100.1.3

PC2’s interface on subnet-1: 200.100.1.2

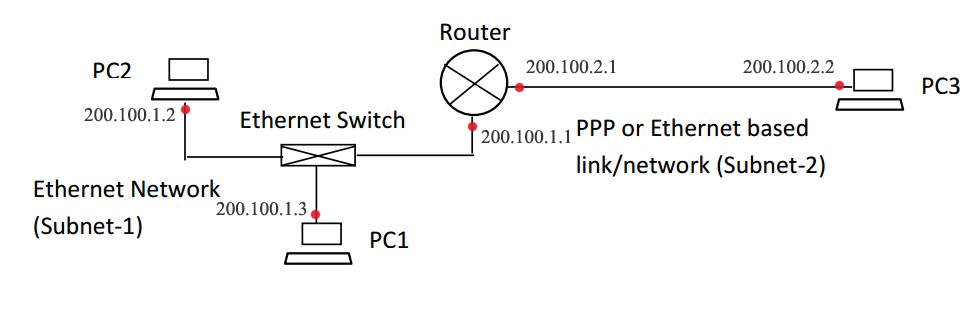
PC3’s interface on subnet-1: 200.100.2.2

Routers interface on subnet-3: 200.100.1.1

Routers interface on subnet-1: 200.100.2.1

When assigning IP addresses the computers were configured from the control panel settings and the router interfaces were configured using the “Tera-term” software installed in the machine which the router’s console is connected (PC 1)

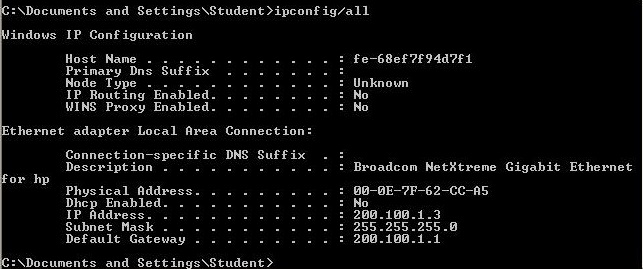
After assigning the devices with these IP addresses we checked whether they all are connected correctly by using the “ping” command. After verifying the connectivity the network be built up is as follows.



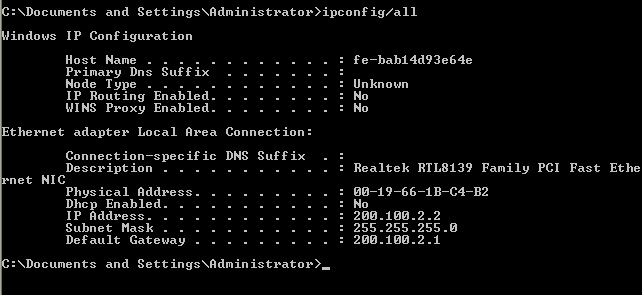
**b. Finding MAC addresses**

To find the MAC address of the machines we used the command “ipconfig/all” was used. The results we obtained from the 3 machines are shown below. The obtained results are as follows.

From PC1

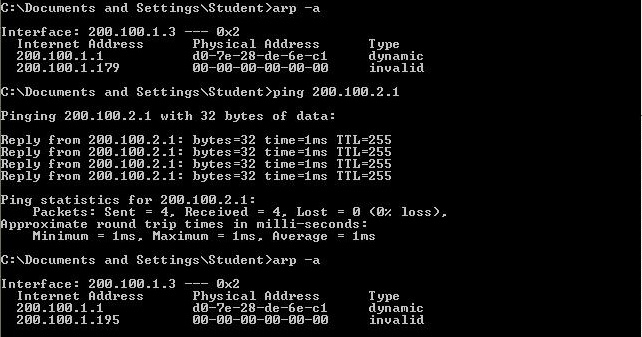


From PC2

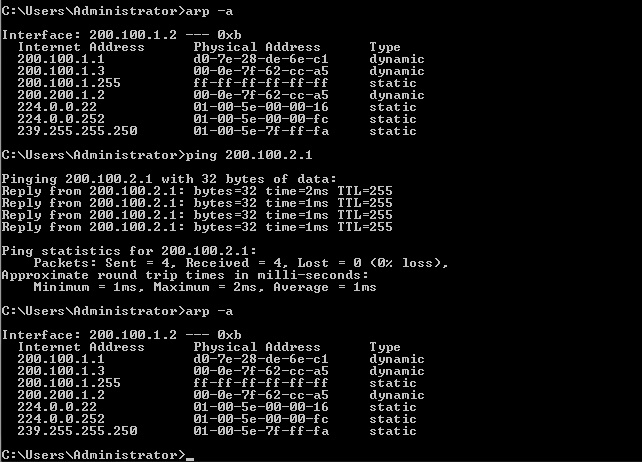
From PC3

The MAC addresses associated with routers are determined using the “arp –a” command. Arp stands for address resolution protocol. It shows a table of data available in the specific machine. Sometimes it might not show the router’s interfaces, in that case we can ping that IP first and then check for “arp –a” . But it didn’t work for the our network. The results obtained are shown below.

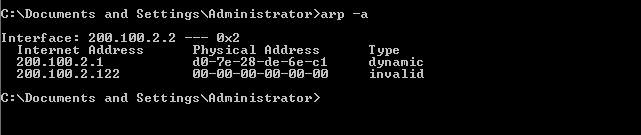
From PC1



From PC2



From PC3



The above results can be summed up as below.

MAC address of PC1 : 00-0E-7F-62-CC-A5

MAC address of PC2 : 00-16-35-66-6A-CB

MAC address of PC3 : 00-19-66-1B-C4-B2

MAC addresses associated with the router :

Subnet-1 : D0-7E-28-DE-6E-C1

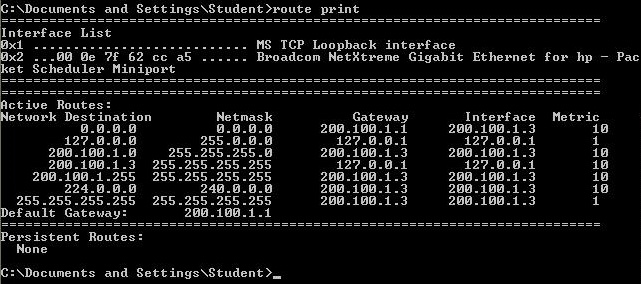
Subnet-2 : D0-7E-28-DE-6E-C1(erroneous)

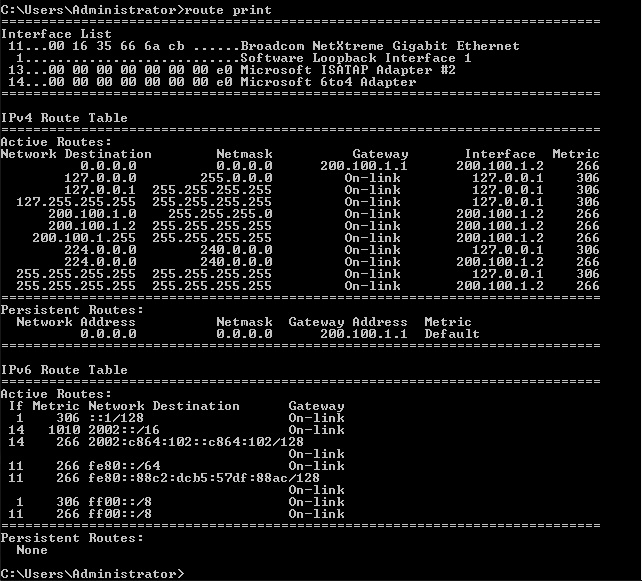
**Part-2: Routing tables (IP tables)**

**a. Routing table of PC1, PC2, PC3**

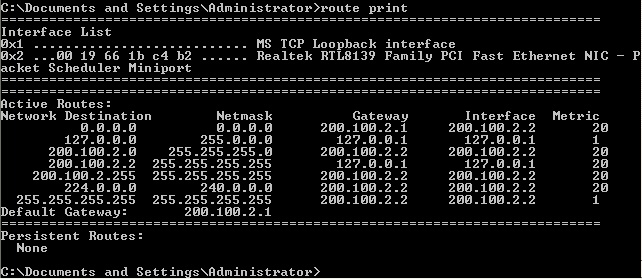
A routing table consists the data of the directly connected networks to the computer.

The routing table of a specific machine can be obtained by the command “route print” . The command tested for the 3PC’s are shown below.

From PC1

From PC2

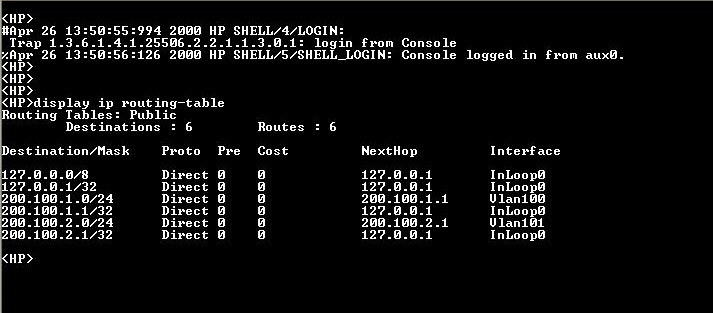
From PC3



From these results we can see that a routing table consists the data of the available destinations; the netmsak , gateway, etic and the interface are prominent among them. It does not show all the possible destinations, but shows the destinations which have learnt from the machine by then. Let’s consider the entries in the routing table one by one.

The “destination” is the destination host, subnet address or network address. A network mask is used to determine the route preciously and the “gateway” is the IP address of the next router where the packet heads to. The “Interface” is the interface that is used to access the next router. The “Metric” is said to be the number of routers to be crossed to reach the destination. Finally the default gateway is shown.

**b. Routing table of the router**

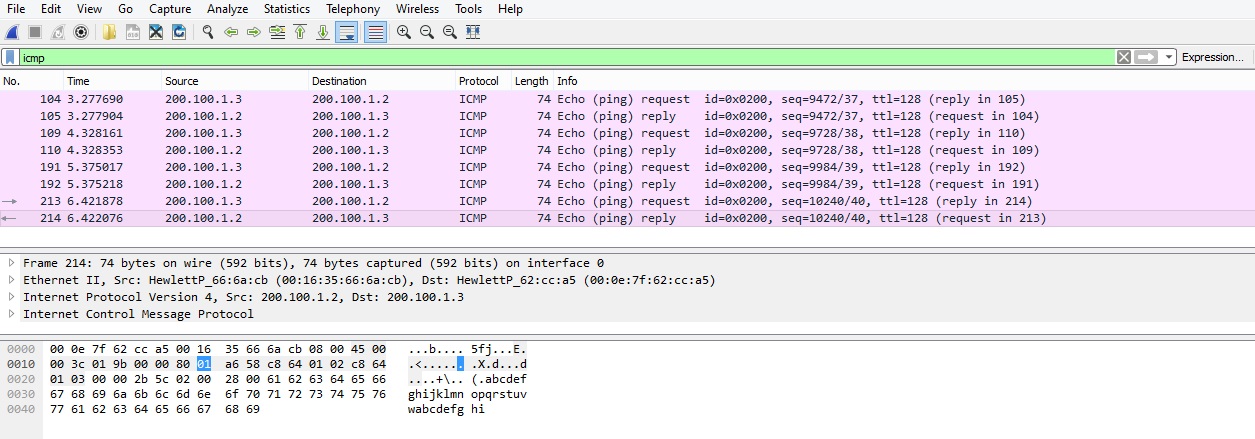
The routing table of the router was obtained by the PC which the console is connected (PC1) using the “Tera-Term” software and thw command “display ip routing-table”.

**Part-3: Encapsulation and the use of routing tables**

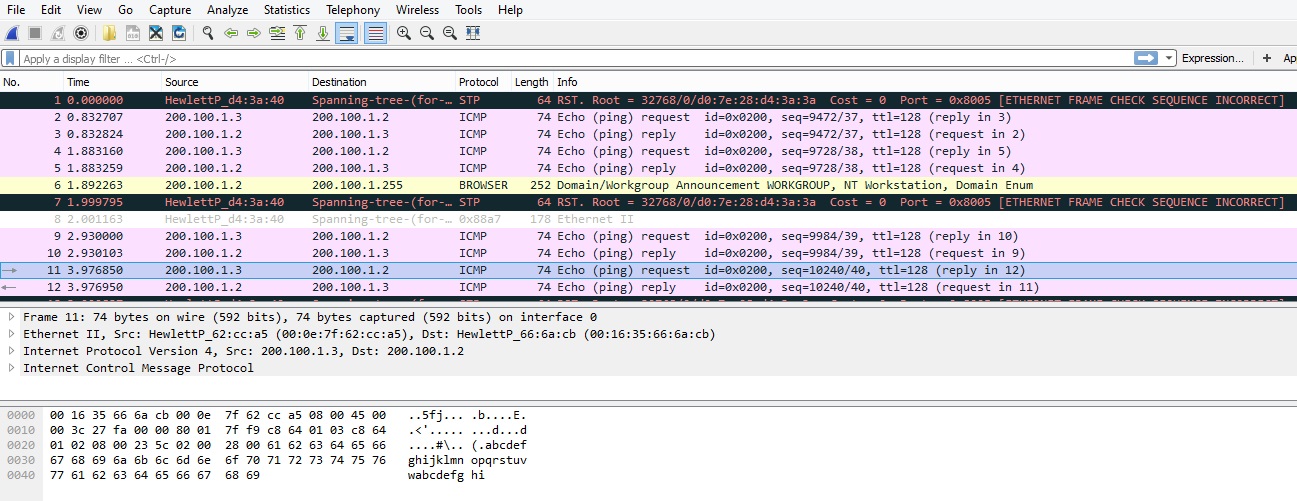
a) Using the ping tool we sent frames from PC1 to PC2. At the same time using the Wireshark network protocol analyzer at PC1 and PC2 we captured the frames sent and received. The saved trace-files are attached below. (Double click to open them)

Filtered results from the Wireshark report obtained by PC1:

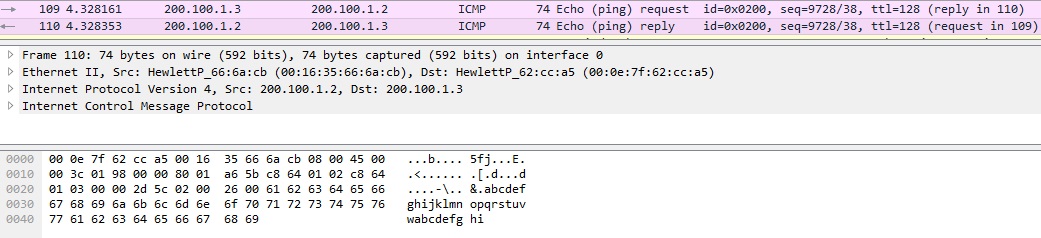


Filtered results from the Wireshark report obtained by PC2:



It is very clear that 4 requests have been sent and 4 replies have been received from each PC. Hence the filtrate gives 8 frames as above. ‘ping’ uses a protocol called the Internet Control Message Protocol (ICMP). Ping makes use of ICMP request and response messages.

Let’s select the 110th frame from the CO223\_Lab3\_3a\_PC1 file. That frame is sent from PC1 to PC2 as a result of the ping command .

Selected frame 110:

b) Let’s consider the selected frame.

In this frame we can see that 40 bytes have been allocated for the Internet control message protocol (ICMP) where the actual data message is stored. The next portion of the packet is allocated for the in the Internet protocol which includes the data about the source and the destination IP addresses. This capsulation is done in the network layer. In this fame this portion is 20 bytes in volume. Next the packet is passed through the data link layer where the packet is encapsulated with the physical addresses which we referred as the MAC address above. The 2 MAC addresses included here are the MAC addresses of PC1 and PC2 respectively which are the source and the destination of the packet. It occupies 14 bytes.

1. a) The data portion of the packet is 40 bytes as discussed above.

2)

The data sending process initiates from through the application layer add UDP headers are added in the transport layer. The Network layer add its IP header which includes the IP addresses of the source and destination. After this encapsulation from the network layer the data is referred to as packets. The protocol used here is specifically referred to as Internet protocol. The IP headers are 20 bytes in volume in the frame we selected. The source IP address is the originating address of the packet which is the PC2 ( 200.100.1.2) and the destination IP is the target’s address which is the IP of PC1 in this case (200.100.1.3) . Here it is interchanged because the selected frame is a reply from PC2. As shown in the filtered results from the Wireshark it confirms our assumptions.

3)

After the packet is formed now it knows the details about the path, then it is directed to the data link layer. When we consider how the packet is directed to the destination it is clear that it is routed accordingly to the data it has. From the PC1 it goes to the Ethernet switch and passes to the PC2. If the destination computer is on a remote network, then the frame is sent to the router or gateway to be routed to the desination. To put this frame on the network, it must be put into a digital signal. Since a frame is really a logical group of 1's and 0's, the Physical layer is responsible for encapsulating these digits into a digital signal which is read by devices on the same local network.

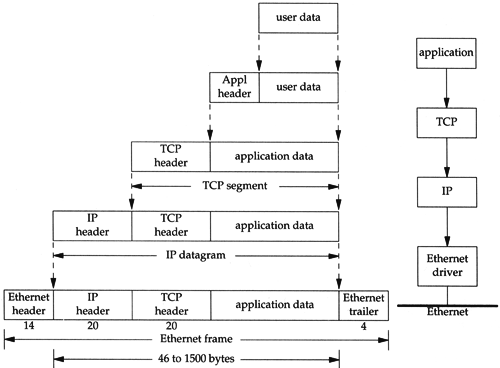
4)

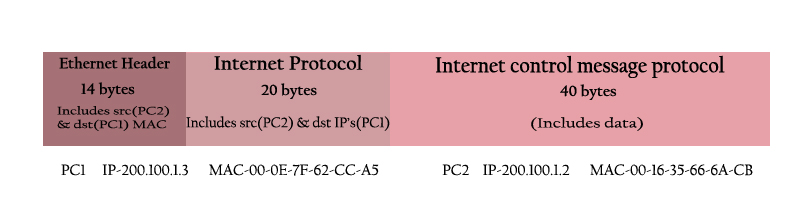
The second encapsulation is the MAC header encapsulation which includes the MAC addresses of origin and destination. The Data link layer is responsible for taking packets from the Network layer and placing them on the network medium. The Data link layer encapsulates each packet in a frame which contains the hardware address of the source and the destination computer. The size of the header files added in this layer are 14 bytes. According to the our scenario since frame 110 is a reply from PC2 the two MAC addresses are PC1’s (00-0E-7F-62-CC-A5) address and PC2’s (00-16-35-66-6A-CB) address which are the destination and the source respectively.

List of control information included in the header fields added by this layer are:

* Start and stop indicator fields - The beginning and end limits of the frame
* Naming or addressing fields
* Type field - The type of PDU contained in the frame
* Quality - control fields
* A data field -The frame payload (Network layer packet)

The above process can be illustrated as below.





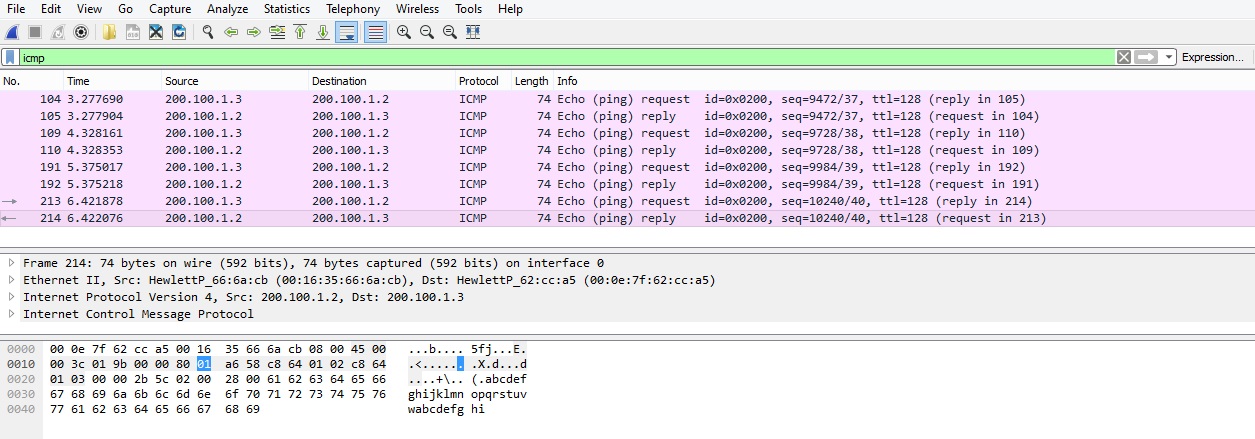
Note: The selected packet is sent from PC2 to PC1.

Frame size= 74 Bytes

Data portion size= 40 Bytes

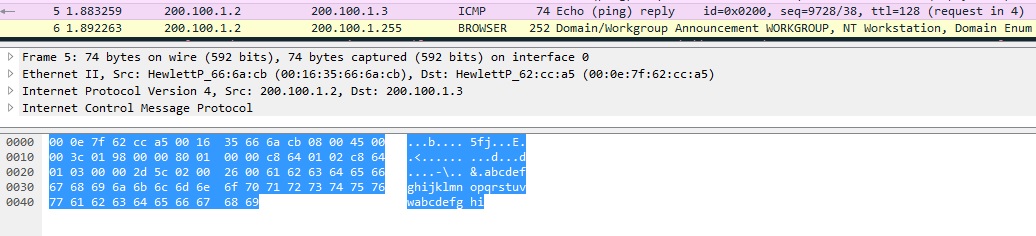
The full control message size to the frame size ratio = 34:74 = 17 : 37

**C) Analyzing the trace-file at PC2 (CO223\_Lab3\_3a\_PC2)**



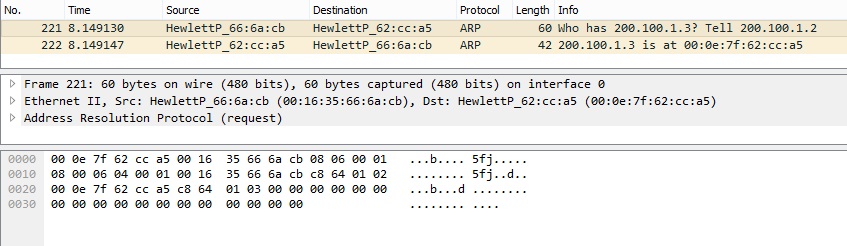
By looking at the above results it is clear that the PC 2 has received and sent corresponding data packets with compared to the PC1’s results.

The corresponding frame we discussed in the PC1 in the PC2 is the frame5



**Homework**

Devices use the MAC address to send frames to other devices on the same subnet. Before two devices can communicate, they must know the MAC address of the receiving device. Hosts use APR (Address Resolution Protocol) to discover the MAC address of a device from its IP address.



To find the MAC address of the destination initially:

First he sending device sends out an ARP broadcast frame (sent packets are shown in the screen shot). The destination MAC address is set to all F's (FFFF: FFFF: FFFF)(The sending MAC address is its own MAC address). The destination IP address is the known IP address of the destination host(The sending IP address is its own IP address)

All hosts on the subnet process the broadcast frame, looking at the destination IP address. If the destination IP address matches its own address, the host responds with a frame that includes its own MAC address as the sending MAC address. 4. The original sender then reads the MAC address from the frame and associates the IP address with the MAC address, saving it in ARP cache.