CS 425: Computer Networks **Jan-Apr 2020**

Lecture 16: Computer Networks – March 3 , 2020

Lecturer: Swaprava Nath *Scribe(s): Abhishek Soni, Aniket Gupta, Naman Gupta, Saurav Prakash*

16.1 Prologue

In the previous lecture, we learned about connecting dissimilar networks via routers, IP addresses, IP prefixes, notation for writing a range of IP addresses, etc. In this lecture, we will wrap up with IP forwarding tables; then we'll learn how a machine is assigned an IP and how it knows the MAC addresses of other machines it wants to communicate with, along with several heuristics used in the process.

16.2 Host routing Tables

- Host sends the traffic to its nearest router and does not participate in routing.
- Routers are dedicated the job for routing the packets

Host forwarding table:

Host forwarding table or host routing table on a particular host yields the forwarding address of the router to be used to reach the desired destination network.

Prefix	**Next**
My_network_prefix	To the device directly
0.0.0.0/0	My_router(default gateway)

The above table conveys that, when the packets are send within the IP range of the network prefix of the host, then the MAC address of the destination is found through the ARP protocol(discussed later), and the packet is sent to that address. The packets which are not within this range are forwarded to the default gateway, which decides the further routing of the packet. A default gateway serves as an access point or IP router that a networked computer uses to send information to a computer in another network or the internet.

route command in linux is used to show the details of kernel routing table entries.

```
~ ❯❯❯ route -n | grep  --color=none "wlp"
0.0.0.0         172.23.23.254   0.0.0.0         UG    600    0        0 wlp62s0
172.23.16.0     0.0.0.0         255.255.248.0   U     600    0        0 wlp62s0
```

Figure 16.1: route command output on linux

Now we will discuss these two major topics for routing:
1) How to get the IP address (DHCP protocol)
2) Mapping of IP address of destination to its link-layer address (ARP protocol)

16.3 Getting IP address

Setup:
1) Device wakes up
2) Gets it's own IP address
3) Tries to find it's nearest Router/Gateway

There are 2 ways for configuring IP Settings:

- **Manual Configuration**:
  Some Network administrator will come and set up the IP, Gateway etc for you. It's outdated and obsolete for large networks, since it may be possible that two systems have the same IP and hence the packets won't be sent correctly.

- **Automatic Configuration**:
  Dynamic Host Configuration Protocol (DHCP) is a protocol responsible for the automatic configuration of machines on a network.

16.3.1 DHCP

DHCP is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. With DHCP, every network must have a DHCP server that is responsible for configuring machines in the network. Following are the functions of DHCP:

- Leases the IP address to the host i.e. you get an IP whenever you connect to the network, and it is freed as soon as you disconnect. Can potentially get different IP every time you connect.

- Provides other important configurations for the network setup, such as:

  - Network Prefix (Netmask)
  - Address of local router (Gateway)
  - DNS server , Time server

16.3.2 DHCP STACK

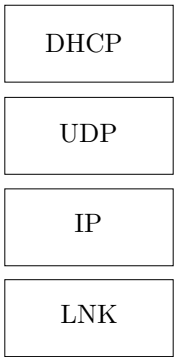

Figure 16.2: DHCP Stack

DHCP basically behaves as a client-server model, where:

- Client is the host requesting an IP address and,
- Server is the machine that assigns the IP address.

UDP Port number 67 is used by the (DHCP) server to receive client requests and port number 68 is used by the client to receive (DHCP) server responses.

16.3.3 DHCP addressing

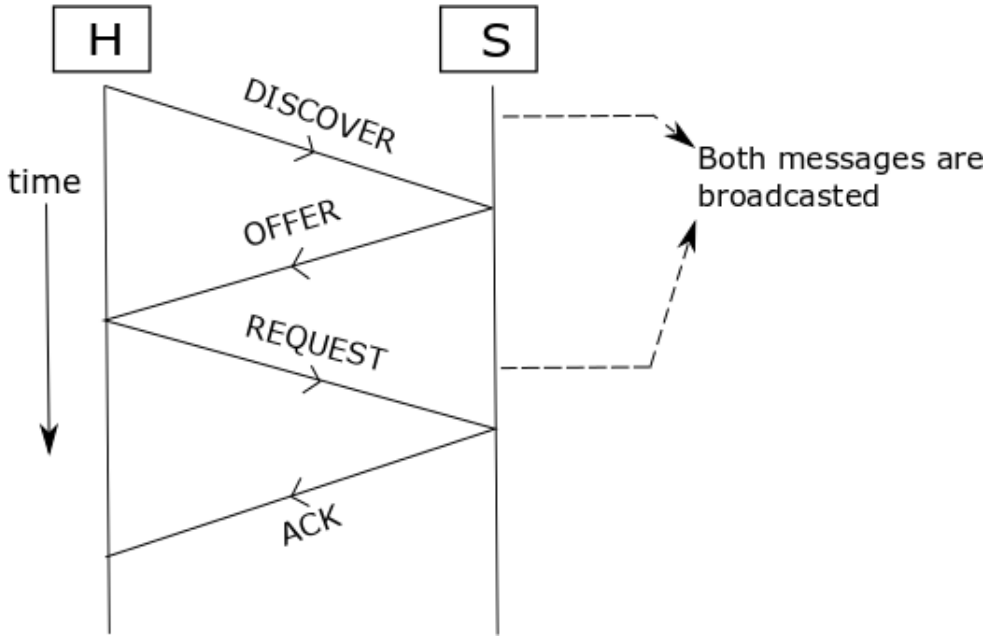

Figure 16.3: DHCP mechanism

DHCP includes four major steps. We will discuss each of them separately:-

- DISCOVER
- OFFER
- REQUEST
- ACK

DISCOVER First the client host broadcasts the DISCOVER message in order to discover if there is any DHCP server present in a network or not. Basically, client asks for an IP address from any available DHCP server.
For broadcasting destination MAC address(server) is FF:FF:FF:FF:FF:FF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting). As the discover message is broadcasted to find out the DHCP servers in the network, therefore, broadcast IP address and MAC address is used.

OFFER The DHCP server sends an available IP address to the client MAC address.

REQUEST In response to DHCP offer client replies with REQUEST to register itself with that IP address. This message is broadcasted because a client may recieve offers from multiple servers, but will accept only one; so all DHCP servers must be notified about which IP address the host has chosen.

ACKNOWLEDGEMENT The DHCP server then sends an ACK which contains a lease time and other configuration settings to the client that it has accepted the request to associate the client's MAC address with the requested configuration. The DHCP server can also send negative acknowledgements in some cases e.g., when the server has no IP address unused or the pool is empty.

RENEW To renew an existing lease of a configuration (which is done periodically), only the last two steps i.e. REQUEST and ACK are performed. The first two are generally not needed.

16.4 Sending an IP packet

A node needs Link layer addresses to send a frame over the local link.

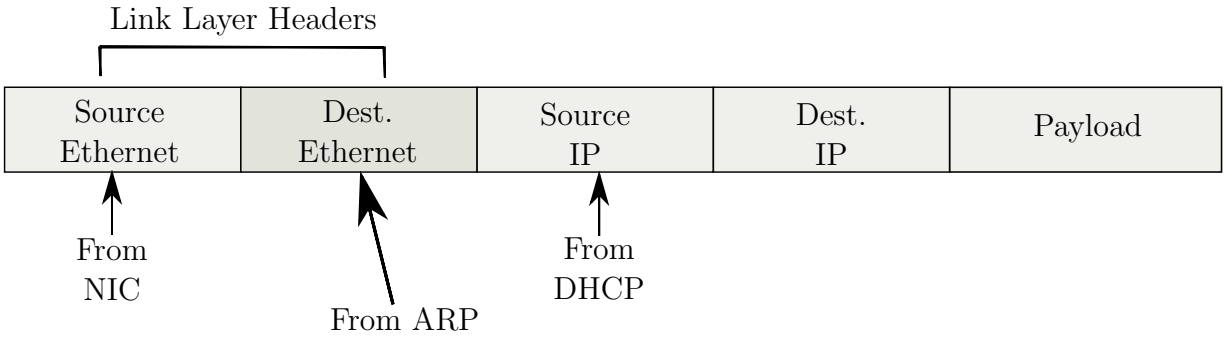

Figure 16.4: LL Frame

The problem here is to find a MAC address given the IP address.

16.4.1 Address Resolution Protocol (ARP)

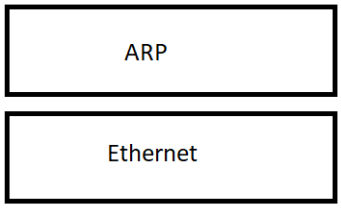

Figure 16.5: ARP-stack

GOAL: Map a local IP address to it's link layer address.

If a machine talks to another machine in the same network, it requires its physical or MAC address. But, since the application has given only the destination's IP address it requires some mechanism to bind the IP address with its MAC address. This is done through Address Resolution protocol (ARP). IP address of the destination node is broadcast and the destination node informs the source of its MAC address.

- ARP sits right above Link layer
- No servers, it just asks the node with the target IP address
- It broadcasts the destination IP address
- Destination replies it with its MAC address
- Source maintains a cache of IP and MAC address bindings

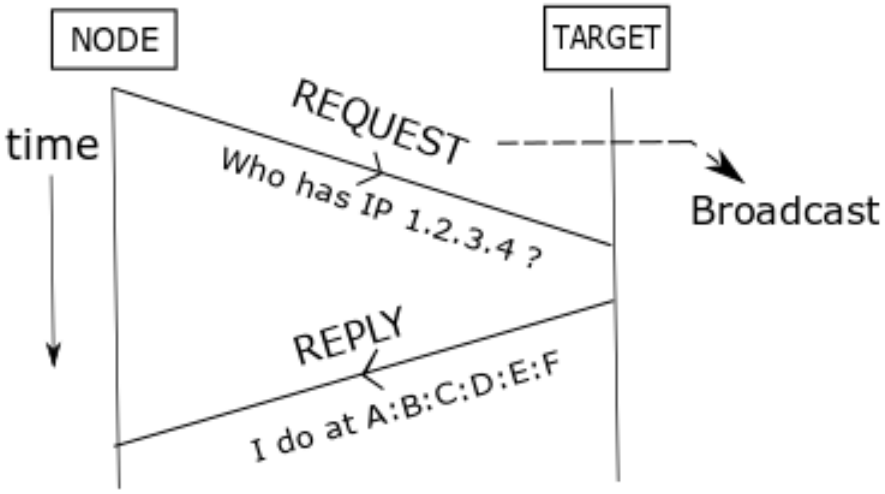

Figure 16.6: Working of ARP

ARP preceedes IP
Request: Who is 1.2.3.4(IP Address) ? (This message is broadcasted)
Reply : I do at A:B:C:D:E:F(MAC Address). (An example reply)

```
~ ❯❯❯ sudo arp-scan -l
Interface: wlp62s0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 2048 hosts (http://www.nta-monitor.com/tools/arp-scan/)
172.23.16.1     00:27:e3:b4:53:50 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.2     f8:66:f2:81:e6:84       CISCO SYSTEMS, INC.
172.23.16.17    30:4b:07:71:12:d4 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.27    4c:18:9a:b7:0f:8c (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.33    b4:c4:fc:b8:1e:aa (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.34    fc:64:ba:1d:9b:e9 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.35    00:23:15:eb:86:33 (c0:64:e4:67:0f:60)   Intel Corporate
172.23.16.43    0c:9d:92:70:0a:61 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.54    d8:63:75:fe:64:7d (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.80    98:3b:8f:b4:70:e4 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.89    d0:c5:d3:d2:e0:c9 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.90    a0:af:bd:da:95:e9 (c0:64:e4:67:0f:60)   (Unknown)
172.23.16.91    b4:c4:fc:71:d7:59 (c0:64:e4:67:0f:60)   (Unknown)
```

Figure 16.7: output arp-scan on linux

The **ARP Scan** Tool (AKA ARP Sweep or MAC Scanner) is a very fast ARP packet scanner that shows every active IPv4 device on your subnet with its corresponding MAC Address.

16.5 Fragmentation

Consider the following networks connected by routers where each network has it's own upper limit on the size of data packet that could be transmitted through it.

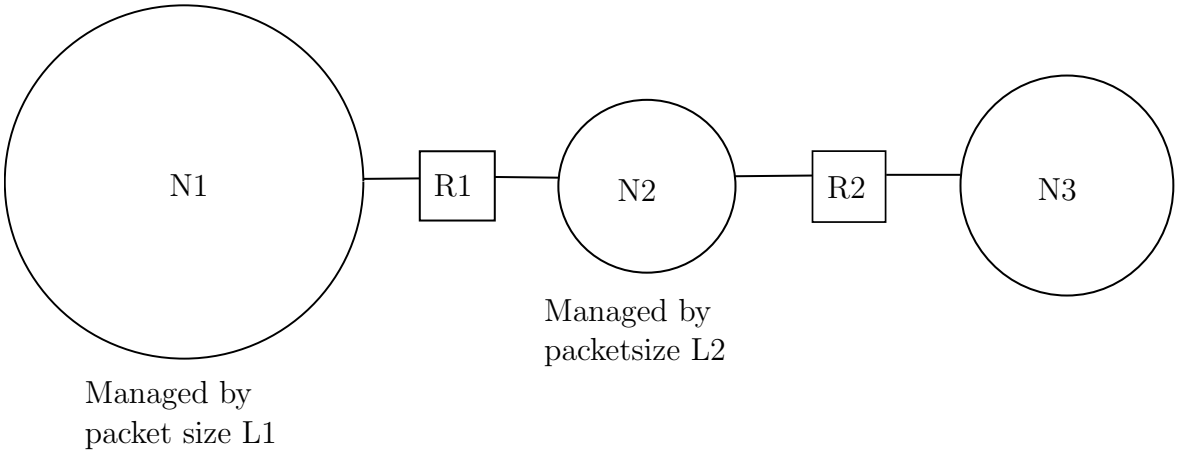

Figure 16.8: Fragmentation (L1 > L2)

A router R cannot forward a packet bigger than the one supported by the next network. Thus we have to fragment a data packet if its size is bigger. Each network has it's own Maximum Transmission Unit (MTU), which is same as this limit.

The MTU for Ethernet is 1500 Bytes and for 802.11(wifi) is 2300 Bytes.

How to solve the problem of different MTU's?

One way network layer accomplishes it is by breaking packets into smaller fragments so that they can pass through a link with a smaller MTU.

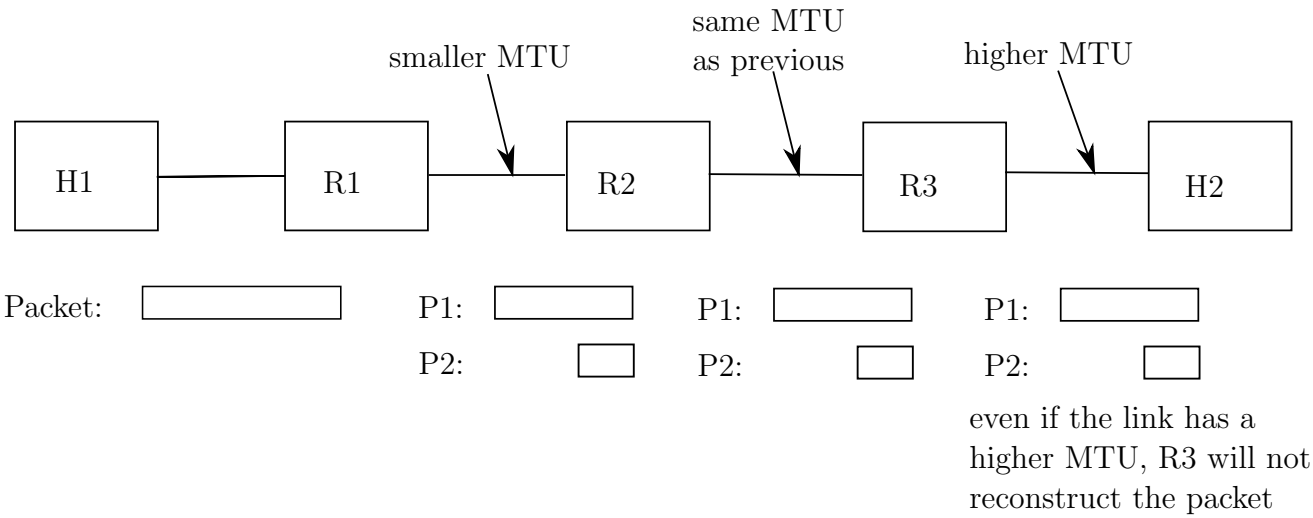

Figure 16.9: Fragmentation of packets by the router

- Packets keep on fragmenting depending upon the next network's MTU.
- Packets are not reconstructed in the routers; it is only done in the last step.
- Host is responsible for the reconstruction of packets.

Version Number (4 bits)	Header Length (4 bits)	Type of Service (8 bits)	Total Length (16 bits)	
ID (16 bits)			Flags (3bits)	Flag Offset (13 bits)
Time To Live (8 bits)		Protocol (8 bits)	Header Checksum (16 bits)	
Source (32 bits)				
Destination (32 bits)				
Options				

Figure 16.10: IPv4 packet

- Total length field changes when a packet is fragmented.
- ID identifies multiple fragments of the same packet and thus remains the same across all the fragments.
- OFFSET dictates the point where the original packet is fragmented.
- MF (more fragment) tells whether this is the last fragment of the packet or not. Could be 0 or 1.
- DF (Don't fragment) It could take values 0 or 1. If the DF flag is set and fragmentation is required to route the packet, then the packet is dropped

Example: Consider a packet P of size 2300 Bytes passing through a router which has the MTU = 1500 Bytes for the next network. The packet would fragment into 2 packets P1,P2 of size 1500 Bytes and 800 Bytes respectively.

**Note: Ignore the size of headers for this problem
If P has these fields :
P1 → ID = 0x12ef
length = 2300
OFFSET = 0
MF = 0

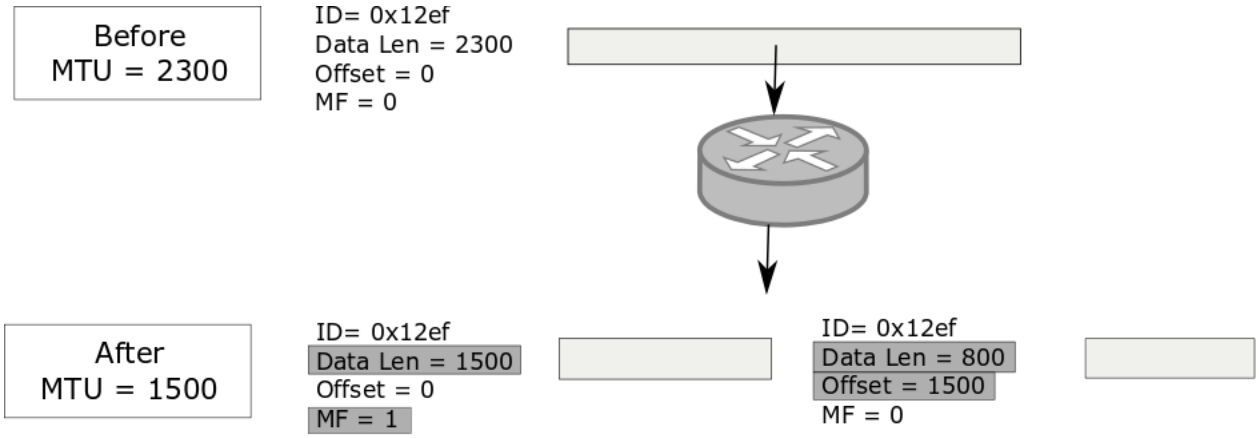

Figure 16.11: Fragmentation example

Then P1 and P2 would have the following fields:
P1 → ID = 0x12ef
length = 1500
OFFSET = 0
MF = 1

P2 → ID = 0x12ef
length = 800
OFFSET = 1500
MF = 0

16.5.1 Advantages

- It is a simple one-step process.
- It speeds up the data flow within the network.

16.5.2 Disadvantages

- If one fragment is lost, the whole packet is lost.
- One router cannot see the whole content until it gets all fragments; thus it hides the data from the router and thus the data cannot be corrected at intermediate routers.

16.6 References

[1] https://en.wikipedia.org/wiki/Bootstrap_Protocol

[2] https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[3] https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/

[4] https://courses.cs.washington.edu/courses/csep561/

[5] https://www.netscantools.com/nstpro_arp_scan.html

[6] https://www.cse.iitk.ac.in/users/dheeraj/cs425/

[7] http://ccnaeducation.com/host-routing-tables/