DEVICE MOBILITY

Enabling mobility with logical addressing

Frame Addressing

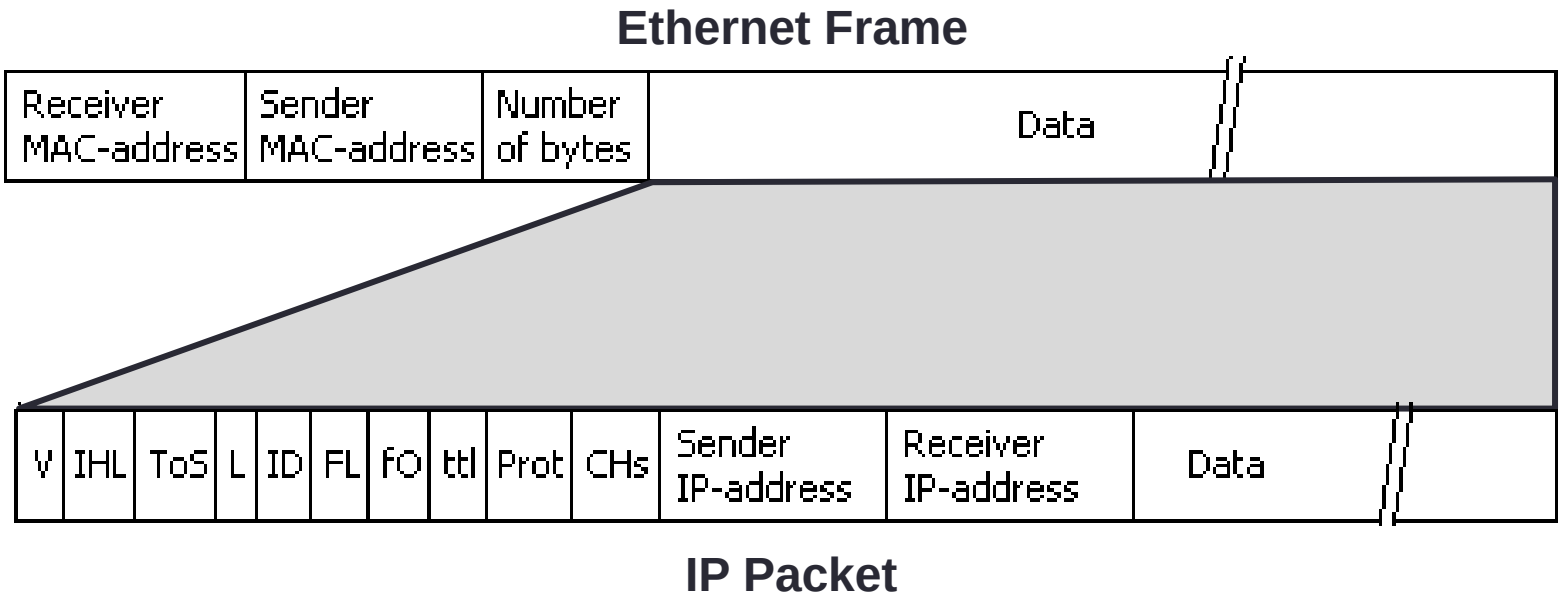
- Frames use hardware addresses to exchange Data, this means that you should know the hardware address of your destination.
- This means that a device wanting to exchange data with 200 other devices spread around the world would have to find a process to discover the MAC addresses of the destinations.
- Also, what would happen if the device moves to another location ?

Logical Addressing

- Logical addresses are part of the Packet header, the same way that Hardware addresses are part of the frame header.
- The difference between a packet and a frame is the level of encapsulation.
- Once a frame as been processed all the frame information is removed, the header and the trailer, leaving only the frame payload
- This remaining Payload is the packet

Network Packet

- When the frame information is removed, decapsulated, the remaining information is the Data with the IP header information



Network Packet Cont'd

- The packet header is comprised of round 160 bits and followed by the payload

Version	Internet Header Length	Tos	Packet Length	Identification Tag	Fragment Flag	Fragment Offset	TTL	Protocol	Header Checksum	Source IP	Destination IP
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	13 bits	8 bits	8 bits	16 bits	32 bits	32 bits

- Packets do not have a trailer / footer as the frame already has one

Packet Header

- The *version* 4 bit field specifies if the packet is IPv4 or IPv6
- In IPv6 the header fields are different.

- The *Internet Header length* field contains the length of the header of the packet in multiples of 4 bytes,
- this is necessary because optional flags can be appended to the end of the packet header.
- A standard header is 160 bits, the IHL field will hold the value “5”,(5 x 4 bytes/octets = 20 bytes/octets = 160 bits)

Packet Header

- Then follows 8 bits that contain the *Type of Service*, also referred to as Quality of Service (QoS), which describes what priority the packet should have,
- 16 bits that contain the *length* of the packet in bytes,
- 16 bits that contain an *identification tag* to help reconstruct the packet from several fragments,

Packet Header

- Next, in the *Fragment Flag*. The first bit contains a zero, followed by a flag that says whether the packet is allowed to be *fragmented* or not (DF: Don't fragment), and a flag to state whether more fragments of a packet follow (MF: More Fragments)

- Followed by 13 bits that contain the *fragment offset*, a field to identify position of fragment within original packet

Packet Header

- Then, 8 bits that contain the *Time to live* (TTL), which is the number of hops (router, computer or device along a network) the packet is allowed to pass before it dies

- 8 bits that contain the *protocol* (TCP, UDP, ICMP, etc.)

- 16 bits that contain the *Header Checksum,* a number used in error detection,

Packet Addressing

- The last 2 fields contain the logical addresses coded over 32 bits
- The different between hardware addresses and logical addresses, a part from the length, is the fact that the latter are not hard coded by the vendor, but reflect the network position of the device,
- These IP addresses are globally unique and are assigned by the Network Information Center

IP Addresses

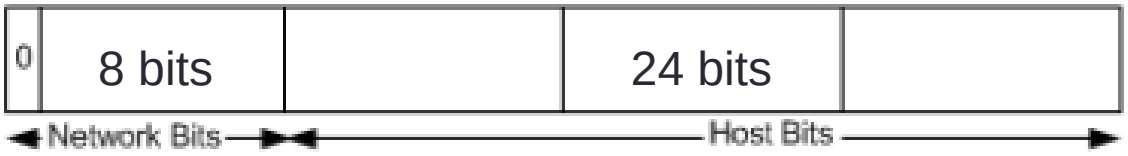
- To be easily read by humans the usual representation of an IP address is in the dotted decimal format, dividing each octet by a dot.
  - Example: 11000000 10101000 00000001 00000001
    Gives the decimals : 192 168 1 1
    Which gives use the IP address 192.168.1.1

- IP Addresses within a network are assigned by the administrators, who received an IP block allocation from the regional NIC.

IP Addresses

- IP addresses are divided into 2 parts:
  - the first part represents the network which the device is on, known as the *Network ID*
  - The second part represents the host, or end device, known as the *Host ID*

- The full IP gives the information:
  - What host ?
  - Where ? (On what network ?)



IP Classes

- The IP address space is divided into different network classes.
  - Class A networks are intended mainly for use with a few very large networks, because they provide only 8 bits for the network address field.
  - Class B networks allocate 16 bits, and Class C networks allocate 24 bits for the network address field.
  - Class C networks only provide 8 bits for the host field, however, so the number of hosts per network may be a limiting factor.

Class	First Octet Range	Valid Network Numbers*	Total Number for This Class of Network	Number of Hosts Per Network
A	1 to 126	1.0.0.0 to 126.0.0.0	$2^7 - 2$ (126)	$2^{24} - 2$ (16,777,214)
B	128 to 191	128.0.0.0 to 191.255.0.0	2^{14} (16,384)	$2^{16} - 2$ (65,534)
C	192 to 223	192.0.0.0 to 223.255.255.0	2^{21} (2,097,152)	$2^8 - 2$ (254)

IP Classes

- Upon the creation of the world global inter – network, each organization could request a block of IPs from a class.
- So universities, the first organizations to join the global network, where allocated Class A networks
- Companies and country late to join the effort where allocated Class C networks
  - A Class A network uses the 8 first bits for the Network ID, and thus has 24 bits to address hosts, which means 2^{24} or 16,777,216 hosts
  - A Class C Network uses the 24 first bits for the Network ID, creating more available networks, but limiting each network to 2^8 or 256 hosts

Receiving a Packet

- Upon receiving a Frame, the device processes the frame header and determines if the destination hardware address matches the devices own (MAC address)
- If it matches, the frame header and trailer are stripped of leaving only the frame Payload

- The Frame payload then gets treated by a different process which considers it as a packet, each field of the packet header is analyzed, and the process determines if the destination logical address matches its own (IP address)
- If it does, the packet is passed on for further processing, if not it is dropped

Sending a packet

- When a device wants to send data to another device it has to construct the packet, so it needs:
  - The Data to send
  - The Source IP (the device's IP)
  - The Destination IP, provided by upper application layers
- This information enables to construct the IP packet and pass it to the *Framing* process as payload
- The Framing process will prepend the Frame Header and append the Frame Trailer

Next-hop Determination

- A network host device is usually configured with the following constants:
  - An IP address
  - A Subnet mask
  - A default gateway
- With these 3 elements the device and calculate the following constants:
  - The Network address of the network it’s on
  - The Broadcast address of the network it’s on
- These calculated constants are the elements used to make the correct decisions to get data to its destination.

Network Identifier

- The first constant is the Network or Subnetwork Identifier (Net ID)
- It is calculated when a device is configured with an IP and Network mask by operating a logical AND between the values
  - 1 + 1 = 1, anything else = 0
- The subnet mask enables to tell a device which bits in it's IP are assigned to the network id, and which bits identify the host in the network
- Devices in the same network must share the same network id and the same subnet mask, only the host identifier section of the IP must be unique

Net ID

- Example: 192.168.2.1
  - In binary format :
    - IP : 1100 0000.1010 1000.0000 0010.0000 0001 = 192.168.2.1
    - Mask : 1111 1111.1111 1111.1111 1111.0000 0000 = 255.255.255.0
    - ---------- **Logical AND**
    - Result : 1100 0000.1010 1000.0000 0001.0000 0000 = 192.168.2.0

- Since all other devices in the same network will have the same first part of their IP and the same network mask, their network identifiers will be the same

- This is how a device knows if the destination is local to it's own network or not

Sending Data to another Network

- We a device wishes to send data to another it tries to find out if the destination is local to the network or is on another network
- It does this by calculating the destination's Net ID,
  - The source device doesn't know the destination's network mask, but if they are on the same network it should be the same
- If the calculated destination Net ID is different from the local Net ID then the data is sent to a local gateway
- The IP destination remains the same, the MAC destination is the hardware address of the local gateway

Packet Encapsulation

- The Framing process is known as packet encapsulation, and it needs the following information:
  - The source MAC address (It's own hardware address)
  - The destination MAC address
- The destination MAC address is the missing variable, there would be no point in having logical addresses if the hardware addresses where known.
- To get the destination MAC, the source goes through a process known as ARP

Address Resolution Protocol

- ARP, address resolution protocol, is used to find MAC addresses from IP addresses
- When a host first comes online in an Ethernet enviroment, the only address it knows is its own Layer 2 Mac address.
- But if the host wants to communicate it needs the destination address to build the frame.
- So the hosts send out and ARP request

	Time	Source	Destination	Protocol	Length	Info
343	116.289468000	FreeboxS_bc:5e:5b	Dell_61:94:f0	ARP	62	Who has 192.168.1.11? Tell 192.168.1.254
344	116.289488000	Dell_61:94:f0	FreeboxS_bc:5e:5b	ARP	42	192.168.1.11 is at 5c:26:0a:61:94:f0

```
Frame 59: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: FreeboxS_bc:5e:5b (00:24:d4:bc:5e:5b), Dst: Dell_61:94:f0 (5c:26:0a:61:94:f0)
Address Resolution Protocol (request)
VSS-Monitoring ethernet trailer, Source Port: 0
```

ARP Request and Reply

- An ARP Request is a Frame destined to everybody, this frame bears one question:
  - Who has this IP X.X.X.X ?
  - The IP is known, what we are searching for is the MAC Address
  - The destination MAC of this Frame is 48 bits of binary 1s, the highest possible address,
- Each device in the network will receive this frame and read it,
- Only the device that owns the IP will reply,
  - The ARP Reply message will contain the device's MAC address as source of the reply, thus informing the querier of the answer

ARP Cache

- When the device sourcing the ARP Request receives the reply it immediately records the information in a table known as the ARP Cache
- The ARP Cache contains the known IP to MAC address mappings

```
Interface: 192.168.1.16 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.12          00-11-32-00-fa-f1     dynamic
  192.168.1.15          00-25-22-eb-ee-8e     dynamic
  192.168.1.18          00-17-31-83-b2-b3     dynamic
  192.168.1.254         00-24-d4-bc-5e-5b     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```