_/_/_

Module-3

* Network layer services
- Routing and Forwarding
- Packetizing
- Provide services to Other layers (upper layers)
- Error Control, Congestion Control, Flow Control, QoS and security

• Total Address space is 2^{32} bits in an IPv4.
Address IPv4 is 32 bit long.

• If any protocol uses N bit to define an address, address space is 2^N because each bit can have 2 different values and N bits can have 2^N values

* Classful Addressing

(1) Finding class in binary notation, decimal notation

	First Byte	Second Byte	Third Byte	Fourth Byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

Class A	0-127	$0\boxed{0000000}$ to $0\boxed{1111111}$
Class B	128-191	
Class C	192-223	
Class D	224-239	8bit 8bit 8bit
Class E	240-255	No. of subnets (1st bit chodke)

No. of subnets : $= 2^7$
No. of Hosts $= 2^{24}$ } Class A

__/__/____

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	NetId	HostId		
class B	NetId		HostId	
class C	Net Id			Host Id
class D	Multicast Address			
class E	Reserved for future use.			

- Class A: 2^{31} Address space
- Class B: 2^{30} Address space
- Class C: 2^{29}
- Class D: 2^{28}
- Class E: 2^{28}

* Mask

- A mask is a 32-bit binary number that gives the first address in the block also called as network address when bitwise ANDed with an address in the block.

$$\begin{array}{ccccc} & & \text{Mask} & & \\ & & \downarrow & & \\ \text{An address in the block} & \longrightarrow & \text{AND Operation} & \longrightarrow & \text{Network Address} \end{array}$$

- Network address is found by applying default mask to any of the addresses including itself
- It retains the net id and sets the host ids to 0.

eg: Address of Block: 73.22.17.25

→ No.of addresses in block : $2^{32-n} \Rightarrow n = 8 = 2^{32-8} = 2^{24}$ → net id has 8 bits

First address of block: We keep leftmost 8 bits and change remaining 24 bits to 0. So here it will be 73.0.0.0/8 (8 is

Last address is : We keep first 8 bits and change last 24 bits to 255. So last address is 73.255.255.255

(special address)

* ~~Broadcast~~ address: Types:

1. Direct broadcast address:

It used by router to send message to every host on the ~~our~~ same ~~local~~ network. However, Packet is blocked by routers to confine the packet to local network.

Direct broadcast address is used by a router to send a message to every host on local network. Every host/router receives ~~to~~ and processes the packet with a direct broadcast address.

Net Id - Specific   Host Id - All 1s

2. Limited broadcast address:

Limited broadcast address is used by host to send packet to every host on the same network. However, Packet is blocked by routers to confine the packet to the local network.

Net Id & Host Id : All 1's.

3. 'This' Host on 'This' address:

A host does not know its IP address uses IP address 0.0.0.0 as source address and 255.255.255.255 as the destination address to send message to a bootstrap server.

Net Id & Host Id : All 0's.

4. Specific Host on 'This' network:

Used by router /host to send a message to a specific host in same network

Net Id: All 0's   Host Id: Specific

5. Loopback Address:

Packet with loopback will not reach the network

/ /

Private Address :

Number of blocks in each class are assigned for private use.

They cannot be recognised globally.

7. Network address:

- First address of the network.
- It defines the network to the rest of the Internet.
- If network address is known, we can find class, block, range of addresses in the block.

8. Public Address:

* NAT

- The distribution of addresses through ISP has created a new problem. Businesses and households grow and need a larger range. But ISP may not be able to grant those demands because addresses before and after the range may be allocated to other networks. In most situations, only a portion of computers need access to Internet simultaneously. To Technology that can help us in such a case in is NAT (Network Address Translation)

(See dig. from pdf)

- If using one global address, only one private-network host can be used to access the same external host.
- Two private-network hosts cannot access the same external program at the same time by using same global address.
- If there is a pool of global addresses, let's say 4 then only 4 private-network addresses can access the global address.

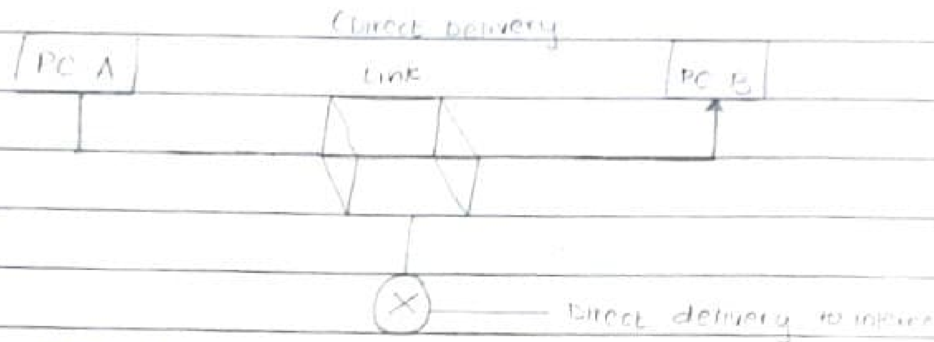
__/__/__

* Delivery and Forwarding of IP Packets

* **Delivery:** The network layer supervises the handling of the packets underlying in the physical network. The successful delivery of packet from source to its final destination can be done using two methods:

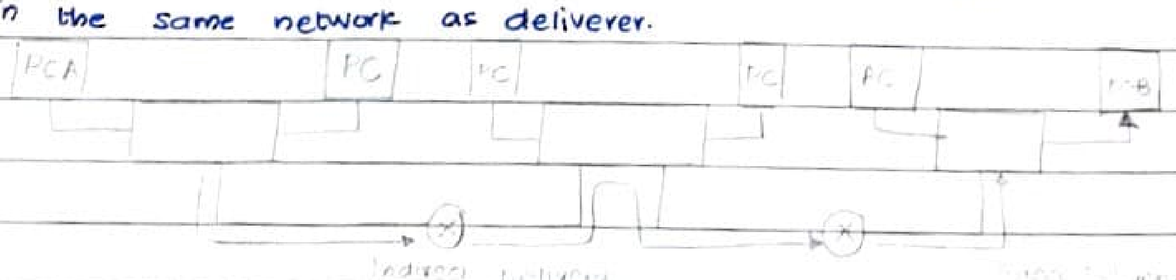
(1) **Direct Method:**

Here the final destination of packet is a host connected to same physical network as the deliverer.



2. **Indirect Method:**

Here, the packet goes from one router to another until it reaches the ~~physi~~ router connected to the same physical layer as the destination. Destination source is not in the same network as deliverer.



* **Forwarding:** Forwarding means placing the packet in its route to destination. Forwarding means to deliver the packet to the next hop which is either the final destination or an intermediate connection.

1. Next Hop

eg: See dig. from figure

For A

Destination	Next Hop
B	R1, R2, Host B

For R1

Destination	Next Hop
Host B	R2, Host B

For R2

Destination	Next Hop
Host B	Host B

2. Network Specific

eg: For S

Destination	Next Hop
N2	R1

3. Host-Specific

eg: For S

Destination	Next Hop
A	R1
B	R1
C	R1
D	R1

4. Default Routing

eg: Routing table for A

Destination	Next Hop
N2	R1
Default	R2

5. Simplified Forwarding in classful addresses without subnetting

__/__/____

3 Address Deletion Problem in Classful Addressing

Short term Solution
- Use of Private addresses
- Subnetting
- Supernetting
- Use of NAT and DHCP
- Classless Addressing

Long term Solution
- IPv6

* Classless Addressing

* Prefix Length: slash Notation.

- In classless addressing, prefix length needs to passed separately.
- It added to address
- Notation is informally referred as slash notation and formally as CIDR.
- In classless addressing we need to know one of the addresses and prefix length to define the block.

→ slash notation

byte	.	byte	.	byte	.	byte	.	/	n

↳ Prefix Length

Class A: n = 8   Class C: 24

Class B: n = 16

* Subnetting

g:1 Destination Address: 200. 45. 34. 56

Subnet Mask: 255. 255. 240. 0

Subnetwork address?

Destination Address: 11001000 . 00101101 . 00100010 . 00111000

Subnet Mask : 11111111 . 11111111 . 11110000 . 00000000

AND Subnet Address: 11001000 . 00101101 . 00100000 . 00000000

1, 0

⟹ 200. 45. 32. 0

eg: 2 Destination Address: 00010011. 00011110.01010000.00000101

Mask : 11111111. 11111111. 11000000. 00000000

AND Subnetwork address: 00010011. 0011110. 01000000. 00000000

19. 30. 64. 0

- No. of subsets must be a power of 2

eg: 3 Site address: 201. 70. 64. 0 (Classful Addressing)

Company need 6 subnets.

Since 6 is not a power of 2, we take closest value which is 8 (2^3).

Since it is a class C addressing, total no. of 1's is 24

Now we need 3 more 1's.

∴ We have now 24+3 = 27 1's and 32-27 = 5 0's.

The mask is 11111111. 11111111. 11111111. 11100000

255. 255. 255. 224

The no. of addresses are $2^5 = 32$ (5 no. of zeros)

The no. of subnets are 8.

eg: 4 Site address: 181. 56. 0. 0 (Classful Addressing)

Company needs 1000 ~~addresses~~ subnets

Since ~~comp~~ 1000 is not a power of 2, we take nearest value - 1024 (2^{10}).

Since it is a class B addressing, 16 1's are already fixed.

Now we need 10 more 1's.

∴ We have 16+10 = 26 1's fixed and 32-26 = 6 0's

∴ Mask is 11111111. 11111111. 11111111. 11000000

255. 255. 255. 192

Total no. of addresses: $2^6 = 64$

Total no. of subnets: 1024

__/__/__

eg: 5 Network Address: 200.50.100.0 (Classful Addressing)

Mask is /27

- Initial Mask is 24 (Class C)

New mask: 27

- No. of bits used for subnetting = ~~24~~ 27-24=3

$\therefore$ No. of subnets created: $2^3 = 8$

- No. of addresses in each subnet = $2^{(32-27)} = 2^5 = 32$

- Network Address of Subnet 1: 200.50.100.0

Subnet 2: 200.50.100.32

Subnet 3: 200.50.100.64

Subnet 4: 200.50.100.96

Subnet 5: 200.50.100.128

Subnet 6: 200.50.100.160

Subnet 7: 200.50.100.192

Subnet 8: 200.50.100.224

eg: 6 Network/ IP address : 170.50.100.70

No. of subnets made = 4094

Since it is not a power of 2, we consider 4096 (2^{12})

$\therefore$ No. of masks for subnets : 12+2 = ~~14~~ 10

No. of host bits = n

$\therefore$ 4094 is no. of hosts (valid)

$\therefore$ $4094 = 2^n - 2$

$\therefore n = 12$

Network bits: 20

No. of subnets = 2^{20}

Subnet address of first subnet:

_/_/_

Classless addressing sums:

Beginning addressing: 205.16.37.24 /29
Prefix

First 29 bits are fixed. We change last 3 bits to 1
There will be 2^3 addresses only then.
So last address will be 205.16.37.31
Verifying by converting to binary
Beginning: 11001101. 00010000. 00100101. 00011000
Ending: 11001101. 00010000. 00100101. 00011111
first 29 bits fixed.

Verified only 8 addresses available.

2 What is the network address if one of the addresses is 167.199.170.82/27.
We keep first 27 bits the same. We change only last 5 bits.
Last 5 bits affect the 4th byte which is 82
82 ⇒ 01010010. Changing last 5 bits to 0 we get:
01000000 = 64
∴ Network address is 167.199.170.64/27

eg 3: 130.34.12.64/26
Total addresses in block: $2^6 = 64$ (32-26=6)
4 subnets, each subnet 16 addresses
4 subnets ⇒ 2 mask (2 1's added to prefix)
First address of subnet 1 (Range): 130.34.12.64/28 - 130.34.12.79/28
Add 15 for subnets and find for all 4

_/_/_

eg:4. Total no.of addresses: $2^8 = 256$

First address : 19.24.74.0/24

Last address: 14.24.74.265/24

(a) For first block, 120 is not power of 2 so we can assign 128 addresses

∴ Mask = 25 (10000000) 1 one got fixed so from 24 become 25

(b) For second block, we assign 64 addresses)

∴ Mask = 26 (01000000) 2 places got fixed

(c) For third block, we assign 16 addresses

∴ Mask = 28 (00010000) (00010000)

eg 5: $N_C = 32$ $N_W = 16$

$N_E = 16$

First address : 70.12.100.128/26

(a) For N_c, 32 addresses assigned, one value gets fixed so the fourth byte now has 3 values fixed.

Mask = 27

(b) For N_e, 16 addresses are assigned, 2 values more are fixed so in total four values from 4th byte are fixed.

Mask = 28

(c) similarly, for N_W, Mask = 28

Starting address: 190.100.0.0/16

Group 1

64 customers and each need 256 addresses. Total = 64x256

$= 2^{14}$

New mask = 18 (because 14 occupies 216 places)

First address : 190.100.0.0/18

Last address. 190.100.63.255/18

Group 2:

128 customers need 128 addresses each.

Total = 2^{14}

New mask = 18

First address: 190.100.64.0/18

Last address: 190.100.127.255/18

Group 3:

128 customers need 64 addresses

Total = 2^{13}

New mask = 19

First address = 190.100.128.0/19

Last address = 190.100.159.255/19

__/__/__

* Supernetting:
- Aggregating smaller networks into a larger network.
- Main purpose is to reduce the size of routing table on routers.
- It saves memory and processing resources on routing devices.
- Also helps in slowing down the exhaustion of IP addresses through the use of CIDR
- In supernetting, we need first address of supernet ~~mask~~ and supernet mask to define range of addresses

: Make a Supernet network out of 16 Class C blocks. What is the mask?

→ For 16 blocks, we convert 4 ~~zeros~~ 1's of third byte of class C to 4 0's. So default mask is:

11111111 11111111 11110000 00000000

See other from ppt.

Address Routing Protocol (ARP)

To make a distinction between logical address and IP address.

Describe how mapping of a logical address to a physical address can be static or dynamic.

Delivery of a packet from host or a router requires two levels of addressing: logical and physical.

We must be able to map a logical address to its corresponding physical address and vice-versa.

This mapping can be done using static or dynamic mapping.

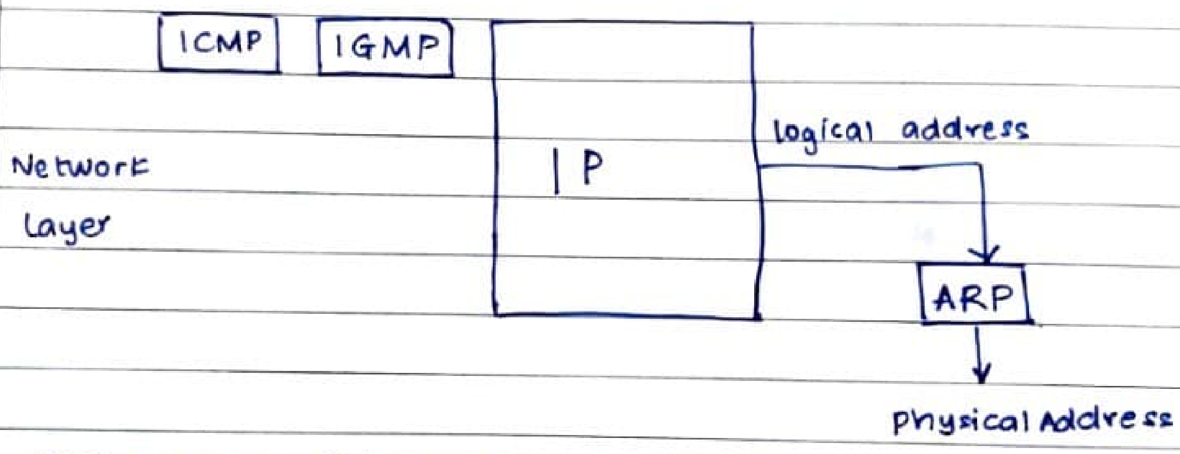
_/_/_

* **Address Mapping:**

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical address of the receiver. But the IP datagram must be encapsulated in one frame to be able to pass the physical network.

- Sender needs the physical address of receiver. A mapping corresponds to the logical address to the physical address.

- ARP accepts a logical address from the IP protocol, maps the address to the physical address and pass to data link layer.



- ARP request is broadcast and ARP reply is unicast

- ARP Packet :

Hardware Type		Protocol Type
Hardware Length	Protocol Length	Operation Request 1, Reply 2
Sender Hardware Address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

Encapsulation of ARP:

ARP request or reply packet

Preamble and SFD	Destination address	Source Address	Type 0X0806	Data	CRC

Four cases using ARP:

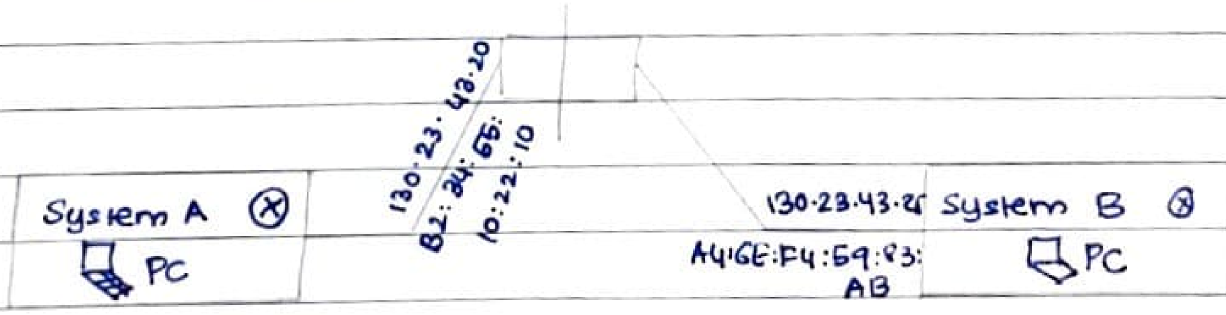
1. Host has a packet to send to a host in the same network.
   Target IP address: Destination Address in the IP datagram.

2. Host has a pactet to send to a host on another network.
   Target IP address: IP address of a router.

3. ~~Host~~ Router has to send ~~s~~ a packet to host on another network
   Target IP address: IP address of router.

4. Router has to send a packet to a host in same network
   Target IP address: Destination address in IP datagram.

eg: Host IP address (logical /hardware) : 130.23.43.20
Host Physical address: B2: 34: 55 :10: 22:10
Receiver IPaddress: 130. 23 . 43.25
Physical address: A4:6E:F4: 59: 83: AB



_/_/_

~~From~~ Request

From A to B →

0X0001		0X0800
0X06	0X04	0X0001
0X B23465102210 0X 8217B14		
0X 000000000000		
0X 8217B2B19		

130.23.43.20 ...

130.23.43.25 ....

Preamble and SFD	0XFFFFFFFFFFFF (12)	0XB23455102210	0X0806	Data 28 bytes	CRC

Reply

From B to A ←

0X0001		0X0800
0X06	0X04	0X0002
0X A46EF45983AB		
0X 82172B19		
0X B23455102210		
0X 82172B14		

Preamble and SFD	0XB23455102210	0X A46EF45983AB	0X0806	Data	CRC

* ~~Proxy ARP~~ ATM ARP

- When IP packets are moving through an ATM WAN, a mechanism protocol is needed to find the physical address of exiting point router
- This same task is performed by ~~ATM~~ ARP on LAN. Although, LAN is a broadcast network and ARP uses broadcasting capability of LAN to send /broadcast an ARP request.

* ATMARP Packet

Hardware Type		Protocol Type	
Sender Hardware Length	Reserved	Operation	
Sender Protocol Length	Target Hardware Length	Reserved	Target Protocol Length
Sender Hardware Address			
Sender ~~Target~~ Protocol Address			
Target Hardware Address			
Target Protocol Address			

- LIS allows each ATM network to be divided into several logical subnets.
- To use ATMARP we need a separate server for each subnet.

* ARP Package

- ARP Package has 5 components:

(1) Cache Table (2) Queues (3) Output Module (4) Input Module
(5) Cache Control Module.

(See fig)

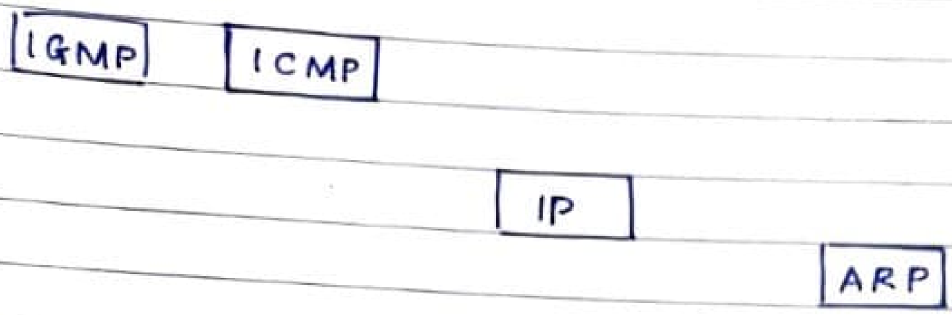
* ICMP Version 4 (Internet Control Message Protocol)

ICMP is basically used to overcome 2 problems of IP Protocol:

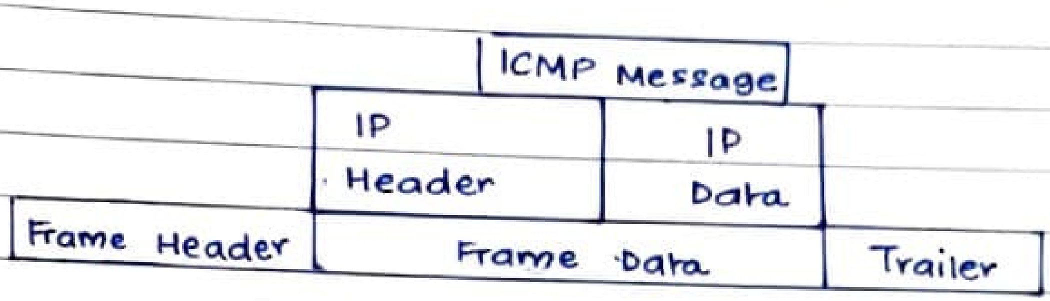
(1) No. error handling / correction
(2) lacks mechanism queries.

__/__/__

* **Position:**



* **Encapsulation:**



* **Messages:**

- ICMP messages are divided into two types:

(1) Error reporting: These messages report problems faced by a router or a host when it processes an IP packet.

(2) Query messages: Occurs in pair where the host or network manager get specific information from router or another host. Host can discover and learn about their networks and help node redirect its messages.

- General Format:

8 bits	8 bits	8 bits — 8 bits
Type	Code	Checksum
Rest of Header		
Data Section		

- Destination unreachable
  Type: 3 Code: 0 to 15
- ~~Score~~ Source quench format
  Type: 4 Code: 0
  (see pdf for detail)

- ICMP reports the error to original source.
- Error reporting messages:

(1) Destination unreachable
(2) ~~Score~~ Source quench
(3) Time exceeded
(4) Parameter Problems
(5) Redirection

_/_/_

- ICMP messages are not generated for:
(1) Datagram carrying ICMP error message.
(2) Fragmented datagram that is not first fragment
(3) Multicast address.
(4) Datagram having special addresses like loopback or 0.0.0.0

(1) Destination Unreachable: (Type: 3, Code: 0 to 15)
- Destination unreachable message can be generated by 2 code 2 or 3 only by destination host.
- Other destination unreachable messages are generated by the router only.

(2) Source- quench: (Type: 4, Code: 0)
- Source quench message informs datagram has been discarde due to congestion in router or destination host.
- Source must slow down the sending of datagrams until the congestion is relieved.
- One source quench message for each datagram that has been discarded.

(3) Time- exceeded: (Type: 11, Code: 0 or 1)
- Whenever a router decrements a datagram with a time-to-live to zero, it discards the datagram and sends this messa to original source.
- When the final destination does not receive all fragments and sends a time exceeded message to original source.
- Code 0 is used only by routers to show that value of tim to live field is zero.
- Code 1 is used only by the destination host to show that no all the fragments have arrived within a set time.

__/__/__

(4) Parameter Problem: (Type : 12, code: 0 or 1)
- It is created by router or destination host.

(5) Redirection : (Type: 5, code: 0 to 3)
- Host gradually starts with a small routing table that is gradually updated and augmented
- One of the tools to achieve this is redirection.
- This message is sent from router to a local host in the same network

6. Echo Request and Ready: (Type : 8 (Echo Request), 0 → Echo Reply , Code: 0)
- An echo-request message can be sent by a host/ router.
- An echo- reply message is sent by host / router that receives the echo request message.
- Both can be used by network managers to check operation of IP protocol.
- They can also trace reachability of a host. This is usually done by invoking ping command.

(7) Time stamp request and reply message: (Type: 13 (request), 14 (reply) code: 0)
- Used to calculate round trip time between a source & destination machine even if their clocks are not synchronised
- Synchronizes two clocks in the two machines if exact one-way time duration is known.

* BOOTP
- Bootstrap Protocol is a client/ server protocol that configures a diskless computer or a computer that is booted for the first time.
- BOOTP provides the IP address, net mask, address of a default router and address of a name server.

- BOOTP is a static configuration protocol
- It is a client/server program, boot server can be anywhere in the internet.
- BOOTP uses a static database.

★ BOOTP Packet Format

<table>
<tr><td>Operation Code</td><td>Hardware Type</td><td>Hardware Length</td><td>Hop Count</td></tr>
<tr><td colspan="4">Transaction Id</td></tr>
<tr><td colspan="2">Number of Seconds</td><td>F*</td><td>unused</td></tr>
<tr><td colspan="4">Client IP address</td></tr>
<tr><td colspan="4">Your IP address</td></tr>
<tr><td colspan="4">Server IP address</td></tr>
<tr><td colspan="4">Gateway IP address</td></tr>
<tr><td colspan="4">Client Hardware address</td></tr>
<tr><td colspan="4">Servername</td></tr>
<tr><td colspan="4">Boot filename</td></tr>
<tr><td colspan="4">Options.</td></tr>
</table>

* Here the F is added only for DHCP. Not for BOOTP.

Option Format

Tag (0)	Padding

Tag	Length	Value (variable length)

Other options

Tag (End)

_/_/_

* DHCP

- Dynamic Host Configuration Protocol provides static & dynamic address allocation that can be manual or automatic.
- DHCP is a successor to BOOTP and is backward compatible
- DHCP server can be on same / different network.

* Packet Format (refer bootp)

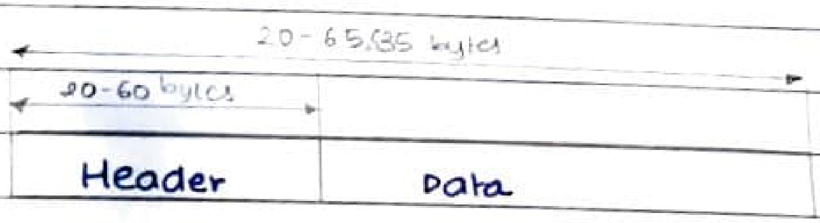
* See transition diagram from ppt once

* IPv4

- The Internet Protocol is the transmission mechanism used by TCP/IP protocols at network layer.
- IP is unreliable and connectionless protocol - a best effort delivery service.

* ~~Packets~~ Datagrams:

- Packet in the network layer are called datagrams. A datagram is a variable-length package consisting of 2 parts: header and data.
- Header is 20 to 60 bytes in length and contains information essential to routing and delivery.
- It is customary in TCP/IP to show header in 4 byte sections.



Datagram

__/__/____

* Header Format

0 3 4 7 8 15 16 31

<table>
<tr><td>VER
(4bits)</td><td>HLEN
(4bits)</td><td>Service Type
(8 bits)</td><td colspan="2">Total Length
(16 bits)</td></tr>
<tr><td colspan="3">Identification
(8 bits)</td><td>Flag
(3bits)</td><td>Fragmentation offset
(13 bits)</td></tr>
<tr><td colspan="2">Time to live
(8 bits)</td><td>Protocol
(8 bits)</td><td colspan="2">Header Checksum
(16 bits)</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40) bytes</td></tr>
</table>

VER: Version

HLEN: Header Length

Service Type: ToS or DSCP

- The total length field defines the total length of datagram including the header.

(see eg. from pdf)

* Fragmentation:

A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it was receives, processes it and encapsulates in another frame. The format and size of received ~~sent~~ frame depends on protocol used by physical network. The frame and size of sent frame depends on protocol used by physical network through which the frame is going to travel.

_/_/_

* IPv6

- An IPv6 address is 128 bits or 16 bytes long (octet)
- Address length is 4 more times of the length of IPv4.
- Entire address space is divided into 8 blocks equal ranges
- Unspecified address in IPv6 is ::/128. It should not be used as Destination.
- In IPv4 this unspecified address is a part of class A and in IPv6 it is a part of the reserved block.
- Loopback addres ::1/128 should never be used as destination address. In IPv4 / classful addressing an entire block is reserved for loopback addresses. Aditionally, the loopback addresses were a part of class A. In IPv6, it is only one single address in the reserved block.

* Embedded IPv4

During transformation of IPv4 to IPv6, hosts can use their IPv4 addresses and embed in IPv6 address.

- Compatible Address:

00000000	All 0's	IPv4 address
96 bits		32 bits

eg: IPv4 ⇒ 2.13.17.14 becomes 0:: 2.13.17.14 (in mixed format)
used when IPv4 using computer wants to send a message to computer using IPv6

- Mapped Address

used when computer that has migrated to IPv6 still wants to communicate with computer using IPv4.

00000000	All 0's	All 1's	IPv4 address
80 bits		16 bits	32 bits

__/__/____

- IPv6 uses 2 large blocks for private addressing. One is at site level and one at the link level.

(1) Unique Local Unicast (FC00::/7)

- A uniquely local unicast block can be privately created and used by a site. It is not expected to be routed.

(2) Link Local Address

(3) Multicast Address

- A permanent group address is defined by internet authorities and can be accessed at all times.
- A transient group address is only used temporarily.
- Third field defines the scope of the group address.

* Global unicast Address (FE::80/10)

- This block is used for one-to-one communication b/w two hosts in the internet called Global Unicast address.
- CIDR notation for this block is 2000::/3 which means 3 leftmost bits are same for all addresses. Size of this block is 2^{125} bits, which is more than enough for internet expansion in the years to come.

$\underbrace{\text{Global Routing Prefix}}_{n \text{ bits}}$ | $\underbrace{\text{Subnet Identifier}}_{128-n-m \text{ bits}}$ | $\underbrace{\text{Interface Identifier}}_{m \text{ bits}}$

eg: EUI-64 }
MAC } see their block diagrams from ppt

(SEE PPT for IPv6)

* IPv4 to IPv6

1. Dual Stack
2. Tunneling Strategy
3. Header translation.

} see dig. Vimp