www.jntuworldupdates.org

UNIT-VI
NETWORK LAYER

- Logical addressing
- internetworking
- tunneling
- Address Mapping
- ICMP
- IGMP
- Forwarding
- Uni-cast routing protocols
- Multicast routing protocols.

Logical addressing:-

- Communication at N/w Layer is host-to-host (computer-Computer).
- The sender computer should need to communicate with receiver computer, which is very far. So, the packet transmitted by the sender may pass through several LAN's (or) WAN's before reaching the destination computer.
- For this level of communication, we need a global addressing scheme, called as logical addressing.
- Logical address is known as Ip-address (Internet Protocol address).
- There are 2 types of Ip-addresses: they are:

1. IPV4 (Version 4)
2. IPV6 (Version 6)

① IPV4 (IP version 4) address:

IPV4 is a 32-bit address, which is unique (and provides connection of a device (router/computer) to the internet.

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

↳ Two devices on the internet can never have the same address at the same time. i.e IPV4 addresses are unique & universal.

↳ The address space of IPV4 is $2^{32} = 4,294,967,296$ (4 Billion approximately)

↳ There are 2 types of notations used to represent the IPV4 address: They are:

1) Binary Notation (01110101 10010101 00011101 00000010)
2) Dotted-decimal Notation (117. 149. 29. 2)

↳ The Range of IPV4 addresses are from,

00000000.00000000.00000000.00000000 (0.0.0.0)
(to) (to)

11111111.1111 1111.1111 1111.11111111 (255.255.255.255)

⇒ addressing are of 2 types:

1) classful addressing &
2) classless addressing.

classful addressing:

In this, the address space is divided into five classes:

A, B, C, D & E

Class A	0-127	0.0.0.0 (to) 127.255.255.255	designed for large-scale Organization	Uni cast
Class B	128-191	128.0.0.0 (to) 191.255.255.255	Mid-level Organizations	
Class C	192-223	192.0.0.0 (to) 223.255.255.255	Small-scale Organizations	
Class D	224-239	224.0.0.0 (to) 239.255.255.255	multi-casting	
Class E	240-255	240.0.0.0 (to) 255.255.255.255	Reserved	

↳ On classful addressing, the large part of the available addresses are wasted.

www.smartzworld.com www.specworld.in

www.jntuworldupdates.org

↳ In classful addressing, an IP address in class A, B, C is divided into network-id (nid) & host-id (hid).

	NID	HID	
Class A	1Byte	3Bytes	⇒ 1+3 = 4 bytes = 32 bits
Class B	2Bytes	2Bytes	⇒ 2+2 = 4
Class C	3 bytes	1Byte	⇒ 3+1 = 4

↳ mask (or) default mask is used in classful addressing.

Ex:

Class A : | 16 | 2.18.5 | (Nid | hid)

Class B : | 129.16. | 5.1 | (Nid | hid)

Class C : | 192.16.8 | 2 | (Nid | hid)

↳ default masks of classful addressing are shown as:

Class	Binary	Dotted decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

CIDR = class-less Interdomain Routing (It is a notation (or) Slash notation used in class-less addressing).

↳ Classful addressing, is almost absolute & is replaced with Classless addressing.

www.specworld.in

www.jntuworldupdates.org

↳ To overcome address depletion & give more organizations access to the internet, classless addressing was designed & implemented. In this scheme, there are no classes, but the addresses are still Granted in blocks.

↳ In classless addressing, when a small/large organizations needs to be connected to the Internet, it is granted a block (range) of addresses (address Blocks).

↳ The size of the block (no. of addresses) varies based on the nature & size of the entity.

Ex: A household may be given one/two address, whereas a large organization may be given thousands of addresses.

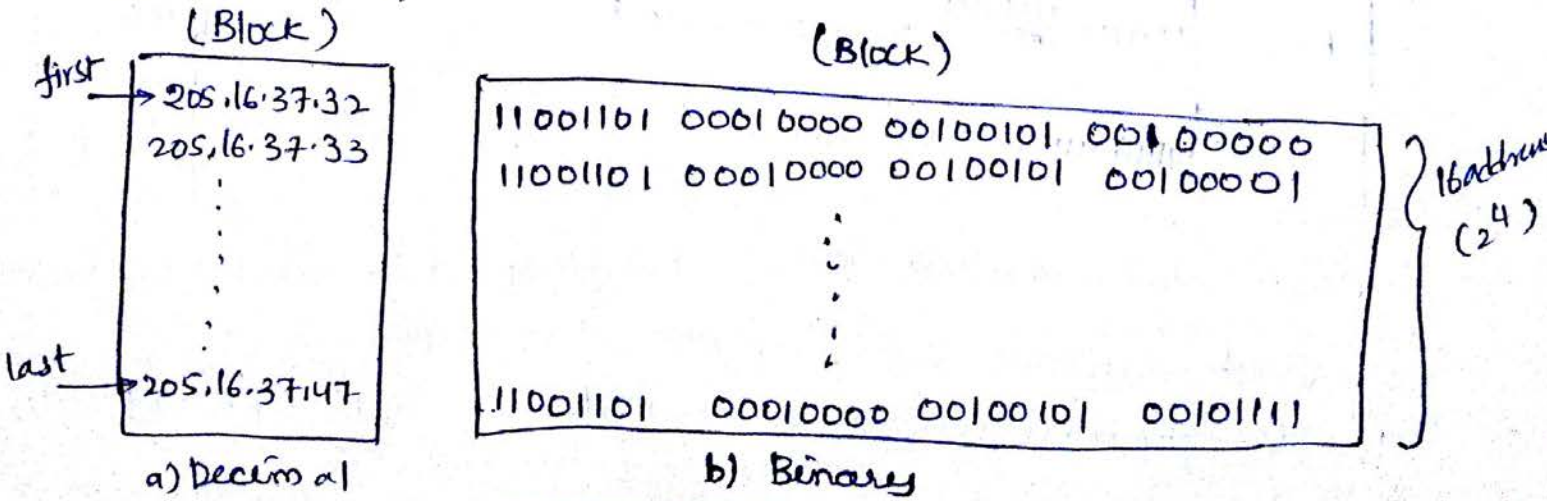
↳ An Isp (Internet Service provider), may be given thousands (or) hundreds of addresses, based on the no. of customers it may serve.

↳ To simply the handling of addresses, the Internet authorities impose three restrictions on classless address Block.

1. The address in a block must be contiguous, one after another
2. The no. of addresses in a block must be a power of 2 (1, 2, 4, ...)
3. The first address must be evenly divisible by the no. of addresses

Ex: $(\frac{32}{16})$.

Ex: A block of 16 addresses granted to a small organization.



www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

⇒ In IPV4 addressing, a block of addresses is defined as: $x.y.z.t/n$

where, $x.y.z.t$ defines one of the addresses, n defines the mask

ex: 192.168.2.2/24

192.168.2.2 → logical address

/24 → default mask

⇒ To find first address in a block, when any address within a block is given:

ex: A block of addresses is granted to a small organization we know that one of the addresses is 205.16.39.39/28. What is the first address in the Block.

sol: 205.16.37.39/28

Binary representation is;

11001101 00010000 00100101 00100111

The first address in the block can found by setting the right most (32-n) bits to 0's

i.e., 32-28; n=28 = 4 bits to 0's (right most)

i.e.,

11001101 00010000 00100101 00100000

(last 4 bits set to 0's)

i.e

205.16.37.32 is the first address.

⇒ The last address in a block can be found by setting the right most (32-n) bits to 1's

ex: To find last address of 205.16.37.39/28 is:

205.16.37.39/28

11001101 00010000 00100101 00100111

(32-28 = 4 bits)

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

i.e.,

11001101 00010000 00100101 00101111

↓↓,

4 bits to 1's.

i.e 205.16.37.47 →

∴ The actual Block is from

205.16.37.32
⋮
205.16.37.47

} Block of 16 addresses

∴ To find total no. of addresses,

when, n = 28,

total no. of addresses is 2^{32-28} = 16 addresses.

* Network addresses:

A very important in IP addressing is the Network address. when an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the internet.

→ The first address, in a block is always treated as a special address (or) Network address, & it defines the Organization Network.

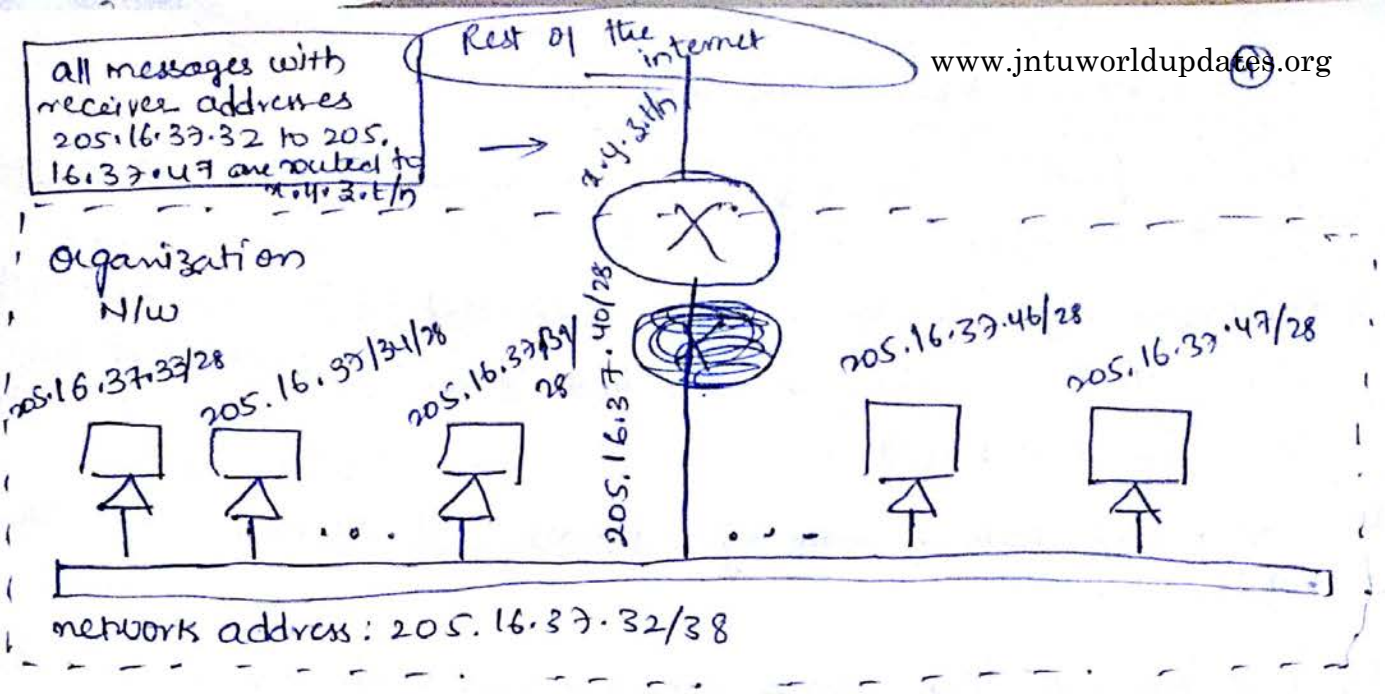
↳ Network address defines the organization itself to the rest of the world

→ see the example figure,

⇒ The following figure shows an organization that is granted as a 16-address Block.

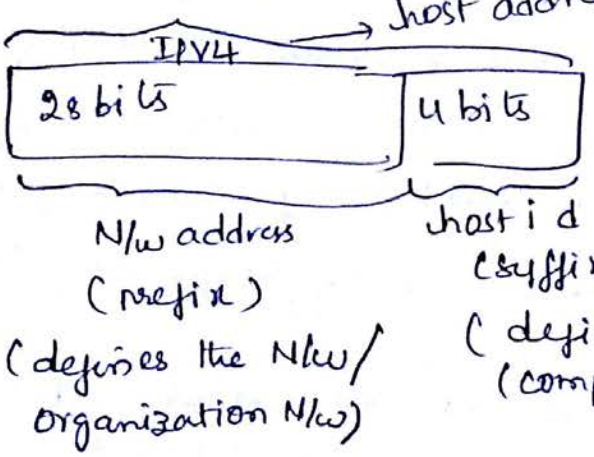
i.e., a NW configuration for the block (→NA
205.16.37.32/28
to
205.16.37.47/28)

www.smartzworld.com www.specworld.in

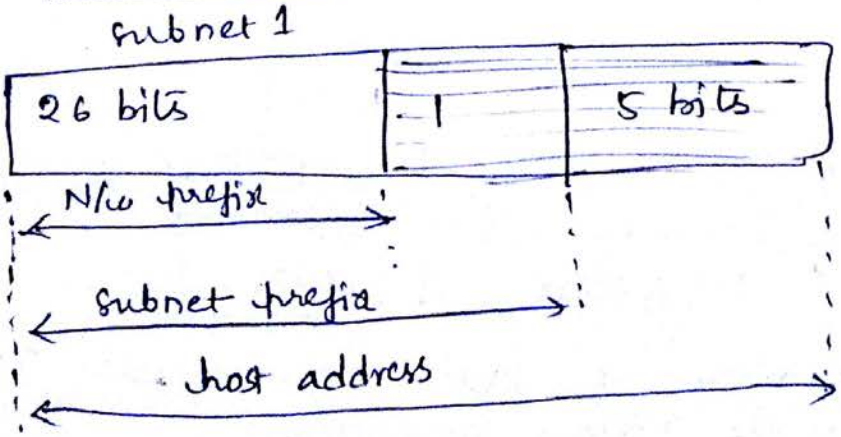


⇒ The first address in a block is normally not assigned to any device; it is used as the N/w address that represents the organization to the rest of the world.

⇒ Two-level hierarchy of Ip address, with No subnetting:



⇒ Three-level hierarchy of Ip address, with subnetting:



www.jntuworldupdates.org

NAT (Network Address Translation):

The no. of home users & small businesses that want to use the internet is ever increasing.

↳ In beginning, a user was connected to the internet with a dial-up line, which means that she was connected for a specific period of time.

↳ Using ISP (with a block of address) will dynamically assign an address to this user.

↳ But, Now, a days, home users & small businesses are connected by an ADSL line (or) cable modem, and they are not happy with one address; many have created small N/w with several hosts & need an IP-address for each host.

· With the shortage of IP addresses, this is a serious problem.

↳ A quick solution to this problem is NAT.

↳ NAT enables a user to have a large set of addresses internally & one address, (or) a small set of addresses, externally.

↳ The traffic inside can use the large set; the traffic outside, the small set.

↳ So, they seperated addresses used inside the home (or) busin-ess & the ones used for the internet.

↳ The Internet authorities have reserved three sets of addresses as private addresses.

Private addresses

Range	Total
10.0.0.0 (to) 10.255.255.255	2^{24}
172.16.0.0 (to) 172.31.255.255	2^{20}
192.168.0.0 (to) 192.168.255.25	2^{16}

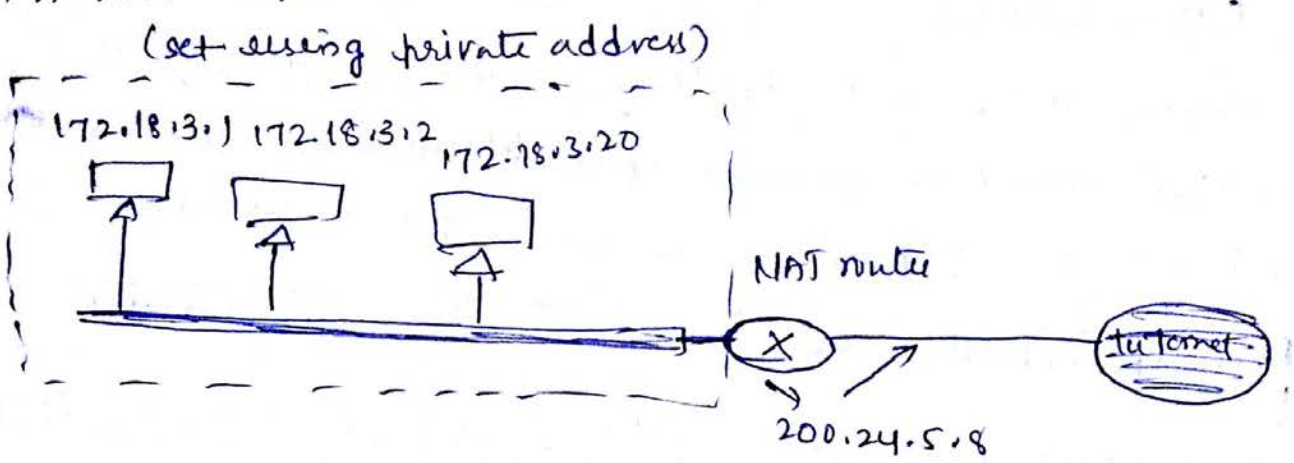
↳ Any organization can use these addresses, without any Permission from the Internet authorities.

↳ The following figure shows the private network using private addresses. The Router that connects the N/w to the global

www.specworld.in

address uses one private address & one global address. The private N/w is transparent to the rest of the internet, the rest of the internet sees only the NAT router with the address 200.24.5.8.

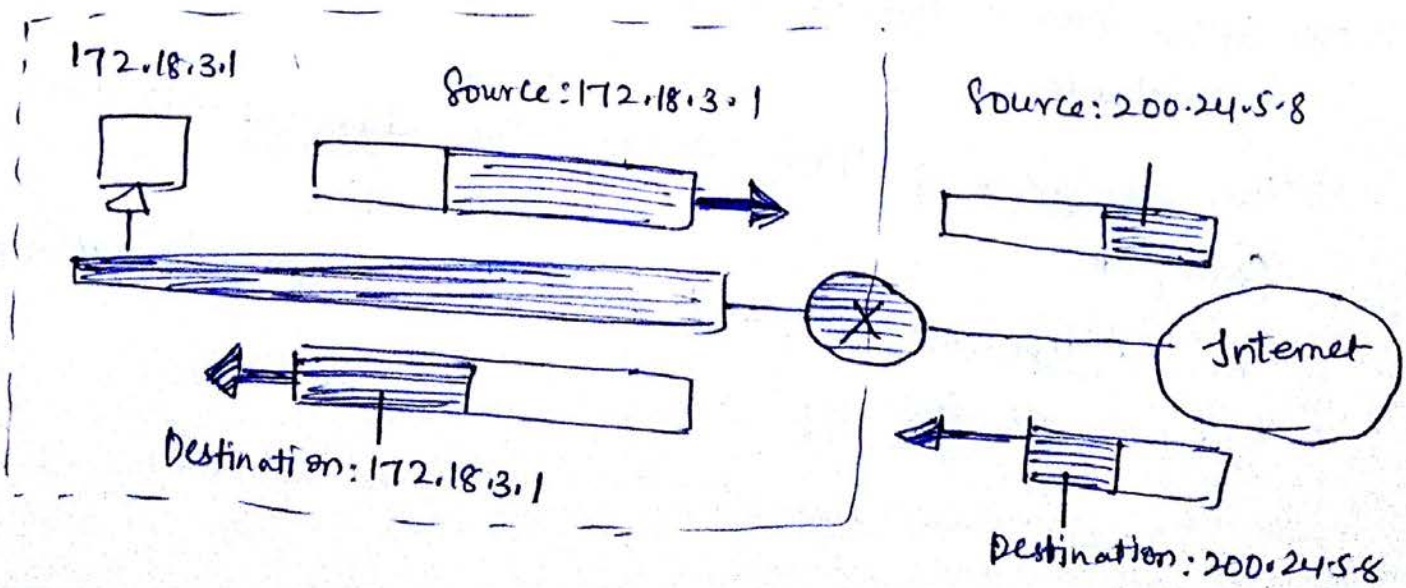
⇒ A NAT implementation



Address Translation:

All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.

⇒ Examples of address Translation:



www.jntuworldupdates.org

IPV6 Addresses:

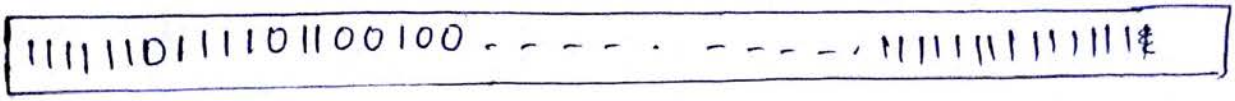
Even though NAT solves the problem of address shortage, it is not a permanent solution.

→ So, another and permanent alternate is extension of IPV4 to IPV6 (IP-Version 6)

→ IPV6 address is 128 bit long (or 16 byte octets)) (16×8=128)

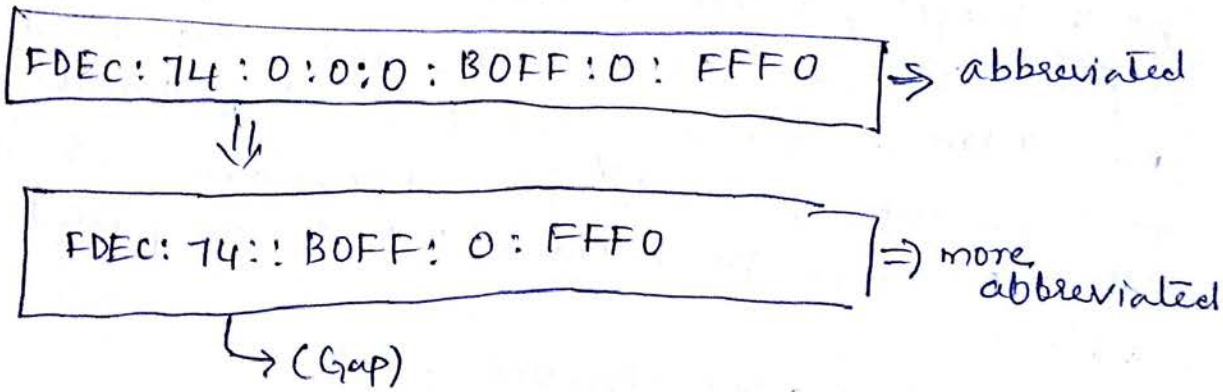
→ IPV6 uses hexa-decimal representation (colon notation)

→ IPV6 binary & hexadecimal colon notation is shown as:



FDEC : 0074 : 0000 : 0006 : 0000 : BOFF : 0000 : FFFF ⇒ original

⇒ This representation can be abbreviated as:



⇒ IPV6 has a much larger address space, 2^{128} addresses available

⇒ The designers of IPV6 divided the addresses into several categories.

⇒ A few leftmost bits, called the type prefix, in each address define its category

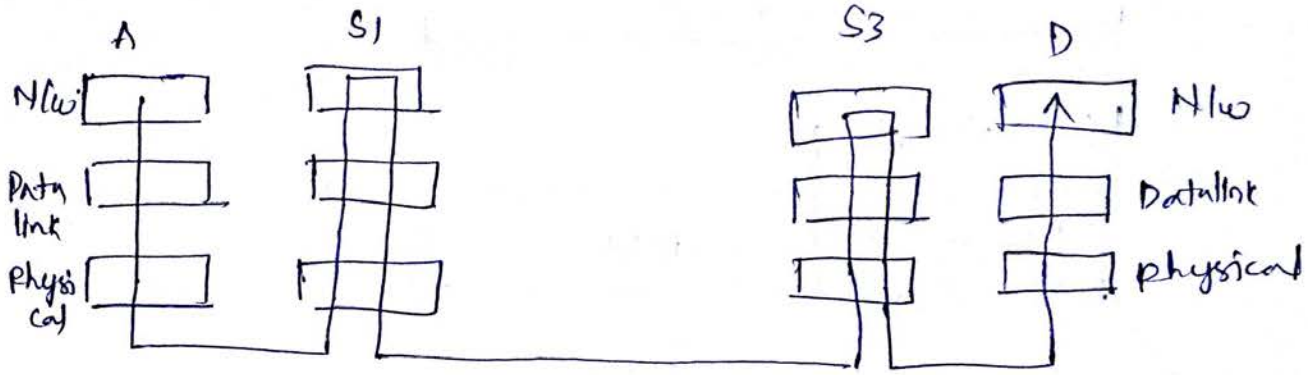
www.smartzworld.com
www.specworld.in

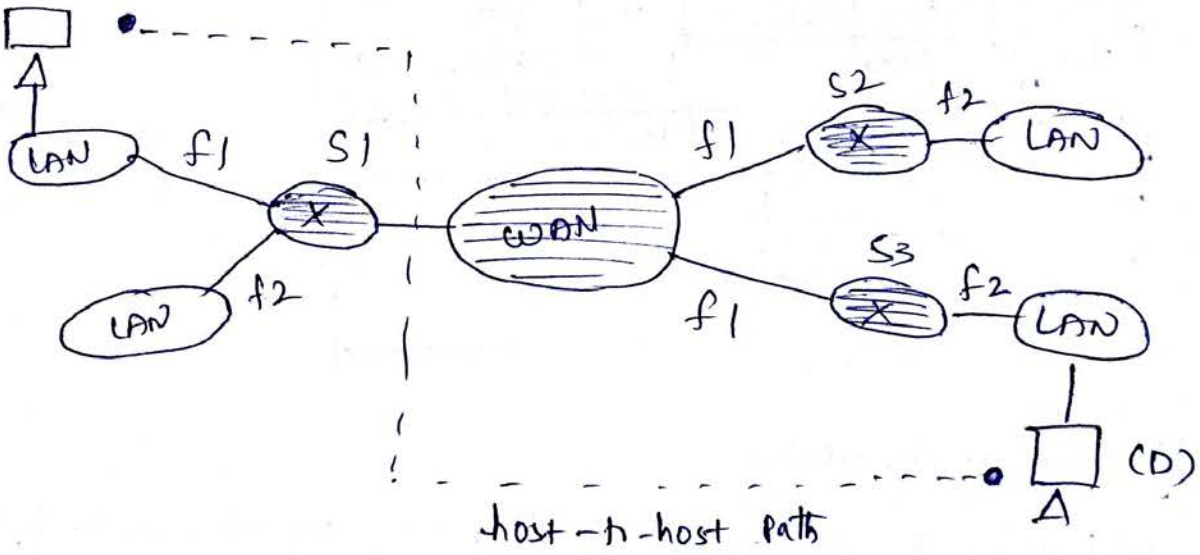
www.jntuworldupdates.org

Inter Networking:

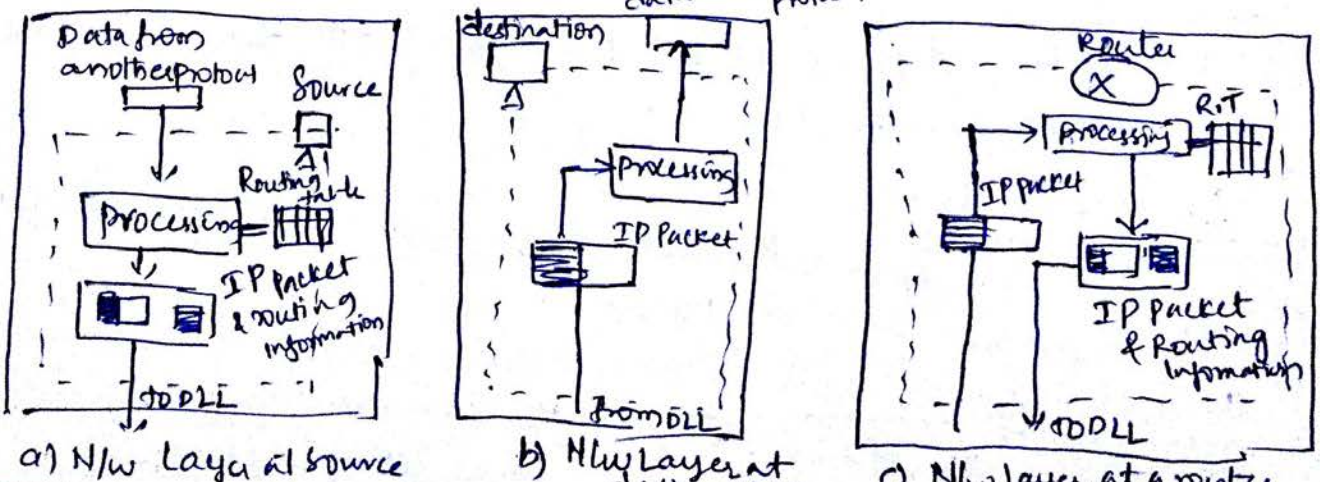
Network layer is responsible for host-to-host communication/delivery. Internetworking routes the packet in the N/w, to the proper destination.

⇒ The following N/w, shows the internetworking using N/w layer.





⇒ N/w layer at the source, router & destination



www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

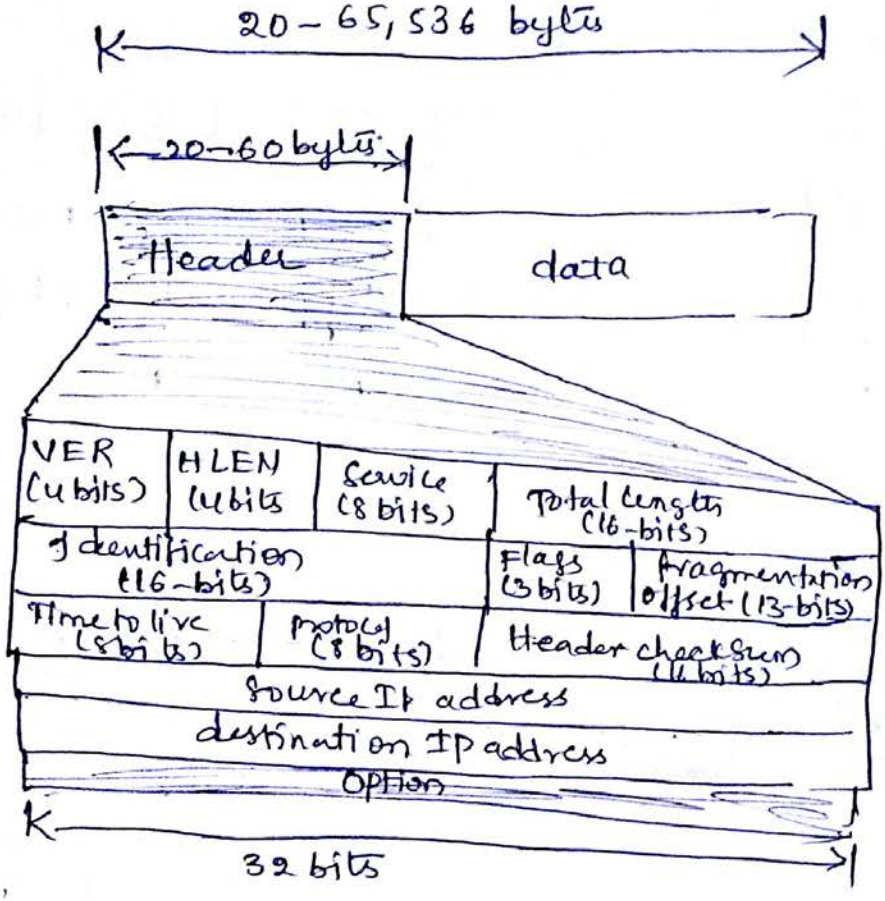
IPV4:

IPV4 is the delivery mechanism used by the TCP/IP protocols

→ IPV4 is used in Nlw Layer.

↳ IPV4 datagram format is shown as:

(Packets in IPV4 layer are called datagrams)



VER (Version): (4bits)

It defines the version of IP, Currently the version is 4.
In future version 6 totally replaces version 4.

HLEN (Header length): (4bits)

The 4-bits defines the total length of the datagram header in 4-byte words (b/w 20-60 bytes)

Service (8 bits)

These bits defines the services & their types. (like delay, throughput, reliability etc.).

Total length (16-bits)

It defines the total length of the datagram including header, (i.e 20-65,536 bytes)

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

Identification (16 bits):
flags (3-bits):
fragmentation offset:
} ⇒ These fields are used for fragmentation. (A datagram can travel through different N/ws, each router decapsulates the IPV4 datagram from the frame it receives, processes it & then encapsulates it in another frame)

Time to live (8-bits):

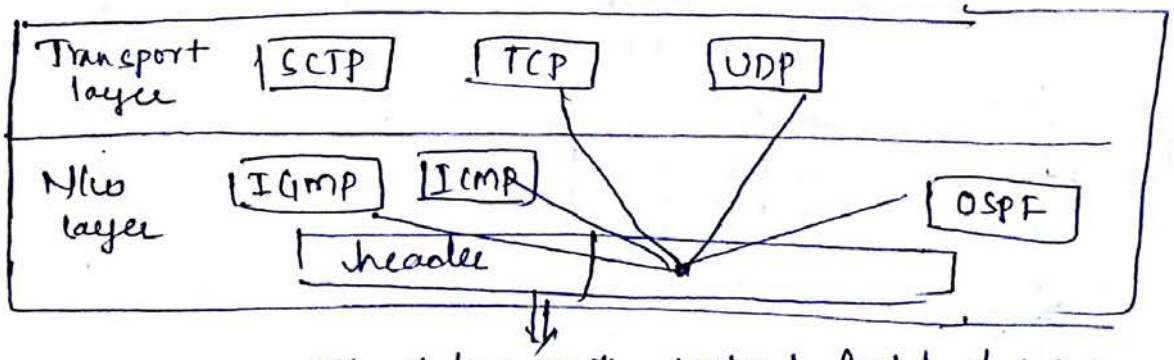
A datagram has a limited lifetime in its travel through an Internet. The datagram is discarded, when the value becomes zero.

protocol (8-bits):

An IPV4 datagram can encapsulate data from several higher-level protocols (such as TCP, VDP, ICMP, IGMP).

i) It defines the higher-level protocol that uses the services of IPV4 layer.

i.e.,



The value of the protocol field defines to which protocol the data belongs.

Checksum: Used for error detection

Source address: (32-bit)

It defines the IPV4 address of the source

destination address: (32-bit)

It defines the IPV4 address of the destination

Options:

It is not compulsory field, they can be used for N/w testing & debugging

www.smartzworld.com
www.specworld.in

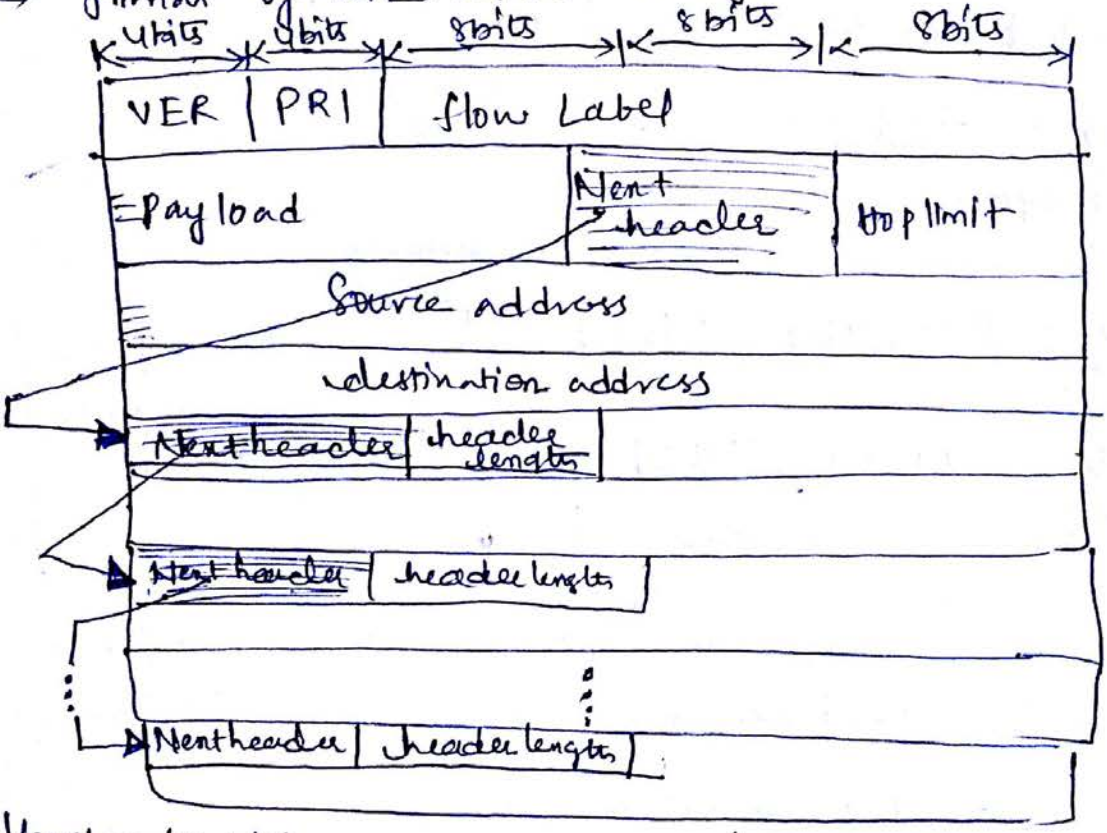
www.jntuworldupdates.org

IPV6: (or) IPng (Internetworking protocol next generation)

To overcome the deficiencies of IPV4, IPV6 is introduced.

Advantages of IPV6 over IPV4 are:

→ Larger address space (128 bits long; i.e 2^{128} address exists)
↳ Better header format
→ New options (additional functionalities)
→ Allowance for extension
→ support for resource allocation
→ support for more security
↳ format of an IPV6 datagram is shown as:



Version (4-bit): The 4 bit field defines the version number of the IP for IPV6, the value is 6.

Priority (4bit): It defines the priority of the packet with respect to traffic congestion.

Flow label: It provides special handling for a particular flow of data.

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

Payload length (2 byte):

The 2-byte payload length field defines the length of the IP-datagram excluding the base header.

Next header:

The next-header is an 8-bit field defining the header that follows the base header in the datagram.

↳ The next header is either one of the optional extension headers used by IP (or) the header of an encapsulated packet such as UDP/IP.

Hop limit:

This 8-bit hop limit field serves the same purpose as the TTL field in IPV4

Source Address:

The source address field is a 16-byte (128 bit) Internet address that identifies the original source of the datagram.

Destination address:

The destination address field is a 16-byte (128 bit) Internet address that usually identifies the final destination of the datagram. However, if source routing is used, this field contains the address of the next router.

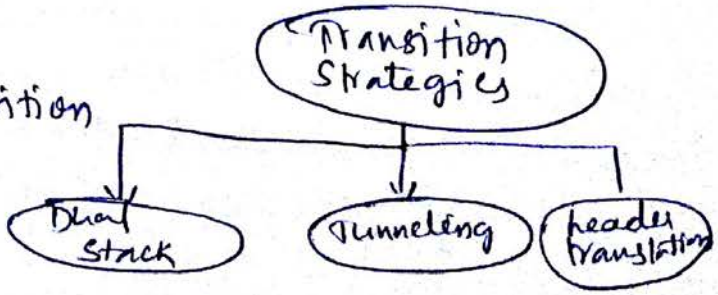
* Transition from IPV4 to IPV6

Because, there are many no. of systems on the Internet, the transition from IPV4 to IPV6 cannot happen suddenly.

→ i.e., it takes some amount of time before every systems in the internet can move from IPV4 to IPV6.

↳ The transition must be smooth to prevent any problems b/w IPV4 to IPV6 systems.

↳ There are three stages (or transition strategies)



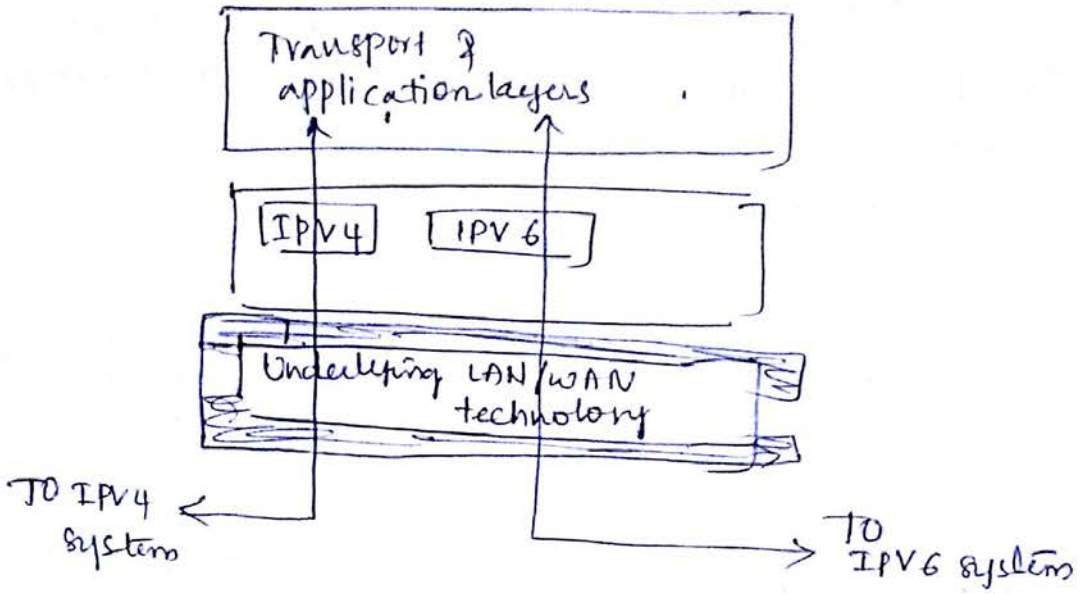
www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

a) Dual stack:

Before migrating completely to version 6, have a dual stack of protocols

→ A station must run IPV4 & IPV6 simultaneously until all the internet uses IPV6



b) Tunneling:

It is a strategy used when two computers using IPV6 wants to communicate with eachother and the packet must pass through a region that uses IPV4

↳ To pass through this region, the packet must have an IPV4 address So, that the IPV6 packet is encapsulated in an IPV4 packet when it enters the region, & it leaves its capsule when it exists the region.

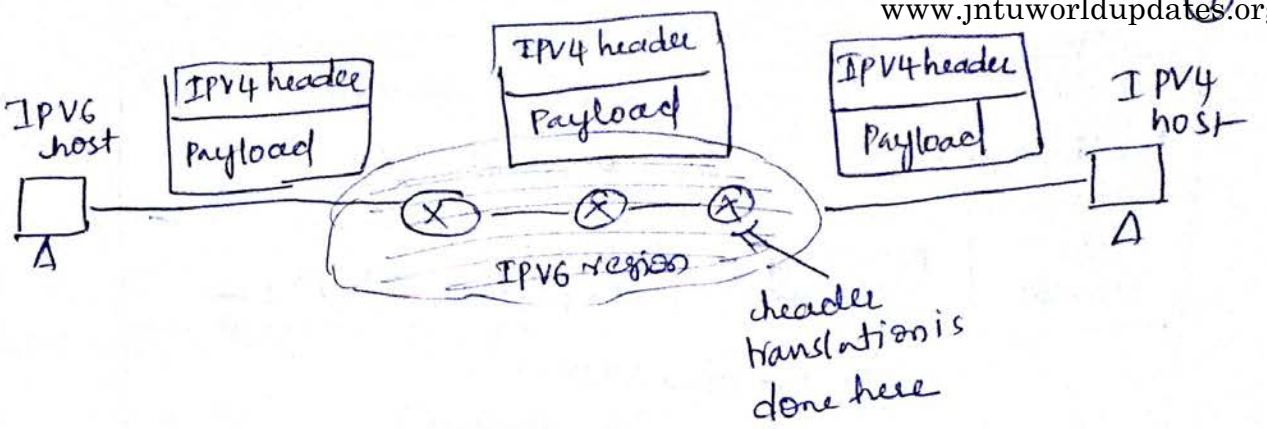
c) Header Translation:

It is necessary when the majority of the internet has moved to IPV6 but some systems still use IPV4. The sender wants to use IPV6, but the receiver doesnot understand IPV6

↳ Tunneling doesnot work in this situation

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org



Address Mapping:

We need some protocols to create a mapping b/w physical & logical addresses.

↳ A N/w is a combination of physical & logical addresses.

physical Layer / datalink layer = MAC addresses / Physical address (frame)

Network layer = logical address (Packet)

↳ There is a need to encapsulate the packet into frame, & vice versa. (where, the packet should be changed into frame, this is done by the ARP (address Resolution protocol) = (logical add) (physical address) packet to frame

RARP (Reverse address Resolution protocol) = frame to Packet (Physical address) (logical address)

⇒ ∴ This concept is known as "Address Mapping".

⇒ Address mapping is of two ways: they are:

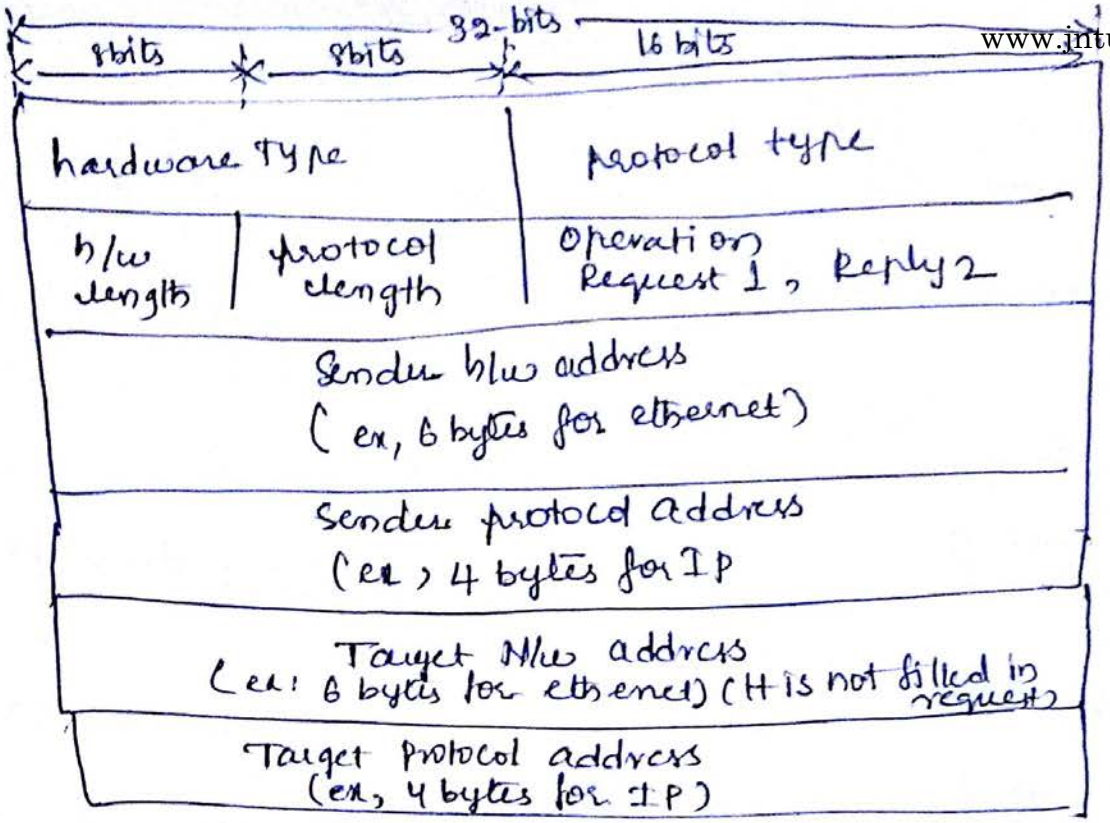
① Mapping logical to physical address (ARP)
② Mapping Physical to logical address (RARP)

① Mapping logical to Physical address (ARP):-

ARP Packet format is shown as:

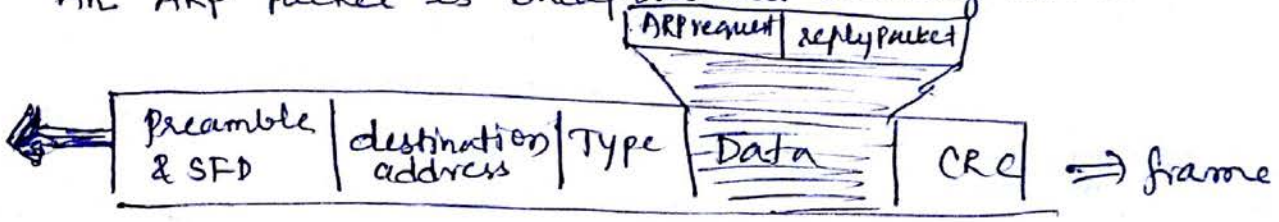
www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org



Encapsulation:

An ARP packet is encapsulated directly into a datalink frame.



② Mapping physical to logical Address (RARP, BOOTP, DHCP)

RARP: RARP finds the logical address for a machine that knows only its physical address.

↳ The IP address of a m/c is usually read from its configuration file stored on a disk file.

↳ For a diskless m/c, it is usually booted from ROM, which has minimum booting information, where as ROM is installed by the manufacturer, so it can't include the IP address because the IP addresses on a N/w are assigned by the Network administrator.

↳ The H/C can get its physical address, by reading its NIC (N/w interface card), which is unique locally and, then we can use the physical address to get logical address by

www.specworld.in

www.jntuworldupdates.org

using the RARP protocol.

↳ RARP request is created & broadcasted on the local N/w. Another M/c on the local N/w that knows all the IP addresses will respond with a RARP reply.

↳ The requesting m/c must be running a RARP client program. The responding m/c must be running a RARP server program.

↳ There is a problem with RARP (Broadcasting is done at the DLL. The physical broadcast address, all 1's in the case of ethernet, doesnot pass the boundaries of a network, i.e., i.e., of an admin has several nkts/several subnets, it needs to assign a RARP server for each nkt/subnet.

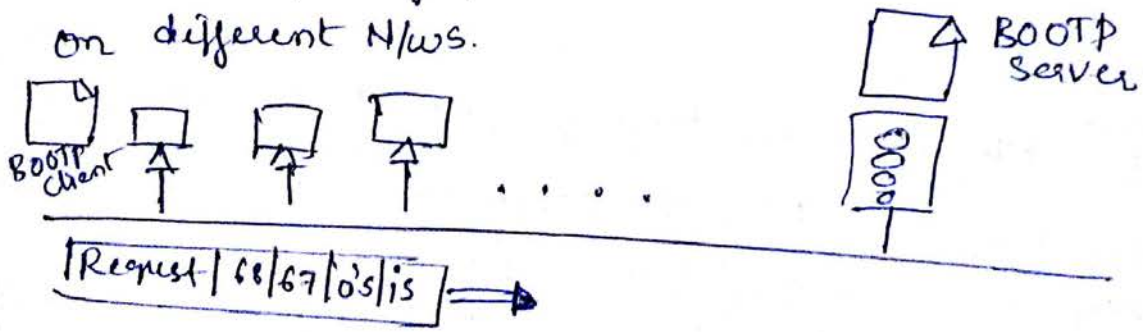
↳ There are two protocols, which replaces RARP, they are BOOTP and DHCP.

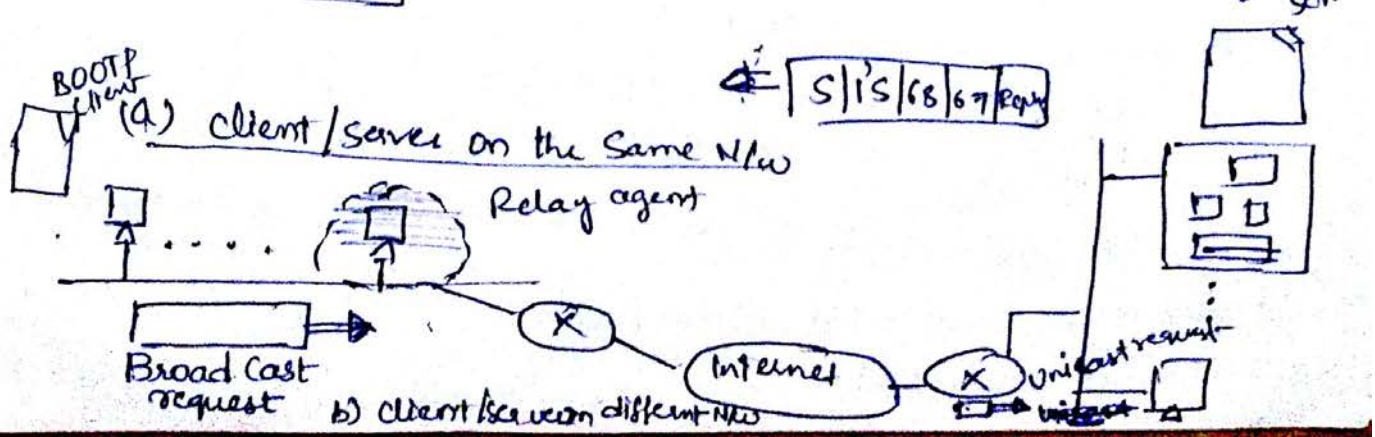
BOOTP (Bootstrap protocol):

It is a client/server protocol, designed to provide physical address to logical address mapping.

↳ BOOTP is an application layer protocol.

↳ The admin, may put the client & the server in the same N/w/ on different N/ws.





www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

↳ One of the advantage of BOOTP over RARP is that the client & Server are application-layer processes. As in other application layer processes, a client can be in one N/w & the server in another, seperated by several other N/w

DHCP (Dynamic host configuration protocol):

BOOTP is not a dynamic configuration protocol, when a client requests its Ip address, the BOOTP server consults a table that matches the physical address of the client with its Ip address i.e the binding b/w physical address & the Ip address of the client already exists i.e, Binding is pre-determined.

↳ consider the situations, If a host moves from one physical N/w to another? what if a host wants a temporary Ip address?

↳ BOOTP can't handle these situations, because binding b/w the physical & Ip address is static & fixed in a table until changed by the administrator.

i.e., BOOTP ~~can't handle these situations, because binding b/w the physical & Ip addresses is static & fixed in~~ is a static configuration protocol

∴ DHCP provides static & dynamic address allocation that can be manual / automatic.

ICMP:

Icmp = Internet control Message protocol.

⇒ Ip provides un-Reliable & connection-less datagram delivery, where it has two deficiencies i.e.,

① lack of error control (no error-reporting & error Correcting)

② lack of assistance mechanisms (lack of mechanism for host & management queries)

Ex: If a host needs to determine if a is alive or not.

↳ So, they designed Icmp protocol, to overcome these two drawbacks.

www.smartzworld.com

www.specworld.in

www.jntuworldupdates.org

Types of messages:

Icmp messages are divided into two categories: They are:

↳ error-reporting messages, and

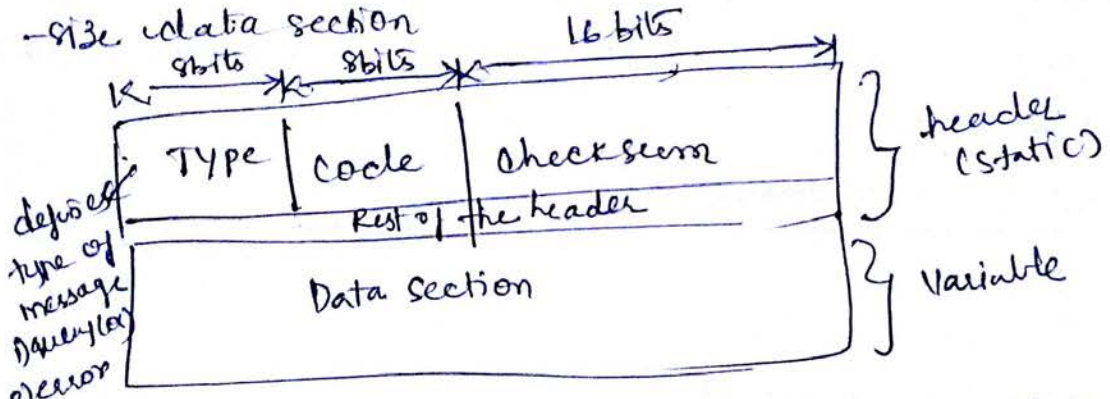
↳ query messages

↳ error reporting messages, report problems that a router/host encounters, when it processes an IP packet.

↳ The query messages, which occur in pairs, help a host/nw manager get specific information from a router/another host.

Message Format:

An Icmp message has an 8-byte header & a variable-size data section



↳ Icmp always reports error messages to the original source

⇒ error-reporting messages are:

- → Destination unreachable (Type-3)
- → Source quench (type-4)
- → Time exceeded (type-11)
- → Parameter problems (type-12)
- → Redirection (type-5)

↳ The following are important points about Icmp error messages:

① NO Icmp error message will be generated in response to a datagram carrying an Icmp error message.

② No Icmp error message will be generated for a fragmented datagram that is not the first fragment.

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

(3) No Icmp error message will be generated for a datagram having a multi-cast address.

(4) No Icmp error message will be generated for a datagram having a special address such as 127.0.0.0 (or) 0.0.0.0

Query Reporting messages are:

- echo request & reply (Type 8 & 0)
- Time Stamp request & reply (Type: 13 & 14)
- Address mask request & reply (Type 17 & 18)
- Router solicitation & advertisement (Type 10 & 9)

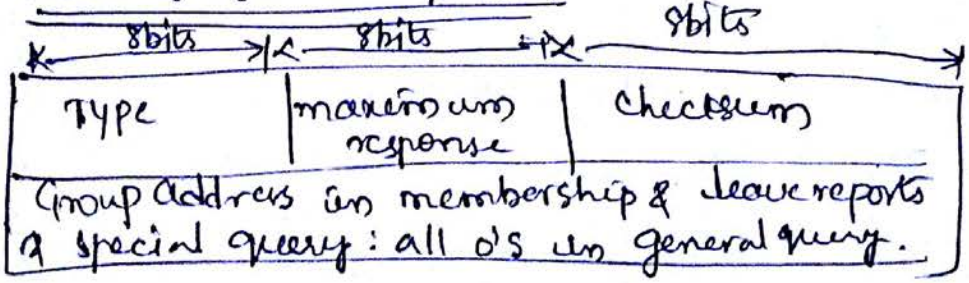
6.6 IGmp (Internet Group Management protocol)

IGmp is a Group management protocol (multicasting)
It helps a multicast router to create & update a list of loyal members related to each router interface.

IGmp messages are:

- General query
- Special query
- membership Report
- leave Report

message format of IGmp is:

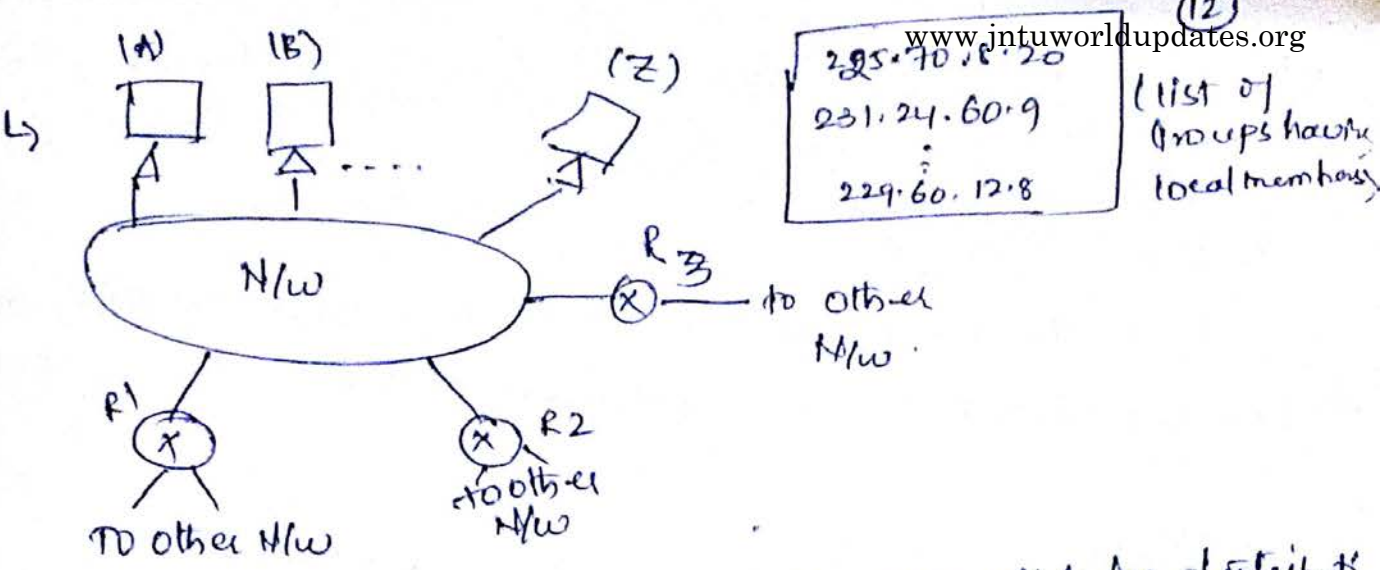


IGmp Operation:

IGmp operates locally: A multicast router is connected to a ~~bracter~~ N/w has a list of multicast addresses of the groups with atleast one loyal member in that N/w

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org



↳ each Group has one router that is responsible for distributing multicast packets, destined for that group.

⇒ Each Group has a Groupid (Unique) & also each host/multicast Router can have membership in a group.

↳ when a host has a membership, it means that a N/w connected to one of its other interfaces receives these multicast packets.

↳ In ICMP, a membership report is sent twice, one after the other.

Delivery, forwarding & Routing:

Delivery: (handling a packet in Nw is delivery)

Delivery refers to a way a packet is handled by the underlying Nw under the control of the N/w layer.

↳ Direct delivery
↳ Indirect delivery.

Direct delivery

The final destination of the packet is a host connected to the same physical Nw as the deliverer.

↳ Direct delivery occurs when the source & destination of the packet are located on the same physical N/w (or)

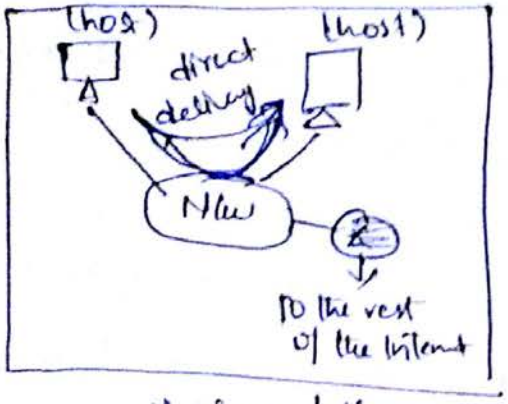
www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

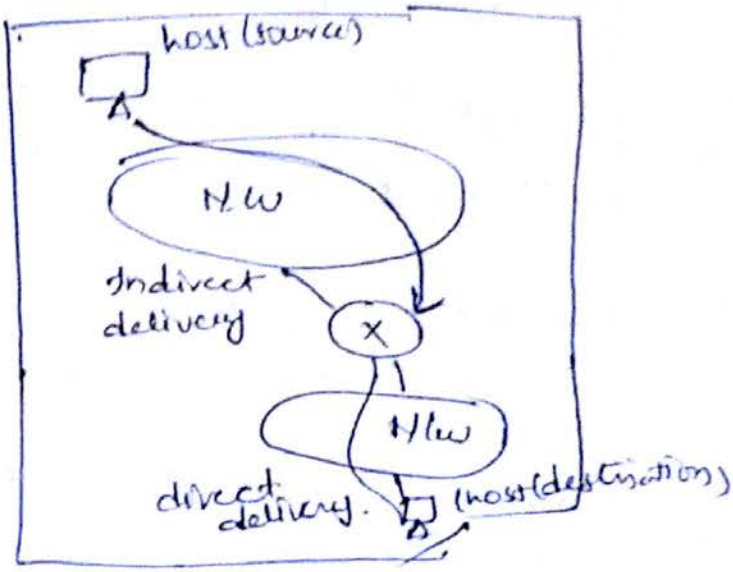
when the delivery is b/w the last router & the destination host.

Indirect Delivery:

Here, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.



a) Direct delivery



b) Indirect delivery

↳ Delivery always involves one direct delivery zero/more indirect deliveries, and also that the last delivery is always a direct delivery.

Forwarding

It refers to the way, a packet is delivered to the next station. forwarding ~~station~~ means to place the packet in its route to its destination.

↳ forwarding requires routing table for each host/router.

↳ when a host, has a packet to send (or)
when a router, has received a packet to be forwarded, it looks at this table to find the route to the final destination.

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

↳ forwarding techniques are:

① Next-hop method Vs Route method

② Network specific method Vs Host-specific method.

① Next-hop method Vs Route method

↳ One technique to reduce the contents of a routing table is called the Next-hop method.

↳ In this technique, the routing table holds only the address of the Next-hop instead of information about the complete route (route method).

↳ The entries of a routing table must be consistent with one another.

↳ The following figure shows, how routing tables can be simplified by using this technique.

(a) Routing table based on route

b) Routing table based on next hop

destination	Route
Host B	R_1, R_2, Host B

Rt for A

destination	Route
Host B	R_1

destination	Route
Host B	R_2, host B

Rt for R

destination	Route
Host B	R_2

destination	Route
Host B	Host B

Rt for R2

destination	Route
Host B	— —

Rt → Routing table

www.smartzworld.com
www.specworld.in

www.jntuworldupdates.org

2) Nlw Specific Vs' Host-specific method:

It also reduces the routing table & simplifies the searching process.

↳ Here, instead of having an entry for every destination host connected to the same physical Nlw (host-specific method), we have only one entry that defines the address of the destination Nlw itself.

i.e all the hosts connected to the same Nlw, are treated as one single entity.

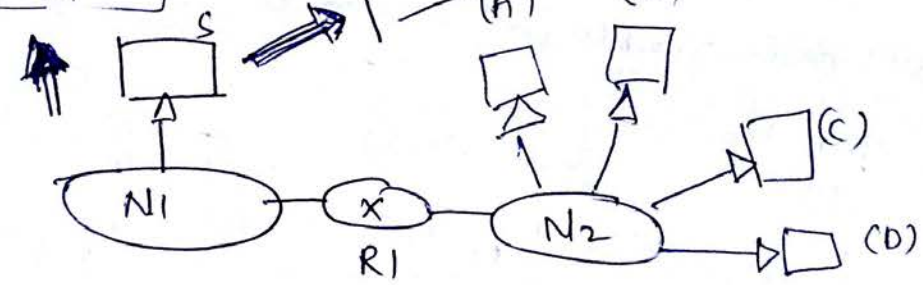
Ex: If 1000 hosts are attached to the same N/w, only one entry exists in the routing table instead of 1000.

destination	Next hop
A	R1
B	R1
C	R1
D	R1

(Routing table for hosts, based on host-specific method)

destination	Next hop
N2	R1

(Routing table for hosts, based on Nlw specific method)



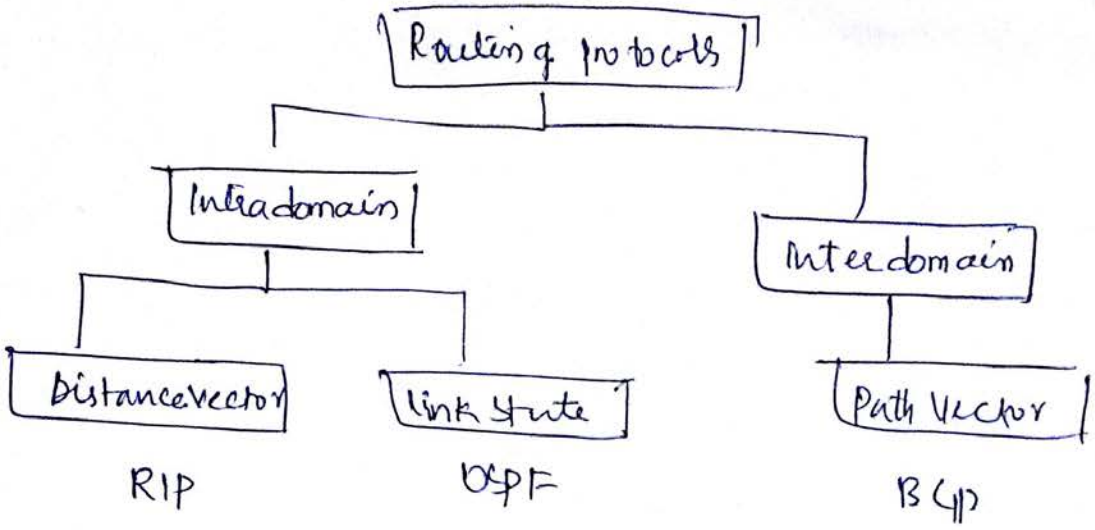
Routing

It refers to the way routing tables created to help in forwarding

1. Uni-cast Routing protocol
2. multi-cast Routing protocol
3. Broad-cast Routing protocol.

www.smartzworld.com
www.specworld.in

Unicast Routing protocols



Multicast Routing protocols