CHAPTER -4

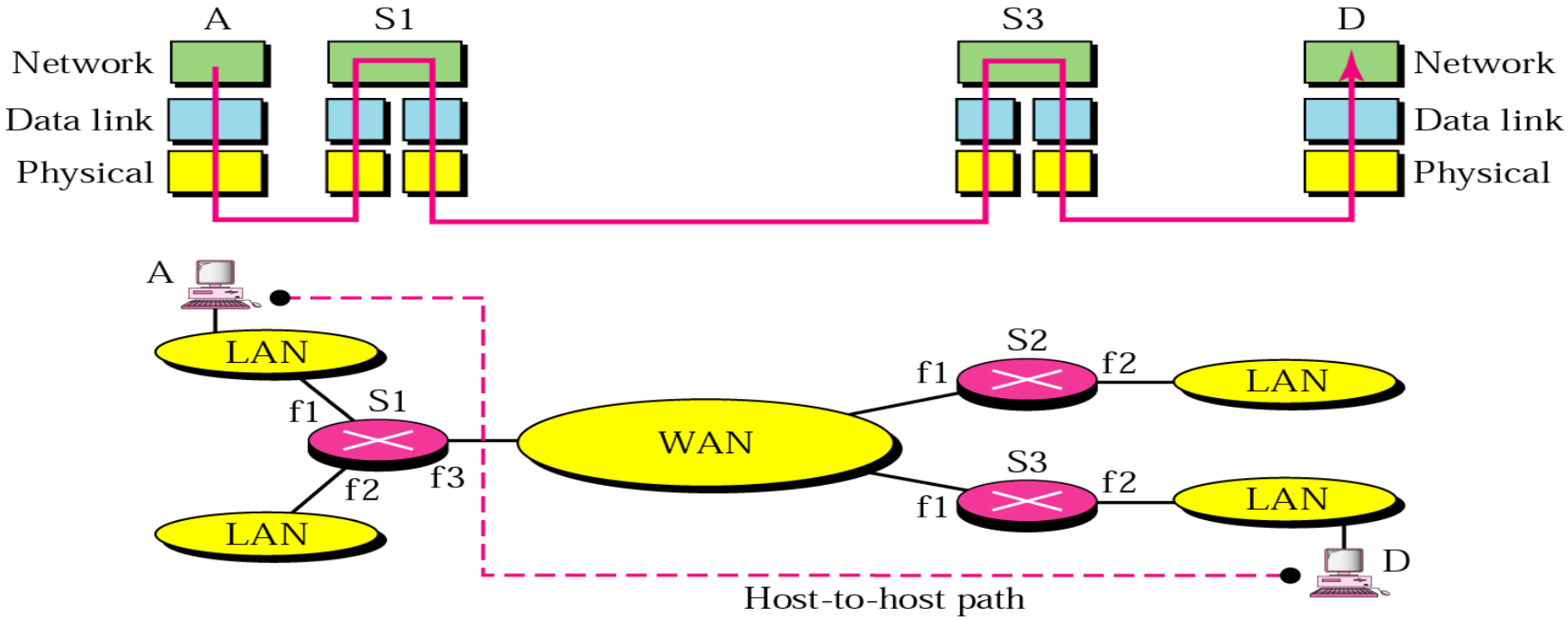
Network Layer

By: Asst. Prof. Sanjivan Satyal

4.1 Introduction

Internetwork

- The process of interconnecting a set of independent networks called internetworking.



Internetworking Devices

- Internetworking devices are considered as a active components because they do more than just simply passing data across a network.
- They make intelligent decision and may direct data in an appropriate path.
- List of some internetworking devices are:
  - Switch
  - Bridge
  - Router
  - Bridges
  - gateways

Connecting devices and OSI model

Application Layer	Gateway	Application Layer
Presentation Layer		Presentation Layer
Session Layer		Session Layer
Transport Layer		Transport Layer
Network Layer	Router	Network Layer
Data Link Layer	Switch/Bridge	Data Link Layer
Physical Layer	Repeater/ Hub	Physical Layer

Network Layer

- It is responsible for the source to destination delivery of a packet across multiple networks.

- If two systems are attached to different networks with devices like routers, then N/W layer is used. Thus DLL overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.

4.1Network Layer Function

1. **Internetworking:** It provides Internetworking.

2. **Logical Addressing:** When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet.

   Network addresses are assigned to local devices by n/w administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol)

3. **Routing:** When independent n/w are connected to create internetwork several routes are available to send the data from S to D. These n/w are interconnected by routers & gateways that route the packet to final destination.

Need for Network layer

- The network layer is responsible for host-to-host delivery
- Routing the packets through the routers or switches
- The network layer at the source is responsible for creating a packet from the data coming from another protocol
- The network layer is responsible for checking its routing table to find the routing information

4.2 IP Address v4

• An IPv4 address is 32 bits long. The IPv4 addresses are unique and universal

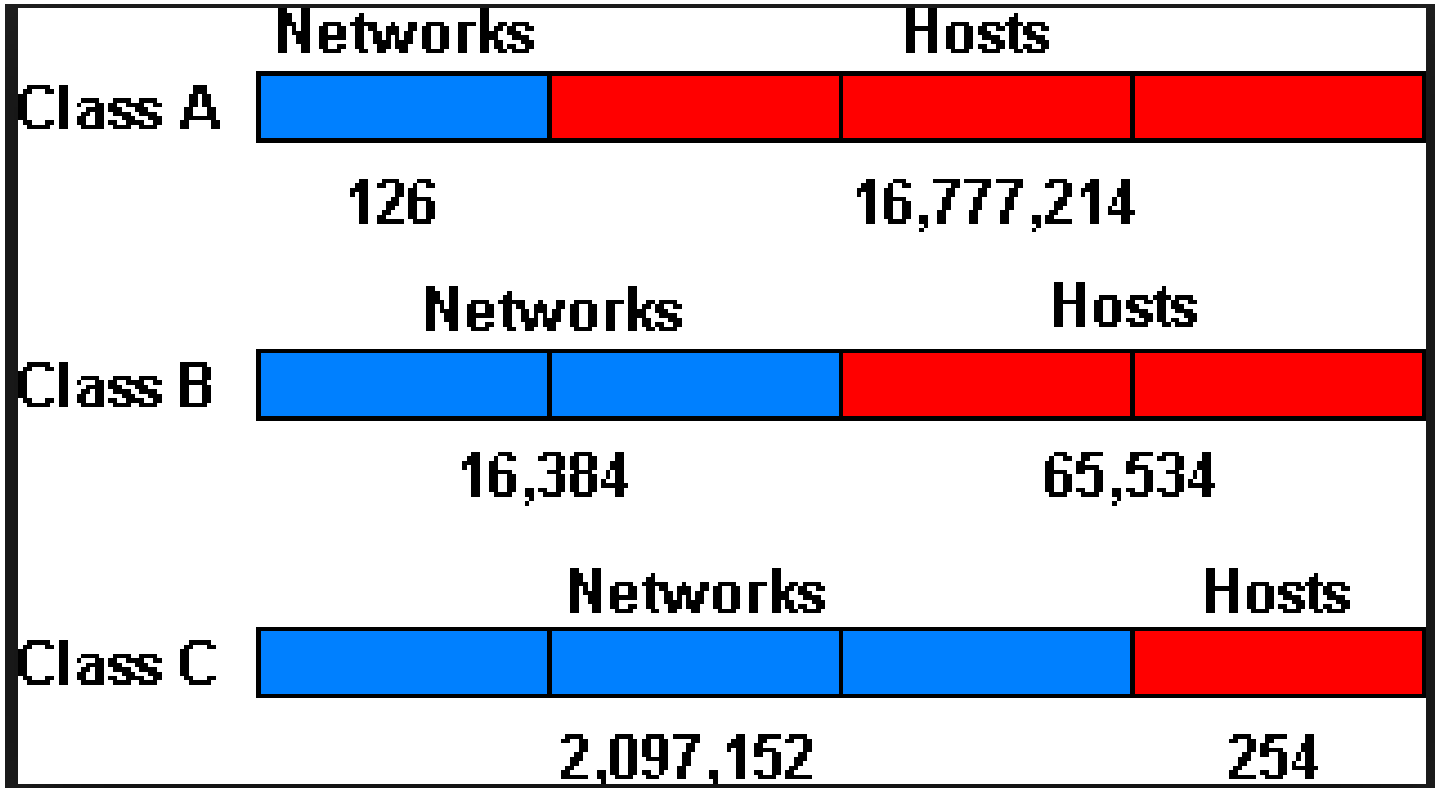
• IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296(Maximum available theoretically)

• IPv4 have 2 types of notations:

1. Doted decimal
   Denoted in decimal format each byte is separated by dot eg: 117.149.29.2
   Mostly used by human configurations
2. 2. Binary notation
   In binary format e.g: 01110101 10010101 00011101 00000010
   Mostly used by devices for processing

Net id & Host ID

- **Class A** :- first byte net-id and last 3 bytes host-id (N.H.H.H)
- **Class B** :- first 2 bytes net-id and last 2 bytes host-id (N.N.H.H)
- **Class C** :- first 3 bytes net-id and last byte host-id (N.N.N.H)
- Subnet mask helps to identify net-id and host-id
- CIDR value is total number of network bits in sub-netmask


Networks
Hosts
Class A
126
16,777,214
Networks
Hosts
Class B
16,384
65,534
Networks
Hosts
Class C
2,097,152
254

Types of IP address

- Public IP
  - Number used in Internet
  - Unique world wide
  - Given by ISP
- Private IP
  - IP that cannot be used in Internet
  - Free to use
  - Used in LAN
  - Any organization can use an address out of this set without permission from the Internet authorities

Subnet Mask and CIDR in Classful IPv4

- The mask can help us to find the netid and the hostid
  - *For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.*
- CIDR value is number I's (ones) in the subnet mask(network bits), usually for class A,B,C CIDR values will be 8,16,24 respectively

Given below table shows various subnet mask, CIDR values of class A,B,C

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*

Default mask

- Default mask for classful address

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

- In IPv4 addressing, a block of addresses can be defined as x.y.z.t /*n* in which x.y.z.t defines one of the addresses and the /*n* defines the mask.

Address Depletion Problem in Internet

- Because of limited number of IP and increasing demand of IP in internet over years lead to depletion of IP address

Solution of depletion are mainly

1. NAT
2. Sub netting
3. IPv6

Network Address Translation(NAT)

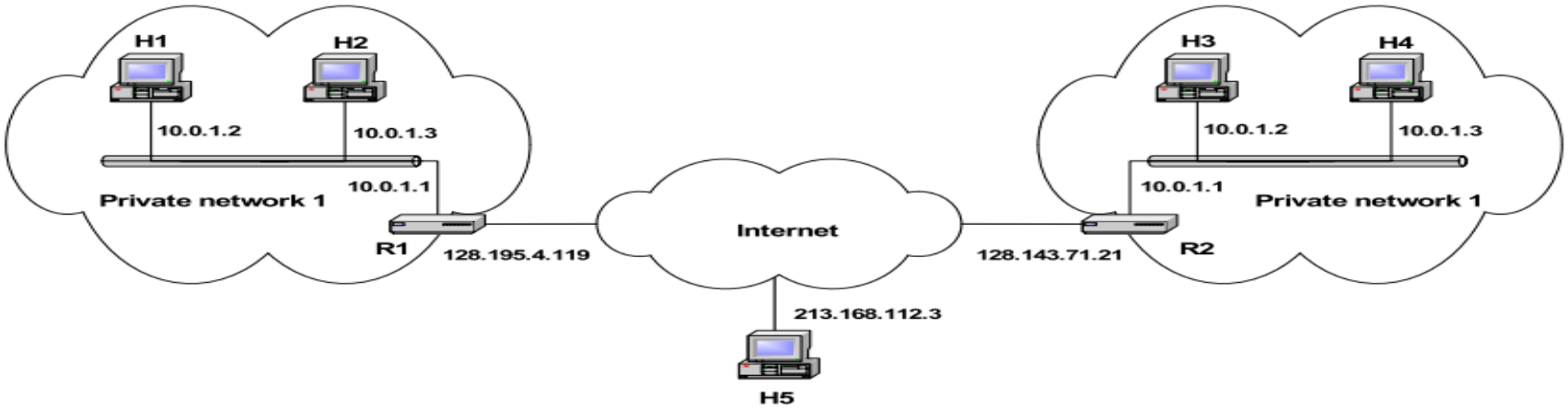
- IP address have public range and private range
- Public range is used for communication in internet and can used only with permission of internet authorities
- Private IP can be used for local communication without permission of Internet authorities

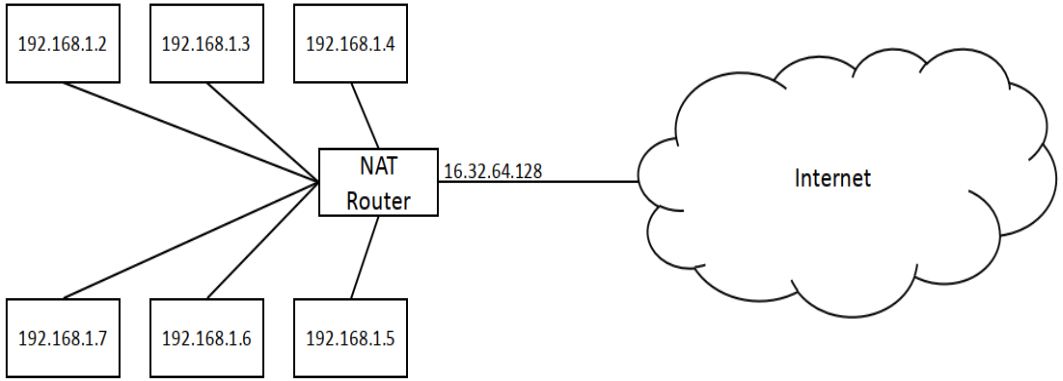
Given below table shows private ranges of class A,B,C

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	192.168.255.255	2^{16}

Network Address Translation(NAT)…

- Public IP should be unique globally
- Private IP should be unique inside a organization, not globally
- NAT router consist of public IP in exit interface and internal interface consist of Private IPs





- Address Translation : Replace outgoing packets Source IP address as NAT router public IP and replaces incoming packet Destination IP with private (Private to public and public to private)
- Translation is done with help of translation table which consist of IP address of private range and public range and port address

Below table showing Translation table in NAT

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
.. .	.. .	. ..	.. .	...

Subnetting

- Subnetting means creating sub-network
- Subnetting means increasing networks bits(i.e. 1s) in subnet mask
- If network bit is increased host bits will be decreased, so number of host will be decreased
- A Class A network have 8 bits for network (2^{24}IP address available) if you wanted smaller block IP from class A increase the network bits / decreasing host bits

Supernetting

- Supernetting means creating bigger network from smaller one
- Supernetting means decreasing networks bits(i.e. 1s) in subnet mask
- If network bit is decreased host bits will be increased, so number of host will be decreased
- A Class C network have 24 bits for network (2^8IP address available) if you wanted bigger block IP from class C decrease the network bits / increasing host bits
- Supernetting just opposite of subnetting

VLSM (Variable Length Subnet Mask)

- Subnetting and supernetting is achieved by varying default subnet mask

- Usually in classful IP address have 8,16,24 default CIDR values for Class A, B, C respectively, but in classless IP no default CIDR value / subnet mask is available CIDR value may be varying

Subnetting/supernetting Steps

- Identify needed block size (always in power of 2 i.e. 2^2, 2^3, 2^4, …2^{31})
- If multiple block size is needed assign largest block first
- Find the host bits from block size (if block size 2^n no of host bit is n)
- From host bits find the CIDR (CIDR=32-n)
- Find subnet mask convert CIDR into doted decimal format (ex:255.255.240.0)
- Find wild card mask (255.255.255.255 - 255.255.240.0= 0.0.15.255)
- Add the first IP in the range to get last IP address