

CS3102 - Computer Networks

Mallikarjuna Nandi
Assistant Professor
Computer Science & Engineering
RGUKT- Ongole-AP

Unit 3- Syllabus

Unit - III

(8 Contact hours)

The Network Layer: Network Layer Design Issues, Routing Algorithms, Congestion Control Algorithms. Internetworking, subnetting, The Network Layer in the Internet.

The Network Layer

Introduction :

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

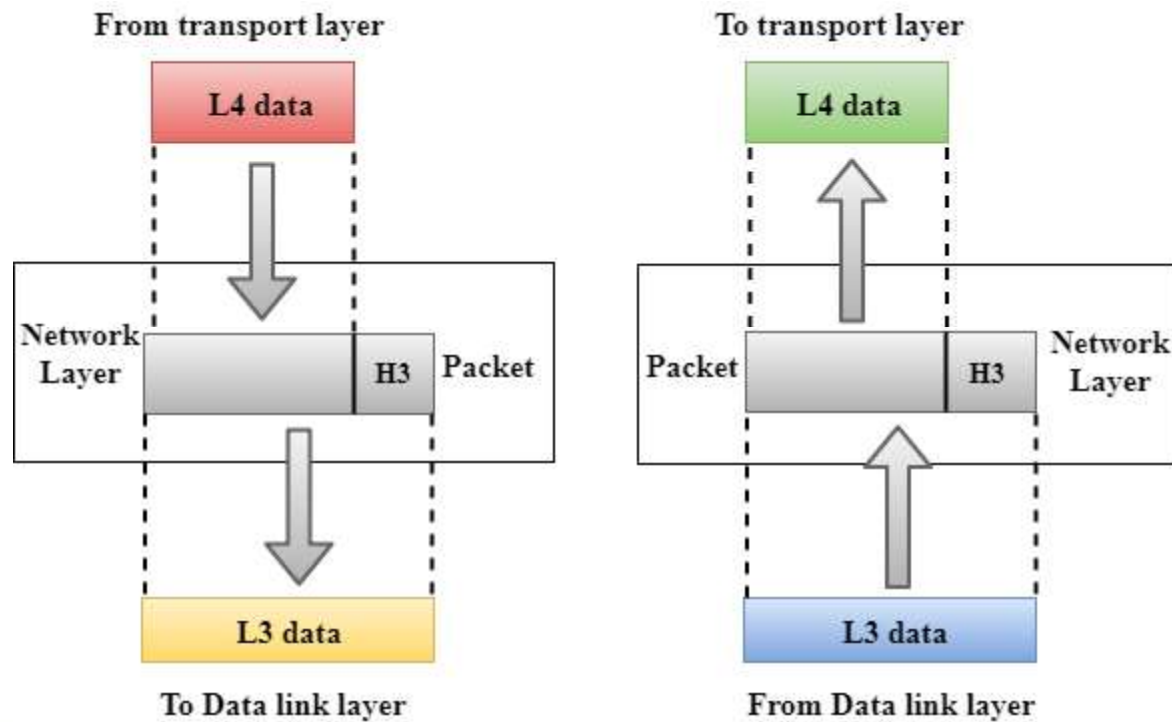
The Network Layer

Introduction : The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

The Network Layer

Introduction :



The Network Layer

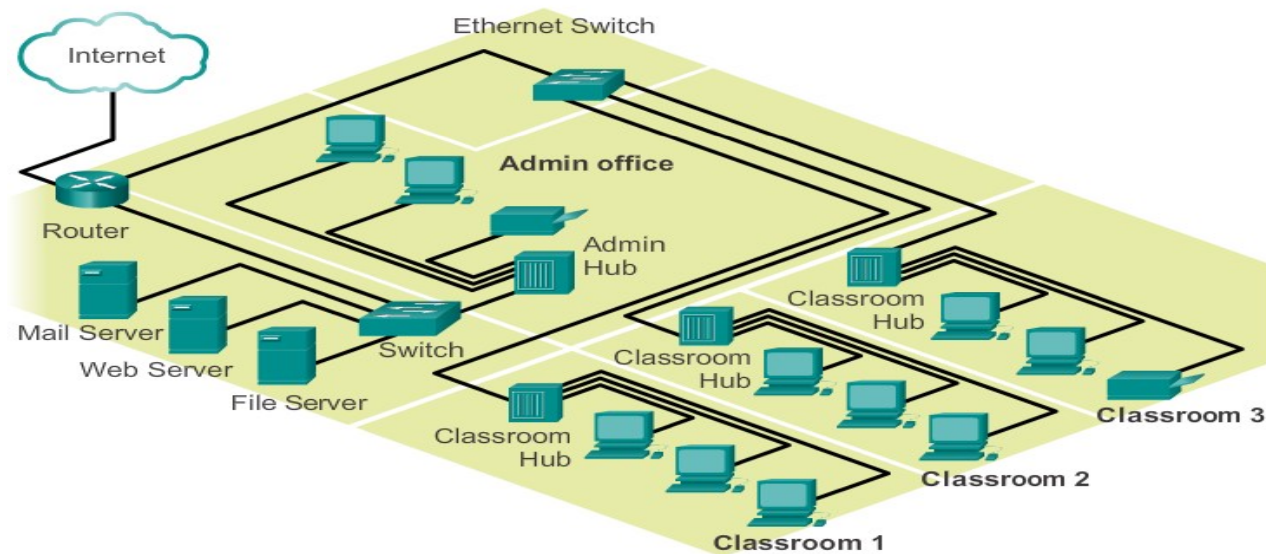
Network Layer Design Issues :

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Topologies

Physical and Logical Topologies

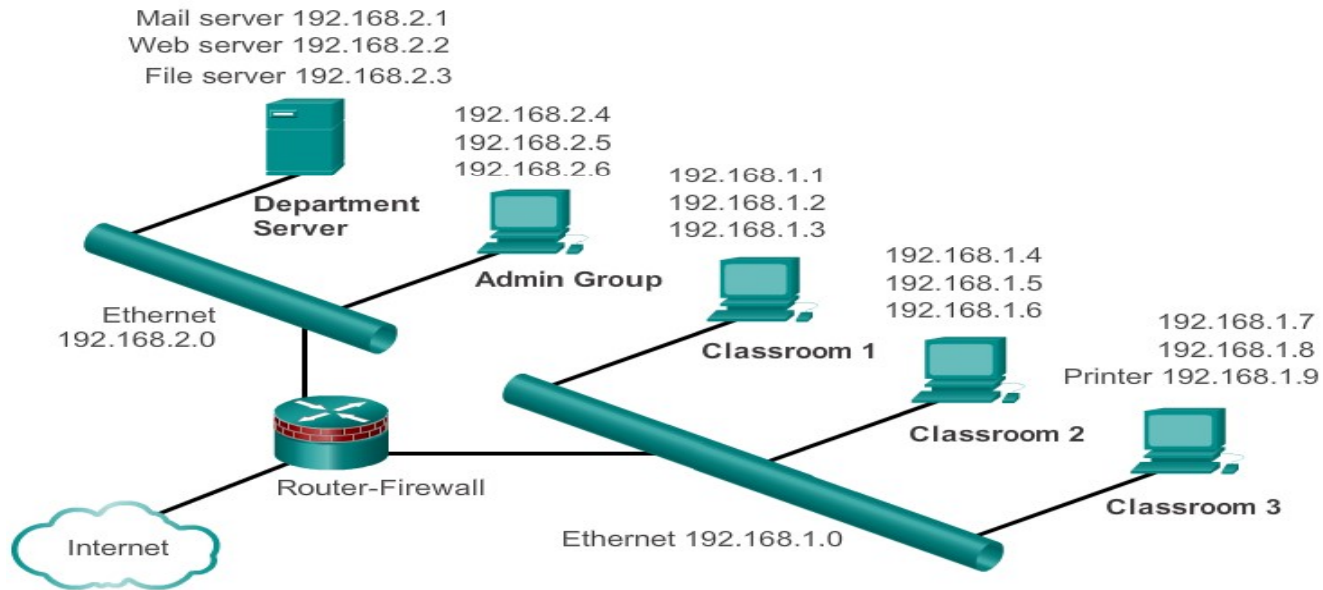
Physical Topology



Topologies

Physical and Logical Topologies (cont.)

Logical Topology



The Network Layer

Addressing :

The Network Layer

Internetworking and Addressing

The Network Layer

Addressing :

- **IP Addressing is Logical Addressing**
- **It works on Network Layer (Layer 3)**
- **Two Versions of Addressing Scheme**
 - ❖ **IP version 4 – 32 bit addressing**
 - ❖ **IP version 6 – 128 bit addressing**

The Network Layer

Introduction :

Bit is a value that will represent 0's or 1's (i.e. Binary)

01010101000001011011111100000001

- **32 bits are divided into 4 Octets known as Dotted Decimal Notation**

First Octet	Second Octet	Third Octet	Forth Octet
01010101.	00000101.	10111111.	00000001

The Network Layer

Addressing :

- **128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons (Colon-Hex Notation)**

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

The Network Layer

Addressing : Taking Example for First Octet :

Total 8 bits, Value will be 0's and 1's

i.e. $2^8 = 256$ combination

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0
0	0	0	0	0	0	0	1	= 1
0	0	0	0	0	0	1	0	= 2
0	0	0	0	0	0	1	1	= 3
0	0	0	0	0	1	0	0	= 4

1 1 1 1 1 1 1 1 = 255

Total IP Address Range

0 . 0 . 0 . 0

to

255.255.255.255

The Network Layer

Addressing • **Total IP Addressing Scheme is divided into 5 Classes**

- **CLASS A**
 - **CLASS B**
 - **CLASS C**
 - **CLASS D**
 - **CLASS E**
- LAN & WAN**
- Multicasting**
- Research & Development**

The Network Layer

- To identify the range of each class a bit called priority bit is used.
- Priority Bit is the left most bits in the First Octet
- CLASS A priority bit is **0**
- CLASS B priority bit is **10**
- CLASS C priority bit is **110**
- CLASS D priority bit is **1110**
- CLASS E priority bit is **1111**

The Network Layer

Addressing : For Class A range : First bit of the first octet should be reserved for the priority bit.

0xxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

0 0 0 0 0 0 0 0 = 0

0 0 0 0 0 0 0 1 = 1

0 0 0 0 0 0 1 0 = 2

0 0 0 0 0 0 1 1 = 3

0 0 0 0 0 1 0 0 = 4

0 1 1 1 1 1 1 1 = 127

Class A Range

0 . 0 . 0 . 0 to
127.255.255.255

Exception

0.X.X.X and 127.X.X.X
network are
reserved

The Network Layer

For Class B range : First two bits of the first octet should be reserved for the priority bit.

10xxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

1 0 0 0 0 0 0 0 = 128

1 0 0 0 0 0 0 1 = 129

1 0 0 0 0 0 1 0 = 130

1 0 0 0 0 0 1 1 = 131

1 0 0 0 0 1 0 0 = 132

1 0 1 1 1 1 1 1 = 191

Class B Range

128. 0 . 0 . 0

to

191.255.255.255

The Network Layer

For Class C range : First Three bits of the first octet should be reserved for the priority bit.

110xxxxx. xxxxxxxxxx. xxxxxxxxxx. xxxxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

1 1 0 0 0 0 0 0 = 192

1 1 0 0 0 0 0 1 = 193

1 1 0 0 0 0 1 0 = 194

1 1 0 0 0 0 1 1 = 195

1 1 0 0 0 1 0 0 = 196

1 1 0 1 1 1 1 1 = 223

Class C Range

192. 0 . 0 . 0

to

223.255.255.255

The Network Layer

For Class D range : First four bits of the first octet should be reserved for the priority bit.

1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

1 1 1 0 0 0 0 0 = 224

1 1 1 0 0 0 0 1 = 225

1 1 1 0 0 0 1 0 = 226

1 1 1 0 0 0 1 1 = 227

1 1 1 0 0 1 0 0 = 228

1 1 1 0 1 1 1 1 = 239

Class D Range

224. 0 . 0 . 0

to

239.255.255.255

The Network Layer

For Class E range : First four bits of the first octet should be reserved for the priority bit.

1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

1	1	1	1	0	0	0	0	= 240
1	1	1	1	0	0	0	1	= 241
1	1	1	1	0	0	1	0	= 242
1	1	1	1	0	0	1	1	= 243
1	1	1	1	0	1	0	0	= 244

1 1 1 1 1 1 1 1 = 255

Class E Range
240. 0 . 0 . 0
to
255.255.255.255

The Network Layer

Addressing :

- **IP address is divided into Network & Host Portion**
- **CLASS A is written as** **N.H.H.H**
- **CLASS B is written as** **N.N.H.H**
- **CLASS C is written as** **N.N.N.H**

The Network Layer

- Class A Octet Format is **N.H.H.H**
- **Network bits : 8** **Host bits : 24**

- **No. of Networks**

$$\begin{aligned} &= 2^{8-1} \quad (-1 \text{ is Priority Bit for Class A}) \\ &= 2^7 \\ &= 128 - 2 \quad (-2 \text{ is for } 0 \text{ \& } 127) \\ &= 126 \text{ Networks} \end{aligned}$$

- **No. of Host**

$$\begin{aligned} &= 2^{24} - 2 \quad (-2 \text{ is for Network ID \& Broadcast ID}) \\ &= 16777216 - 2 \\ &= 16777214 \text{ Hosts/Network} \end{aligned}$$

CLASS A
126 Networks
&
16777214
Hosts/Nw

The Network Layer

- Class B Octet Format is **N.N.H.H**
- **Network bits : 16** **Host bits : 16**
- **No. of Networks**
 - = 2^{16-2} **(-2 is Priority Bit for Class B)**
 - = 2^{14}
 - = **16384 Networks**

- **No. of Host**
 - = $2^{16} - 2$ **(-2 is for Network)**
 - = **65536 - 2**
 - = **65534 Hosts/Network**

CLASS B
16384 Networks
&
65534 Hosts/Nw

The Network Layer

- **Class C Octet Format is N.N.N.H**
- **Network bits : 24** **Host bits : 8**
- **No. of Networks**
 - = 2^{24-3} **(-3 is Priority Bit for Class C)**
 - = 2^{21}
 - = **2097152 Networks**
- **No. of Host**
 - = $2^8 - 2$ **(-2 is for Network)**
 - = $256 - 2$
 - = **254 Hosts/Network**

CLASS C
2097152 Networks
&
254 Hosts/Nw

The Network Layer

Addressing :

- **The network address** is represented with all bits as **ZERO** in the host portion of the address
- **The broadcast address** is represented with all bits as **ONES** in the host portion of the address
- **Valid IP Addresses lie between the Network Address and the Broadcast Address.**
- **Only Valid IP Addresses are assigned to hosts/clients**

The Network Layer

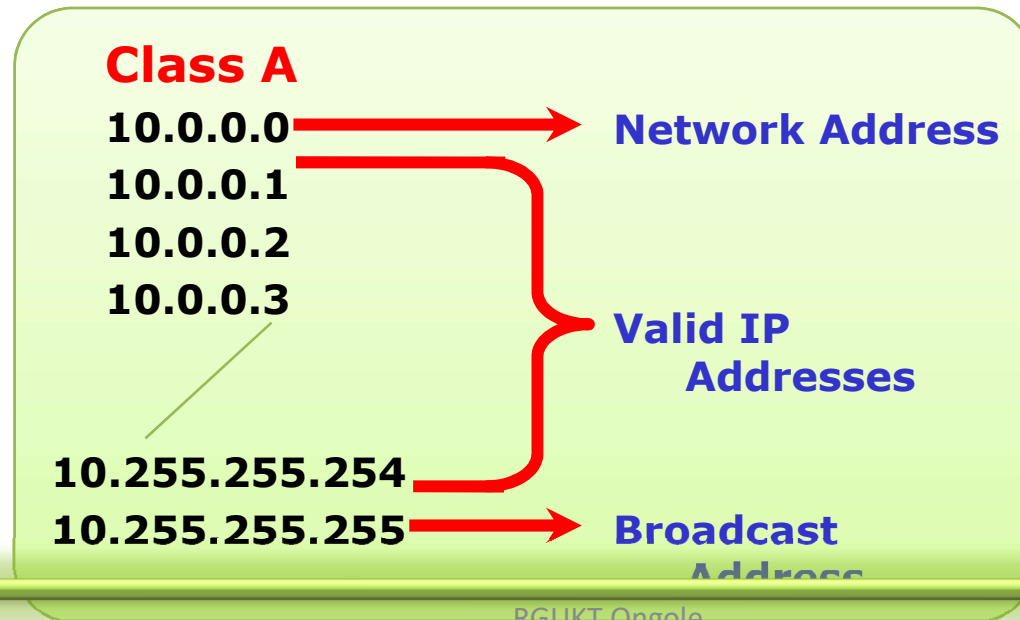
Class A : N.H.H.H

Network Address :

0xxxxxxx.00000000.00000000.00000000

Broadcast Address :

0xxxxxxx.11111111.11111111.11111111



The Network Layer

Class B : **N.N.H.H**

Network Address :

10xxxxx.xxxxxxx.00000000.00000000

Broadcast Address :

10xxxxx.xxxxxxx.11111111.11111111

Class B

172.16.0.0

172.16.0.1

172.16.0.2

172.16.0.3

172.16.255.254

172.16.255.255

Network Address

**Valid IP
Addresses**

**Broadcast
Address**

The Network Layer

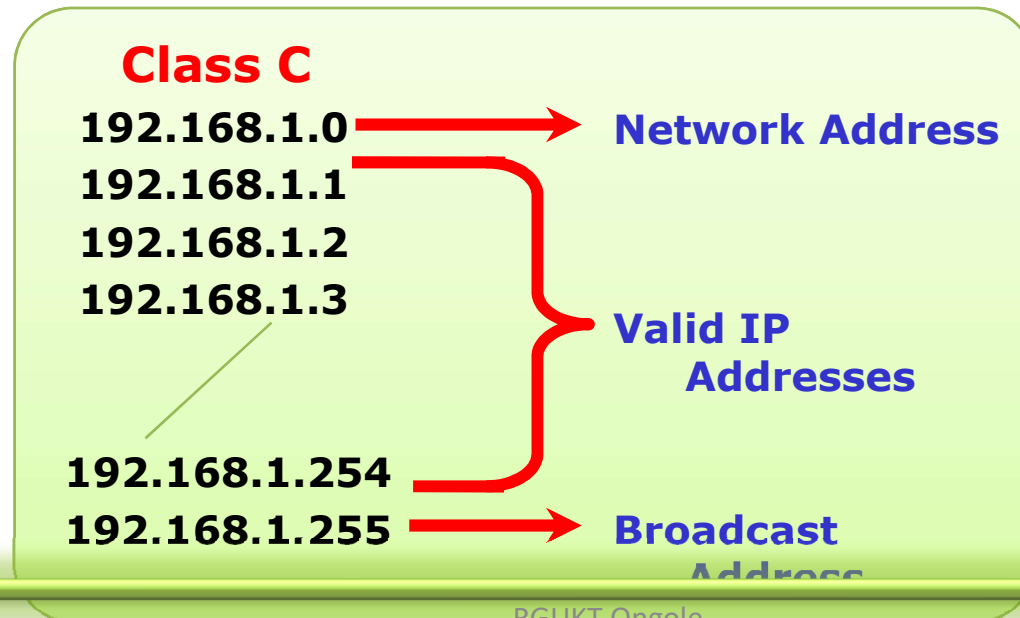
Class C : N.N.N.H

Network Address :

110xxxxx.xxxxxxxx.xxxxxxxx.00000000

Broadcast Address :

110xxxxx.xxxxxxxx.xxxxxxxx.11111111



The Network Layer

- There are certain addresses in each class of IP address that are reserved for LAN. These addresses are called private addresses.
- They can be used for: home & office networks, networks not connected to Internet.

Class A

10.0.0.0 to 10.255.255.255

Class B

172.16.0.0 to 172.31.255.255

Class C

192.168.0.0 to 192.168.255.255

The Network Layer

Addressing :

- **Subnet Mask differentiates Network portion and Host Portion**
- **Subnet Mask is been given for host Identification of Network ID**
- **Represented with all 1's in the network portion and with all 0's in the host portion.**

The Network Layer

Class A : N.H.H.H

11111111.00000000.00000000.00000000

Default Subnet Mask for Class A is 255.0.0.0

Class B : N.N.H.H

11111111.11111111.00000000.00000000

Default Subnet Mask for Class B is 255.255.0.0

Class C : N.N.N.H

11111111.11111111.11111111.00000000

Default Subnet Mask for Class C is 255.255.255.0

The Network Layer

IP Address : **192.168.1.1**
Subnet Mask : **255.255.255.0**

ANDING PROCESS :

192.168.1.1 = **11000000.10101000.00000001.00000001**

255.255.255.0 = **11111111.11111111.11111111.00000000**

=====

192.168.1.0 = **11000000.10101000.00000001.00000000**

=====

**The output of an AND table is 1 if both its inputs are 1.
For all other possible inputs the output is 0.**

AND TABLE

A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

SUBNETTING

The Network Layer

- **Dividing a Single Network into Multiple Networks.**
- **Converting Host bits to Network Bits
i.e. Converting 0's into 1's**
- **Subnetting is also called as FLSM (Fixed Length Subnet Mask)**
- **Subnetting can be done in three ways.**
 - **Requirement of Networks**
 - **Requirement of Hosts**
 - **Cisco / Notation**

The Network Layer





Organization is having 100 PC

- Which Class is preferred for the network ?

Answer : Class C.

- In Organization we have Five Departments with 20 Pcs each

Organization IP address– **192.168.1.0/24**

–	MCSE		192.168.1.1 to 192.168.1.20
–	CISCO		192.168.1.21 to 192.168.1.40
–	FIREWAL		192.168.1.41 to 192.168.1.60
–	SOLARIS		192.168.1.61 to 192.168.1.80
–	TRAININ		192.168.1.81 to 192.168.1.100






The Network Layer

- **Administrator's Requirement :**
Inter-department communication should not be possible ?

Solution.

Allocate a different Network to each Department

i.e.

- **MCSE**  **192.168.1.1 to 192.168.1.20**
- **CISCO**  **192.168.2.1 to 192.168.2.20**
- **FIREWAL**  **192.168.3.1 to 192.168.3.20**
- **SOLARIS**  **192.168.4.1 to 192.168.4.20**
- **TRAINING**  **192.168.5.1 to 192.168.5.20**

- **In the above Scenario inter-department communication is not possible.**

The Network Layer

Problem with the previous Scenario is :-

- **Loss of bandwidth as the broadcasting is done for 254 machines rather than for 20 machines.**
- **Wastage of IP addresses (Approximately 1000)**
- **No Security**

The Network Layer

POWER TABLE

$2^1 = 2$	$2^9 = 512$	$2^{17} = 131072$	$2^{25} = 33554432$
$2^2 = 4$	$2^{10} = 1024$	$2^{18} = 262144$	$2^{26} = 67108864$
$2^3 = 8$	$2^{11} = 2048$	$2^{19} = 524288$	$2^{27} = 134217728$
$2^4 = 16$	$2^{12} = 4096$	$2^{20} = 1048576$	$2^{28} = 268435456$
$2^5 = 32$	$2^{13} = 8192$	$2^{21} = 2097152$	$2^{29} = 536870912$
$2^6 = 64$	$2^{14} = 16384$	$2^{22} = 4194304$	$2^{30} = 1073741824$
$2^7 = 128$	$2^{15} = 32768$	$2^{23} = 8388608$	$2^{31} = 2147483648$
$2^8 = 256$	$2^{16} = 65536$	$2^{24} = 16777216$	$2^{32} = 4294967296$

The Network Layer

VALUES IN SUBNET MASK

Bit	Value	Mask
1	128	10000000
2	192	11000000
3	224	11100000
4	240	11110000
5	248	11111000
6	252	11111100
7	254	11111110
8	255	11111111

The Network Layer

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class C : 192.168.1.0

- **No. of Subnet**
 - = $2^n - 2 \geq \text{Req. of Subnet}$
 - = $2^3 - 2 \geq 5$ (-2 is for First & Last Subnet Range)
 - = $8 - 2$
 - = **6 Subnet**
- **No. of Host**
 - = $2^h - 2$ (-2 is for Network ID & Broadcast ID)
 - = $2^5 - 2$
 - = $32 - 2$
 - = **30 Hosts/Subnet**

The Network Layer

**If you convert 3 Host Bits to Network Bits
6 Subnet & 30 Hosts/Subnet**

**Customize Subnet Mask
255.255.255.224**

Subnet Range

192.168.1.32 to 192.168.1.63 → MCSE
192.168.1.64 to 192.168.1.95 → CISCO
192.168.1.96 to 192.168.1.127 → FIREWALL
192.168.1.128 to 192.168.1.159 → SOLARIS
192.168.1.160 to 192.168.1.191 → TRAINING
192.168.1.192 to 192.168.1.223 → Future Use

The Network Layer

Class C : **N.N.N.H**

110xxxxx.xxxxxxxx.xxxxxxxx.xxxx

Class C : 192.168.1.0

- **No. of Subnet**

$$= 2^n - 2 \geq \text{Req. of Subnet}$$

$$= 2^4 - 2 \geq 14 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 16 - 2$$

$$= 14 \text{ Subnet}$$

- **No. of Host**

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^4 - 2$$

$$= 16 - 2$$

$$= 14 \text{ Hosts/Subnet}$$

The Network Layer

If you convert 4 Host Bits to Network Bits
14 Subnet & 14 Hosts/Subnet

Customize Subnet Mask
255.255.255.240

Subnet Range

192.168.1.16 to 192.168.1.31

192.168.1.32 to 192.168.1.47

192.168.1.48 to 192.168.1.63

192.168.1.64 to 192.168.1.80

192.168.1.224 to 192.168.1.239

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxx

Class C : 192.168.1.0

- **No. of Subnet**
 - = $2^n - 2$
 - = $2^1 - 2$
 - = $2 - 2$
 - = **0 Subnet**
- **One bit masking is Invalid, You are not getting any networks when you convert 1 host bit to network bit.**

The Network Layer

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class C : 192.168.1.0

- **No. of Subnet**

$$= 2^n - 2$$

$$= 2^7 - 2$$

$$= 128 - 2$$

$$= 126 \text{ Subnet}$$

- **No. of Host**

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^1 - 2$$

$$= 2 - 2 = 0 \text{ Hosts/Subnet}$$

- **In this case, You are not getting any host when you convert 7 host bit to network bit.**

The Network Layer

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class C : 192.168.1.0

- **No. of Subnet**

$$= 2^n - 2$$

$$= 2^8 - 2$$

$$= 256 - 2$$

$$= 254 \text{ Subnet}$$

- **No. of Host**

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^0 - 2$$

$$= 0 - 2 = -2 \text{ Hosts/Subnet}$$

- **In this case, You are not getting any host when you convert 8 host bit to network bit.**

The Network Layer

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class C : 192.168.1.0

- **No. of Host**

$$= 2^h - 2 \geq \text{Req. of Host}$$

$$= 2^6 - 2 \geq 40 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 64 - 2$$

$$= 62 \text{ Hosts/Subnet}$$

- **No. of Subnet**

$$= 2^n - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 2^2 - 2$$

$$= 4 - 2$$

$$= 2 \text{ Subnet}$$

The Network Layer

If you convert 2 Host Bits to Network Bits
2 Subnet & 62 Hosts/Subnet

Customize Subnet Mask
255.255.255.192

Subnet Range
192.168.1.64 to 192.168.1.127
192.168.1.128 to 192.168.1.191

The Network Layer

Class C : N.N.N.H

110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class C : 192.168.1.0

- **No. of Host**

$$= 2^h - 2 \geq \text{Req. of Host}$$

$$= 2^2 - 2 \geq 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 4 - 2$$

$$= 2 \text{ Hosts/Subnet}$$

- **No. of Subnet**

$$= 2^n - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 2^6 - 2$$

$$= 64 - 2$$

$$= 62 \text{ Subnet}$$

The Network Layer

- Customize Subnet Mask =

255. 255. 255. 252
 11111111.11111111.11111111.11111100
128 64 32 16 8 4 2 1

- Range of Networks

Network ID		Broadcast ID	
192.168.1.0	-		X
192.168.1.3			
192.168.1.4	-	192.168.1.7	
192.168.1.8	-	192.168.1.11	
192.168.1.12	-	192.168.1.15	
192.168.1.248	-	192.168.1.251	
192.168.1.252	-	192.168.1.255	X

Valid Subnets

The Network Layer

Class C : **N.N.N.H**

110xxxxx.xxxxxxxx.xxxxxxxx.xxxx**xxxx**

Class C : **192.168.1.0/29**

Extra Network Bits = $29 - 24 = 5$

Put n value = 5

- **No. of Subnet**

$$= 2^n - 2$$

$$= 2^5 - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 32 - 2$$

$$= 30 \text{ Subnet}$$

- **No. of Host**

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^3 - 2$$

$$= 8 - 2$$

$$= 6 \text{ Hosts/Subnet}$$

The Network Layer

If you convert 5 Host Bits to Network Bits
30 Subnet & 6 Hosts/Subnet

Customize Subnet Mask
255.255.255.248

Subnet Range

192.168.1.8 to 192.168.1.15
192.168.1.16 to 192.168.1.23
192.168.1.24 to 192.168.1.31
192.168.1.32 to 192.168.1.39

192.168.1.240 to 192.168.1.247

The Network Layer

Class C : **N.N.N.H**

110xxxxx.xxxxxxxx.xxxxxxxx.xxxx**xxx**

Class C : 192.168.1.0/28

Extra Network Bits = $28 - 24 = 4$

Put n value = 4

- No. of Subnet

$$= 2^n - 2$$

$$= 2^4 - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 16 - 2$$

$$= 14 \text{ Subnet}$$

- No. of Host

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^4 - 2$$

$$= 16 - 2$$

$$= 14 \text{ Hosts/Subnet}$$



The Network Layer

If you convert 4 Host Bits to Network Bits
14 Subnet & 14 Hosts/Subnet

Customize Subnet Mask
255.255.255.240

Subnet Range

192.168.1.16 to 192.168.1.31

192.168.1.32 to 192.168.1.47

192.168.1.48 to 192.168.1.63

192.168.1.64 to 192.168.1.80

192.168.1.224 to 192.168.1.239

The Network Layer

Class B : N.N.H.H

10xxxxxx.xxxxxxxx.xxXXXXXX.XXXXXXXX

Class B : 172.16.0.0

- **No. of Subnet**
 - = $2^n - 2 \geq \text{Req. of Subnet}$
 - = $2^2 - 2 \geq 2$ (-2 is for First & Last Subnet Range)
 - = $4 - 2$
 - = **2 Subnet**
- **No. of Host**
 - = $2^h - 2$ (-2 is for Network ID & Broadcast ID)
 - = $2^{14} - 2$
 - = **16384 - 2**
 - = **16382 Hosts/Subnet**

The Network Layer

If you convert 2 Host Bits to Network Bits
2 Subnet & 16382 Hosts/Subnet

Customize Subnet Mask
255.255.192.0

Subnet Range
172.16.64.0 to 172.16.127.255
172.16.128.0 to 172.16.191.255

The Network Layer

Class B : N.N.H.H

10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class B : 172.16.0.0

- **No. of Host**
 - = $2^h - 2 \geq \text{Req. of Host}$
 - = $2^7 - 2 \geq 126$ (-2 is for Network ID & BroadcastID)
 - = $128 - 2$
 - = **126 Hosts/Subnet**
- **No. of Subnet**
 - = $2^n - 2$ (-2 is for First & Last Subnet Range)
 - = $2^9 - 2$
 - = $512 - 2$
 - = **510 Subnet**

The Network Layer

If you convert 9 Host Bits to Network Bits
510 Subnet & 126 Hosts/Subnet

Customize Subnet Mask
255.255.255.128

Subnet Range

172.16.0.128 to 172.16.0.255
172.16.1.0 to 172.16.1.127
172.16.1.128 to 172.16.1.255
172.16.2.0 to 172.16.2.127

172.16.255.0 to 172.16.255.127

The Network Layer

Class B : **N.N.H.H**

10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class B : 172.16.0.0/22

Extra Network Bits = $22 - 16 = 6$

Put n value = 6

- No. of Subnet

$$= 2^n - 2$$

$$= 2^6 - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 64 - 2$$

$$= 62 \text{ Subnet}$$

- No. of Host

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^{10} - 2$$

$$= 1024 - 2$$

$$= 1022 \text{ Hosts/Subnet}$$



The Network Layer

If you convert 6 Host Bits to Network Bits
62 Subnet & 1022 Hosts/Subnet

Customize Subnet Mask
255.255.252.0

Subnet Range

172.16.4.0 to 172.16.7.255
172.16.8.0 to 172.16.11.255
172.16.12.0 to 172.16.15.255
172.16.16.0 to 172.16.19.255

172.16.248.0 to 172.16.251.255

The Network Layer

Class A : N.H.H.H

0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class A : 10.0.0.0

- **No. of Subnet**
 - = $2^n - 2 \geq \text{Req. of Subnet}$
 - = $2^9 - 2 \geq 500$ (-2 is for First & Last Subnet Range)
 - = $512 - 2$
 - = **510 Subnet**
- **No. of Host**
 - = $2^h - 2$ (-2 is for Network ID & Broadcast ID)
 - = $2^{15} - 2$
 - = $32768 - 2$
 - = **32766 Hosts/Subnet**

The Network Layer

If you convert 9 Host Bits to Network Bits
510 Subnet & 32766 Hosts/Subnet

Customize Subnet Mask
255.255.128.0

Subnet Range

10.0.128.0 to 10.0.255.255

10.1.0.0 to 10.1.127.255

10.1.128.0 to 10.1.255.255

10.2.0.0 to 10.2.127.255

10.255.0.0 to 10.255.127.255

The Network Layer

Class A : N.H.H.H

0xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Class A : 10.0.0.0

- **No. of Host**

$$= 2^h - 2 \geq \text{Req. of Host}$$

$$= 2^{18} - 2 \geq 260000 \text{ (-2 is for Network ID \& BroadcastID)}$$

$$= 262144 - 2$$

$$= 262142 \text{ Hosts/Subnet}$$

- **No. of Subnet**

$$= 2^n - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 2^6 - 2$$

$$= 64 - 2$$

$$= 62 \text{ Subnet}$$

The Network Layer

If you convert 6 Host Bits to Network Bits
62 Subnet & 262142 Hosts/Subnet

Customize Subnet Mask
255.252.0.0

Subnet Range

10.4.0.0 to 10.3.255.255

10.8.0.0 to 10.7.255.255

10.12.0.0 to 10.15.255.255

10.16.0.0 to 10.19.255.255

10.248.0.0 to 10.251.255.255

The Network Layer

Class A : N.H.H.H

0xxxxxxx.xxxxxxxx.xxxxXXXX.XXXXXXXX

Class A : 10.0.0.0/20

Extra Network Bits = $20 - 8 = 12$

Put n value = 12

- No. of Subnet

$$= 2^n - 2$$

$$= 2^{12} - 2 \text{ (-2 is for First \& Last Subnet Range)}$$

$$= 4096 - 2$$

$$= 4094 \text{ Subnet}$$

- No. of Host

$$= 2^h - 2 \text{ (-2 is for Network ID \& Broadcast ID)}$$

$$= 2^{12} - 2$$

$$= 4096 - 2$$

$$= 4094 \text{ Hosts/Subnet}$$



The Network Layer

If you convert 12 Host Bits to Network Bits
4094 Subnet & 4094 Hosts/Subnet

Customize Subnet Mask
255.255.240.0

Subnet Range

10.0.16.0 to 10.31.255.255

10.0.32.0 to 10.47.255.255

10.0.48.0 to 10.63.255.255

10.0.64.0 to 10.79.255.255

10.255.224.0 to 10.255.239.255

The Network Layer

- **Subnetting a subnet is called as Variable Length Subnet Mask**
- **VLSMs provide the capability to include more than one subnet mask within a major network**

The Network Layer

- **Administrator does not want inter-department communication in the sub departments ?**

Answer : You will use the subnet range to further divide it into smaller ranges, this time its Subnetting of a Subnet i.e. VLSM.

The Network Layer

Routing :

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

The Network Layer

Routing Metrics and Costs:

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

The Network Layer

Routing Metrics

Hop count: Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.

Delay: It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.

The Network Layer

Routing Metrics and Costs:

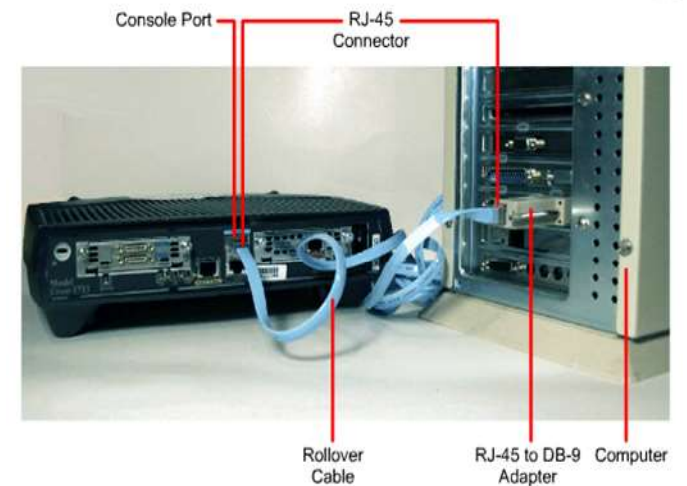
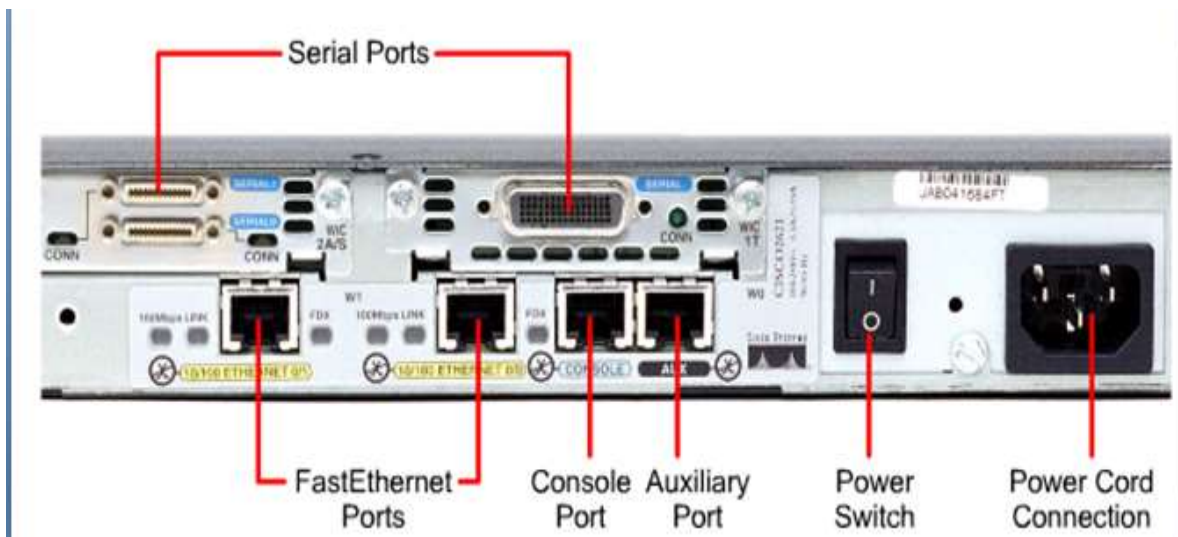
Bandwidth: The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.

Load: Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.

Reliability: Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

The Network Layer

Router



The Network Layer

Router



The Network Layer

Types of Routing :

Routing is classified in to three categories:

- Static Routing (Nonadaptive Routing)
- Default Routing
- Dynamic Routing (Adaptive Routing)

The Network Layer

Static Routing :

- Static Routing is also known as **Nonadaptive Routing**.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages

- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

The Network Layer

Static Routing :

Disadvantages

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

The Network Layer

Default Routing :

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

The Network Layer

Dynamic Routing :

- It is also known as **Adaptive Routing**.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Network Layer

Dynamic Routing protocol should have the following features :

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages	Disadvantages
It is easier to configure.	It is more expensive in terms of CPU and bandwidth usage.
It is more effective in selecting the best route in response to the changes in the condition or topology.	It is less secure as compared to default and static routing.

The Network Layer

Classification of Dynamic Routing protocol

1.IGP

Distance Vector

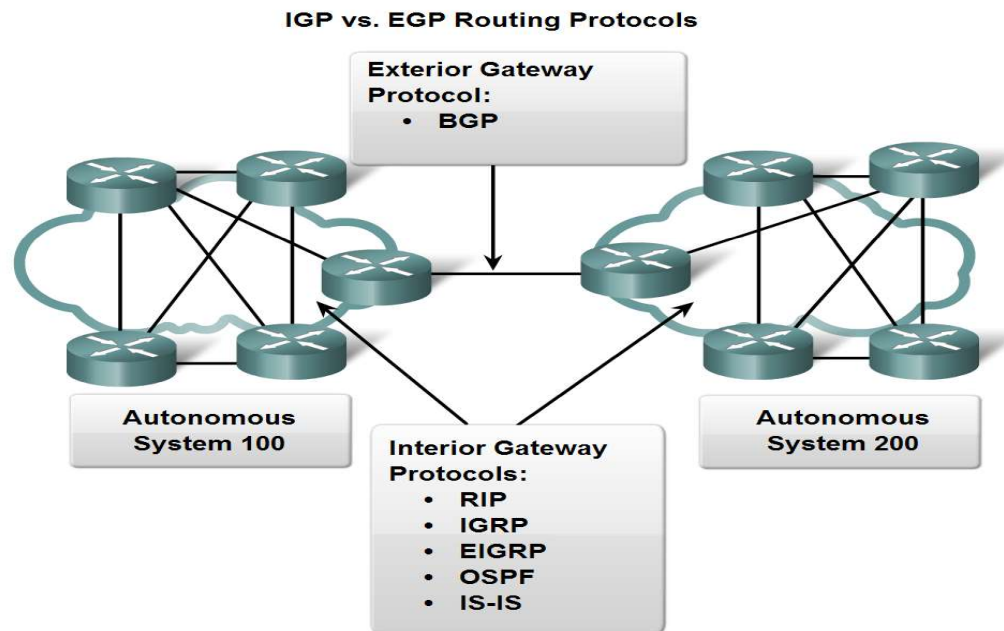
Link State

2.EGP

BGP

The Network Layer

Classification of Dynamic Routing protocol



The Network Layer

Administrative Distance

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

The Network Layer

Distance Vector Routing Algorithm

The Distance vector algorithm is

- **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
- **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in RIP.
- Each router maintains a distance table known as **Vector**.

The Network Layer

Three Keys to understand the working of Distance Vector Routing Algorithm:

Knowledge about the whole network: Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.

Routing only to neighbors: The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.

Information sharing at regular intervals: Within 30 seconds, the router sends the information to the neighboring routers.

The Network Layer

Bellman-Ford algorithm

The Network Layer

Link State Routing :

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

Knowledge about the neighborhood: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.

Flooding: Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.

Information sharing: A router sends the information to every other router only when the change occurs in the information.

The Network Layer

Link State Routing has two phases:

Initial state: Each node knows the cost of its neighbors.

Final state: Each node knows the entire graph.

Route Calculation : Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

➤ The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

➤ The Dijkstra's algorithm is an iterative, and it has the property that after k^{th} iteration of the algorithm, the least cost paths are well known for k destination nodes.

The Network Layer

Dijkstra's algorithm

The Network Layer

The Network Layer

The Network Layer

Congestion Control

When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called congestion.

The network layer and transport layer share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network. To maintain this, network and transport layers have to work together.

The Network Layer

Effects of Congestion

Following are the effects of Congestion

- Because of the increase in the response time, the overall performance is reduced.
- Also, in worst situations, because of the delay that takes place, re-transmission can also occur.

The Network Layer

Congestion Control techniques

To control the congestion in networks, the control techniques are broadly classified under two categories, which are as follows

The Open loop refers to the protocols that should be used in order to prevent congestion. That is, the congestion should not occur in the first place. This is based on the technique of having a good design implementation in order to prevent the congestion from taking place.

The Close loop allows the system to enter in the congestion state if it occurs, detects it and then proceeds to remove the congestion. This is based on the feedback mechanism that is received. With the help of the feedback, one can detect and remove the congestion from the network.

The Network Layer

Open Loop Congestion Control

In this control policies are applied to prevent congestion before it happens. It is handled either by the source or the destination.

Retransmission Policy – This type of policy is sometimes unavoidable. If the sender feels that a packet is lost or corrupted, then it thinks to retransmit. So, a retransmission policy can prevent congestion.

Window Policy – In this type of window the sender may also affect congestion. The selective repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, a number of packets may be resent, although some may have arrived safe and sound at the receiver.

The Network Layer

Open Loop Congestion Control

Acknowledgement Policy – This policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time.

Discarding Policy – A discarding policy by the routers prevents congestion and at the same time may not harm the integrity of the transmission.

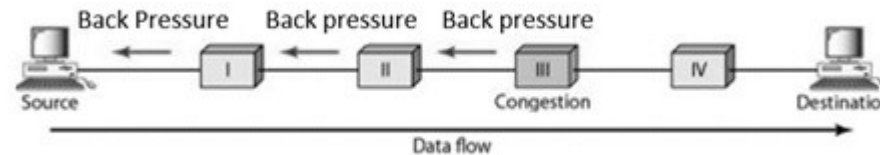
Admission Policy – An admission policy is a quality-of-service mechanism, which prevents congestion in virtual circuit networks.

The Network Layer

Closed Loop Congestion Control

Backpressure

- When a router is congested, it informs the previous upstream router to reduce the rate of outgoing packets.
- If a node becomes congested it can slow down or halt flow of packets from other nodes and halt flow of packets from other nodes.
- It means that other nodes have to apply control on incoming packet rates control on incoming packet rates.

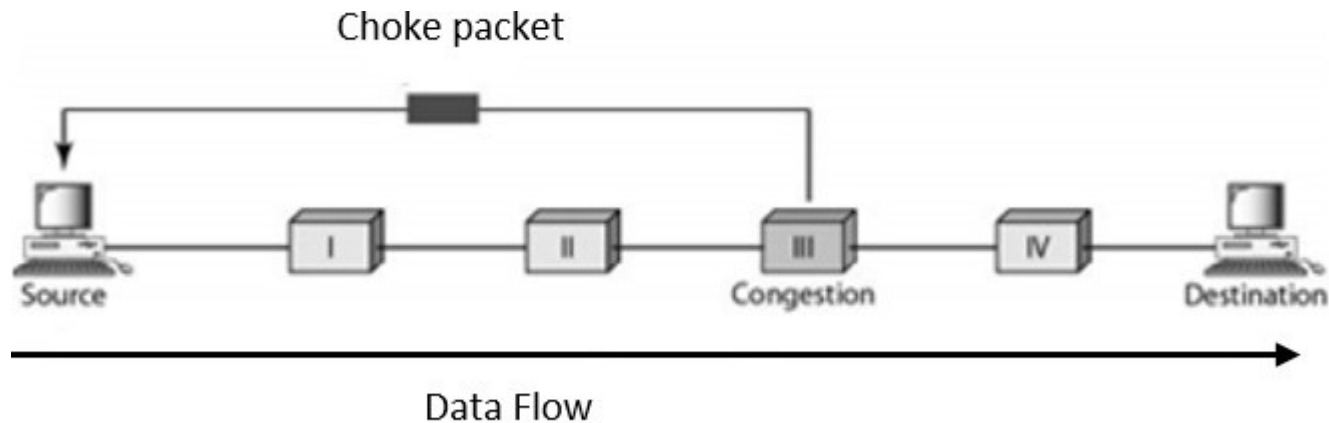


The Network Layer

Closed Loop Congestion Control

Choke packet

- It is sent by router to source, similar to ICMP's source quench packet.



The Network Layer

Difference between flow control and congestion control

Key	Flow Control	Congestion Control
Definition	In Flow Control, Traffic is controlled and Traffic represents flow from sender to receiver.	In Congestion Control also, Traffic is controlled and Traffic represents flow entering into the network.
Layers	Data link and Transport layers handles flow control.	Network and Transport layers handles congestion control.
Prime Focus	Receiver is prevented from being overwhelmed.	Network is prevented from being congested.
Responsibility	Only sender is responsible for the traffic.	Transport layer is responsible for the traffic.
Way	Traffic is prevented by slowing down the sender.	Traffic is prevented by slowing down the transport layer.

The Network Layer

Congestion Control Algorithm

When too many packets are displayed in a method of the subnet, the subnet's performance degrades. Hence, a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

Effects of Congestion

- ❖ As delay increases, performance decreases.
- ❖ If delay increases, retransmission occurs, making situation worse.

There is two congestion control algorithm:

- Leaky Bucket Algorithm
- Token Bucket Algorithm

The Network Layer

Congestion Control Algorithm

Leaky Bucket Algorithm

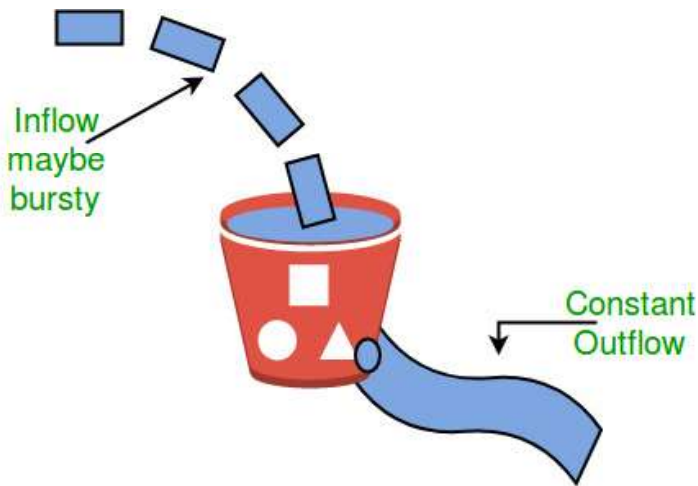
Let us consider an example to understand

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.

The Network Layer

Congestion Control Algorithm

Leaky Bucket Algorithm



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.
- **Token bucket Algorithm**

The Network Layer

Congestion Control Algorithm

Token Bucket Algorithm

The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is. So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.

Step 1 – In regular intervals tokens are thrown into the bucket f .

Step 2 – The bucket has a maximum capacity f .

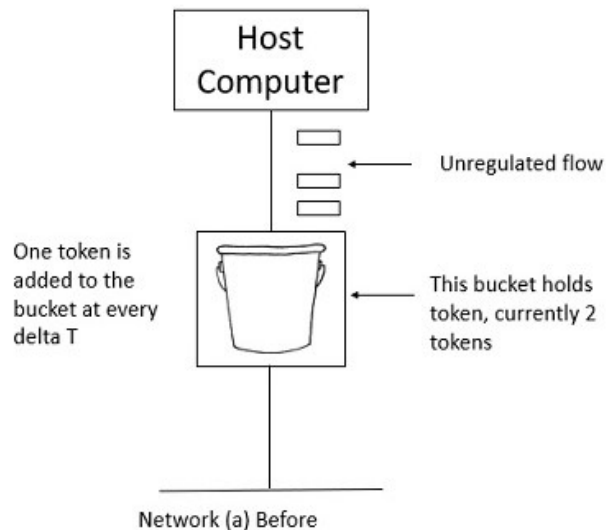
Step 3 – If the packet is ready, then a token is removed from the bucket, and the packet is sent.

Step 4 – Suppose, if there is no token in the bucket, the packet cannot be sent.

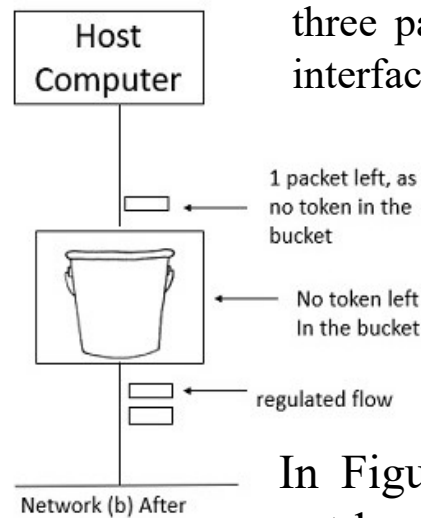
The Network Layer

Congestion Control Algorithm

Token Bucket Algorithm



In figure (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface.



In Figure (b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

The Network Layer

Congestion Control Algorithm

Token Bucket Algorithm

When compared to Leaky bucket the token bucket algorithm is less restrictive that means it allows more traffic. The limit of busyness is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of the token bucket algorithm is easy – a variable is used to count the tokens. For every t seconds the counter is incremented and then it is decremented whenever a packet is sent. When the counter reaches zero, no further packet is sent out.

