Study Material By Manikrao Dhore

Sub: Computer Networks

Section II: Network Layer

CO4: Develop Client-Server architectures and prototypes by the means of correct standards, protocols and technologies

Unit-IV Network Layer:

[CO4 → PO1, PO2, PO3, PO4, PO5,PO6, PO7, PO8,PO9, PSO01,PSO2,PSO3 – CO Strength 3,3,3,2,1,2,3,3,3,3,3,1]

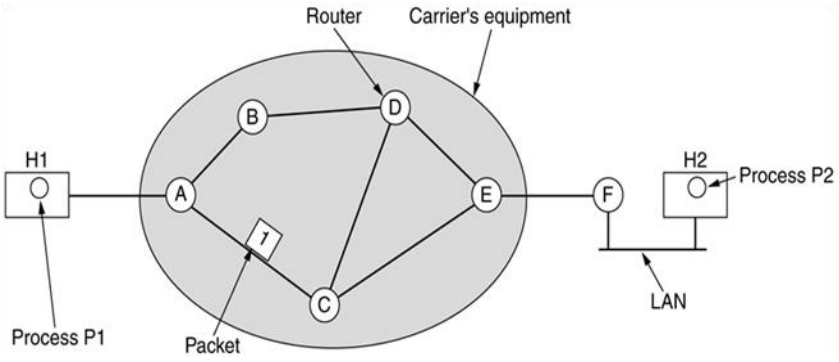
Network Layer: Switching Techniques: Circuit, Message and Packet Switching. Logical Addressing: IPv4 and IPv6, Subnetting, NAT, CIDR. Network Layer Protocols: IP, ICMP, Routing Protocols: Distance Vector, Link State, and Path Vector. Routing in Internet: RIP ,OSPF, BGP, Congestion control and QoS, MPLS, Mobile IP, Routing in MANET : AODV, DSR [6 Hrs]

Functions of Network Layer

1. To determine how packet will route from source to destination (Route selection/decision)
2. End-to-End Communication (Boundary to subnet)
3. Must know topology of N/w (set of router info)
4. To deal with internetworking issues (Heterogeneous n/w problem)
5. To provide services independent of topology
6. Controlling the operation of subnet
7. Apply congestion control (Router Memory Space and Bandwidth)
8. Accounting of packets and billing
9. Address resolution
10. Large packet management

Design Issues:

I. Store-and-Forward Packet Switching

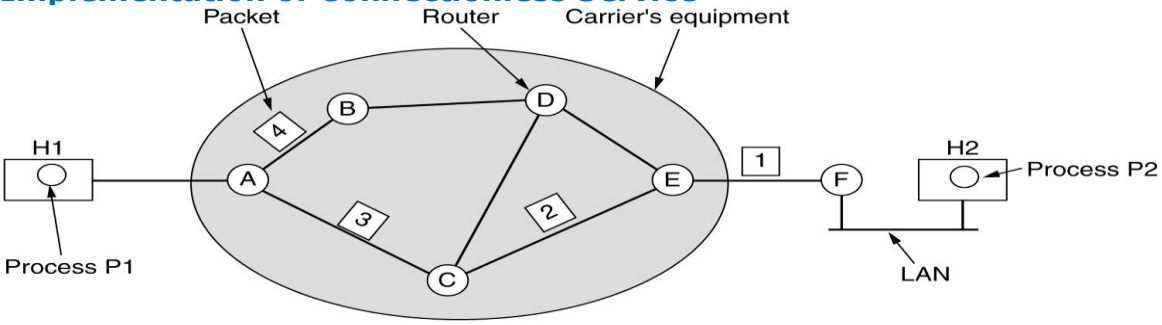


- Store the packet in router memory
- Forward the packet
- Verify checksum at destination
- Remove the packet

II. Services to Transport Layer

- NL is the boundary
- Services independent of topology
- TL should be shielded from number, type and topology of network
- Network addresses should be uniform

III. Implementation of Connectionless Service



A's table

	initially	later
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

Dest. Line

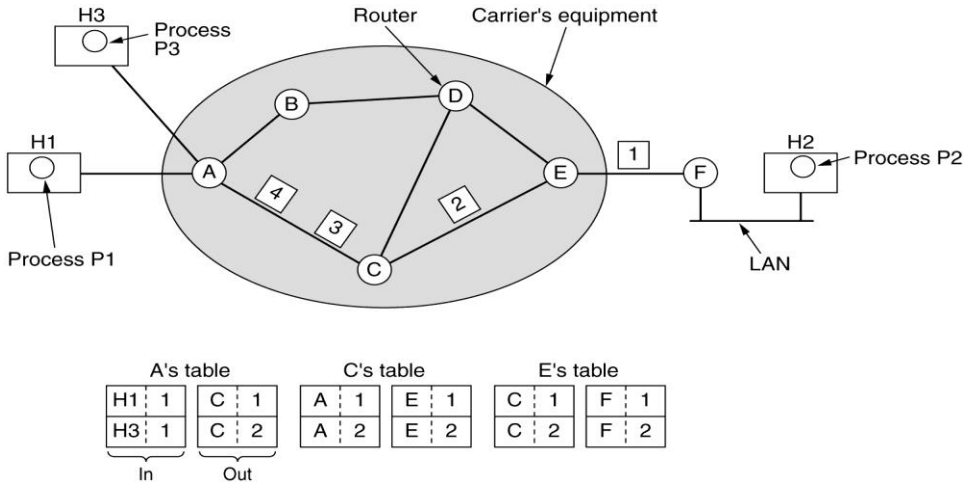
C's table

A	A
B	A
C	–
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

IV. Implementation of connection oriented Service



Comparison

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Autonomous System:

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

IP: Internet Protocol

- Packet Switching protocol
- Virtual Circuit Establishment

- Provides packet delivery
- IP to MAC mapping
- Route selection/decision
- Flow Control
- Congestion Control
- Accounting
- Quality of service
- Unreliable and connectionless

IP Packet Format:

IP Version 4-bit	Header Length 4bit	TOS 8-bit (DTR)	Total length 16-bit
Identification 16-bit	Flags 3-bits (DF, MF)		Fragment offset 13-bit
TTL 8-bit	Protocol 8-bit		Checksum of Header 16-bit
Source IP			
Destination IP			
Options, padding , and then data			

TOS : Priority, Delay, Throughput and Reliability. This field tells the subnet what kind of service it want.

0	1	2	3	4	5	6	7
Precedence			D	T	R	Unused	

Precedence: It is priority from 0 to 7

0 – normal and 7 – Network Control Packets

Delay	D=0 Normal	D=1 Low
Throughput	T=0 Normal	T=1 High
Reliability	R=0 Normal	R=1 High

Satellite Link: High Delay High Throughput

Leased Line: Low delay Low Throughput

Note: In current practice, routers ignore TOS field.

Total Length: Total length including all fields. It allows up to 65,535 bytes

Flags : DF and MF

Don't Fragment and More Fragment

One datagram can have maximum 8192 fragments (13-bit field) and each fragment can have maximum size 64 K.

TTL : Number of hops (If not delivered return to)

Protocol : Transport/ Application Layer protocol to which data belongs to

Padding

Offset of fragment

Packet Size: 64 K

IP packet of size 1400 bytes is to be transferred over a link layer whose MTU is 1000 bytes. What will be values of fragment, Offset and Flag related to fragmentation for all the fragments produced.

[1][0][1],

[2][1000][0],

IP Addressing Version 4

- Mahatma Gandhi, India" or "Albert Einstein, USA,"
- No street address or the city name necessary.
- One can reach *any* website, anywhere without knowing location.
- One can do it so efficiently, quickly within a few seconds
- Solution to all lies in *network routing*

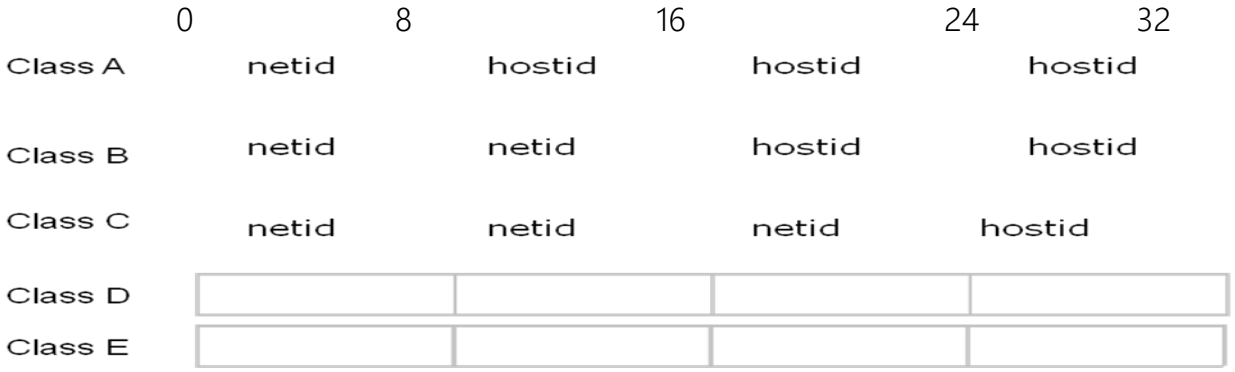
- Routing refers to the ability to send a unit of information from point A to point B by determining a best path through the network
- A key and necessary factor in routing is addressing.
- How addressing structured, plays a critical role in routing
- Addressing in network has similarities to addressing in the postal system.
- Postcard has - name, house number, street, city, state and postal code.
- Processing view to route the postcard uses reverse order
- Starts with the postal code, state, city, street, house no and person.
- Three main parts: the postal code, the street address and the name
- The postcard is routed to geographical region with the postal code.
- The appropriate delivery post office
- Postman or post woman delivers the postcard at the address
- Postal address uses a hierarchical view for routing
- Hierarchical view help to divide the complete address into multiple distinguishable parts to help with the routing decision
- Multiple levels like postal code , street address, and name
- Internet addressing has similarities to the postal addressing system.
- An IP address defines two parts: one part that is similar to the postal code and the other part that is similar to the house address;
- In Internet terminology, they are known as the *netid* and the *hostid*, to identify a network and a host address, respectively.
- Host: web-server, an email server, desktop, laptop, or any computer we use for accessing t he Internet.
- A netid identifies a contiguous block of addresses
- IP Addressing uses TCP/IP protocol
- TCP is in charge of the reliable delivery of information
- IP is in charge of routing, using the IP addressing mechanism.
- IP does not guaranty that information is reliably delivered.
- In the postal system, guaranteed delivery needs an additional fee.
- In network host first sends a beacon to the destination address (host) to see if it is reachable, and waits for an acknowledgment *before* sending the actual message.

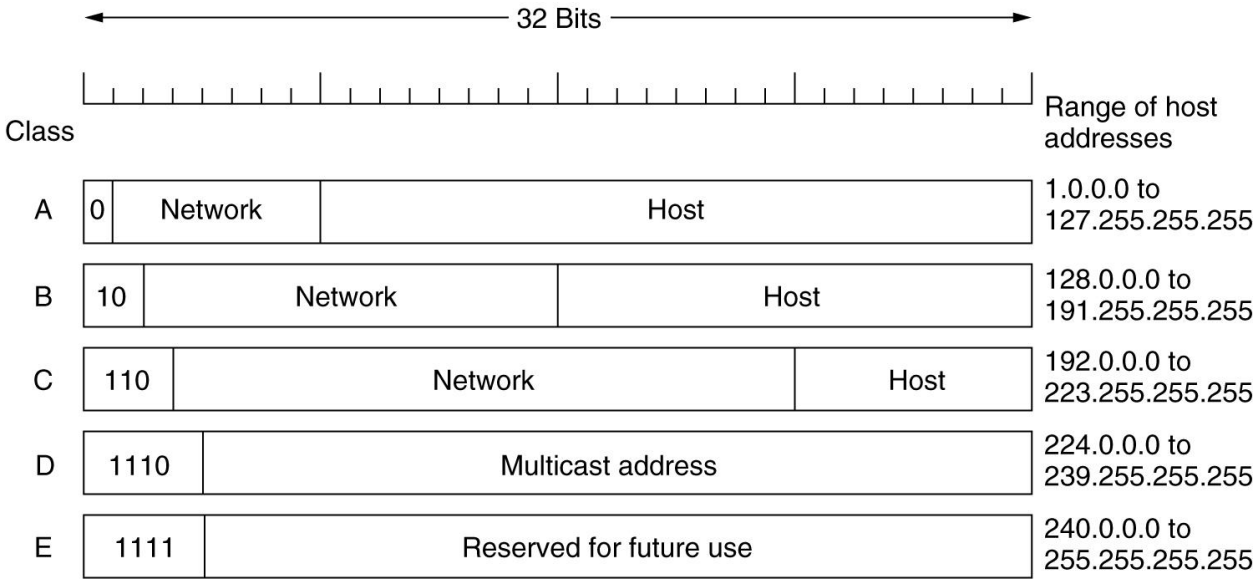
- Acknowledgment and retransmission mechanism is used

Classful Addressing Scheme

- IP address assigned to a host is 32 bits long and should be unique.
- Hierarchy in IP address has network part and a host part *(netid, hostid)*
- Internet is the *interconnection* of networks identified through netids where each netid has a collection of hosts.

- Class Type Network_id host_id





Class	From	dec	To	dec	N/w	Hosts
A	00000001	1	0111 1111	126	126	16777214

B	1000 0000	128	1011 1111	191	16384	65534
C	1100 0000	192	1101 1111	223	2097152	254

Class A: 7 bits netid 2^7 = 128 networks and 2^{24} – 2 hosts

Class B: 14-bit netid, 2^{14} = 16384 networks and 2^{16} – 2 hosts

Class C : 21-bits netid 2^{21} = 2,097,152 networks and 2^8 – 2 hosts.

Dotted Notation

1000 0000 0000 1011 0000 0011 0001 1111

128 . 11. 3 . 31

Class Ranges

A 1.0.0.0 126.255.255.255

B 128.0.0.0 191.255.255.255

C 192.0.0.0 223.255.255.255

D : 224.0.0.0 239.255.255.255

E : 240.0.0.0 255.255.255.255

Default netmask To find netid and hostid

A 255.0.0.0

B 255.255.0.0

C 255.255.255.0

200. 45. 34. 56

11001000 00101101 00100010 00111000

AND

11111111 11111111 11111111 00000000

11001000 00101101 00100010 00000000

Subnetting : To create subnetwork

Subnet mask is used to make multiple separate subnetworks / segments with available IP

It uses / borrows few bits from hostid to create subnetworks.

Consider netmask of class C IP address

Ex . 11111111 11111111 11111111 0000000 : 255.255.255.0

11111111 11111111 11111111 1110000 : 255.255.255.224

Here three bits from hostid are used to create 8 subnetworks $2^3 = 8$

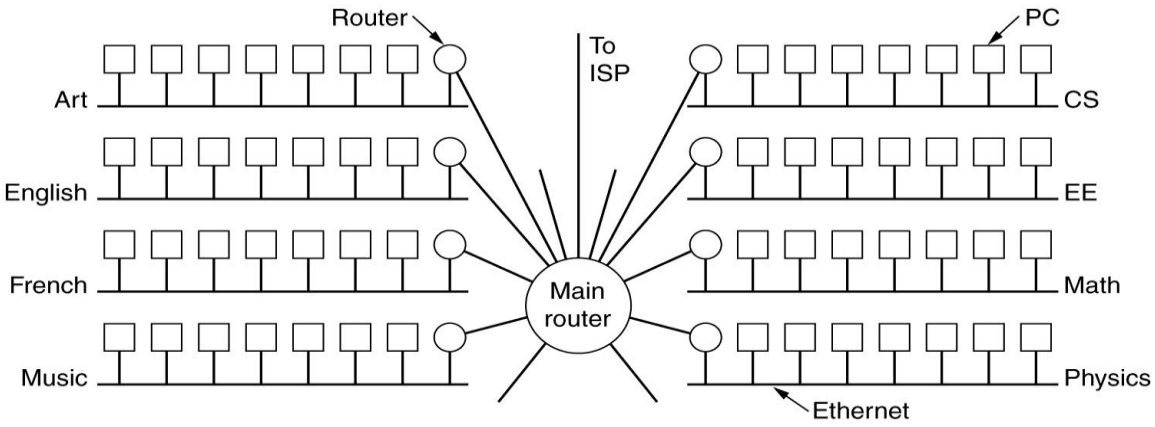
1 bit from hostid will create 2 subnetworks

2 bits from hostid will create 4 subnetworks

3 bits from hostid will create 8 subnetworks

4 bits from hostid will create 16 subnetworks etc

Netmask	1111 1111	1111 1111	1111 1111	0000 000
	255	255	255	0
Subnet	1111 1111	1111 1111	1111 1111	1110 0000
	255	255	255	224



Ex. Suppose VIT has IP address 192.1.1.0. Create 8 subnetworks.

Therefore subnet mask will be 255.255.255.224 and subnetworks as follows

1. 192.1.1.0 to 192.1.1.1.31 ie 192.1.1.00000000 to 00011111
2. 192.1.1.32 to 192.1.1.63 ie 192.1.1.00100000 to 00111111
3. 192.1.1.64 to 192.1.1.95
4. 192.1.1.96 to 192.1.1.127
5. 192.1.1.128 to 192.1.159
6. 192.1.1.160 to 192.1.1.191

7. 192.1.1.192 to 192.1.1.223
8. 192.1.1.224 to 192.1.1.255

Finding Subnet id

192.1.1.56

255.255.255.224

56	0011	1000	
224	1110	0000	
0010	0000	32	hence subnet id 192.1.1.32

Classless Interdomain Routing (CIDR)

- Classful addressing need much more space at router
- It is very difficult to assign block of 2,4,8,16,32,64 etc addresses using IP4
- This problem is solved by using CIDR addressing
- It uses explicit mask with IP4 addresses

a.b.c.d/n

where n is number of ones from left side of mask

192.168.40.0/24

192.168.40.0/20

192.168.40.0/15

Ex. Find the block of addresses from 167.199.170.82/27

Sol : Number of addresses in the block are $2^{32} - 2^{27} = 2^5 = 32$

First address is 10100111 11000111 10101010 01010010

10100111 11000111 10101010 01000000 ie 167.199.170.64/27

Therefore last address will be 167.199.170.95/27

Subnet masks for different blocks in CIDR

Classless Inter-Domain Routing (CIDR) is a replacement for the old process of assigning Class A, B and C addresses with a generalized network "prefix". Instead of being limited to network identifiers (or "prefixes") of 8, 16 or 24 bits, CIDR currently uses prefixes anywhere from 13 to 27 bits. Thus, blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts. This allows for address assignments that much more closely fit an organization's specific needs.

A CIDR address includes the standard 32-bit IP address and also information on how many bits are used for the network prefix. For example, in the CIDR address 206.13.01.48/25, the "/25" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.

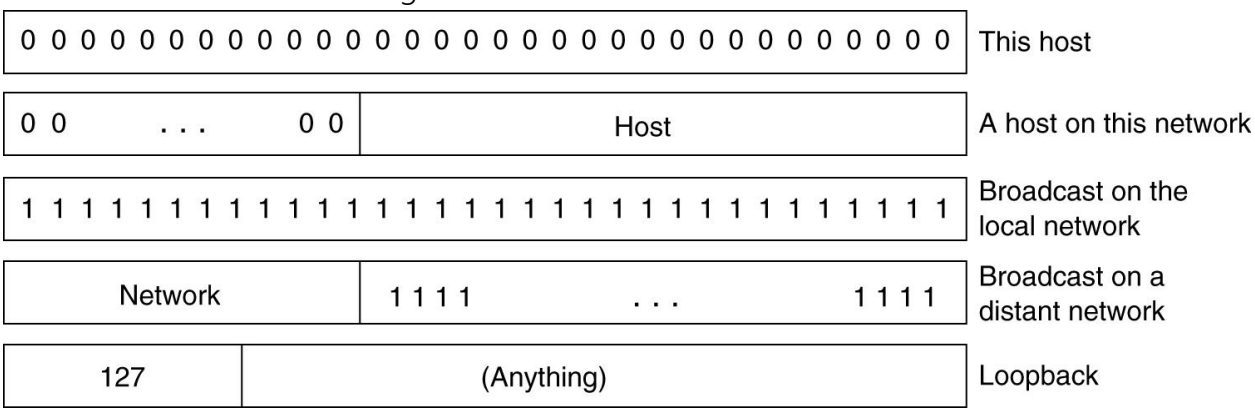
CIDR Block Prefix	# of Host Addresses
/27	32 hosts
/26	64 hosts
/25	128 hosts
/24	256 hosts
/23	512 hosts
/22	1,024 hosts
/21	2,048 hosts
/20	4,096 hosts
/19	8,192 hosts
/18	16,384 hosts
/17	32,768 hosts

Special addresses

- 0.0.0.0/8 source
- 10.0.0.0/8
- 172.16.0.0 to 172.31 .0.0 /12

and

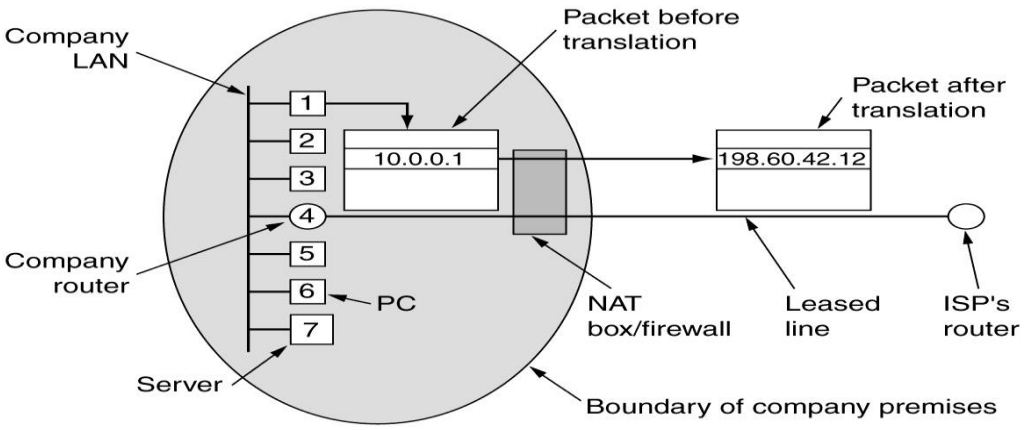
- 192.168.0.0/16 to 192.168.255.0/16 Private use IP network
- 127.0.0.0/1 any : loop back address
- All 1's : limited broadcast
- Netid + all 1's : direct broadcast
- 169.254.0.0 /16 For local link
- 224.0.0.0 multicast
- 224.0.1.7 conferencing



NAT : Network Address Translation

Due to the shortage of IP addresses NAT concept is introduced and allows to use following addresses as a private addresses for Internal Network. NAT box maps these addresses to the unique global IP Address.

10.0.0.0 To 10.255.255.255 Total 2^{24} Hosts
172.16.0.0 To 172.31.255.255 Total 2^{20} Hosts
192.168.0.0 To 192.168.255.255 Total 2^{16} Hosts



What is Routing?

1. Routing packets
2. Deciding outgoing line
3. Ability to cope with changes in topology and traffic

Tradeoffs

Router memory space and bandwidth

Setup time Vs address parsing

Virtual Circuit and Congestion Control with router crashing

Connectionless or connection oriented

Types of Routing Algorithms

Non-Adaptive: Static, Decision does not based on current traffic and topology, Route computed in advance

Adaptive: Dynamic, considers distance, RTT, Current traffic, topology, average queue length, cost, measured delay

Shortest Path Routing Algorithm: Static, Build a graph, Label with weight, Fastest

Flooding: Every incoming packet is sent out on every outgoing line

Selective Flooding: Select only right path: Military and distributed application

Distance Vector Routing:

Discovered by Bellman Ford and Ford Fulkerson.

Distance may be :

No. of hops

Queue length

Delay

Security level

Principle: Each router periodically shares its knowledge about neighbors or internetworks with its neighbors only.

It receives information from directly attached neighbors only.

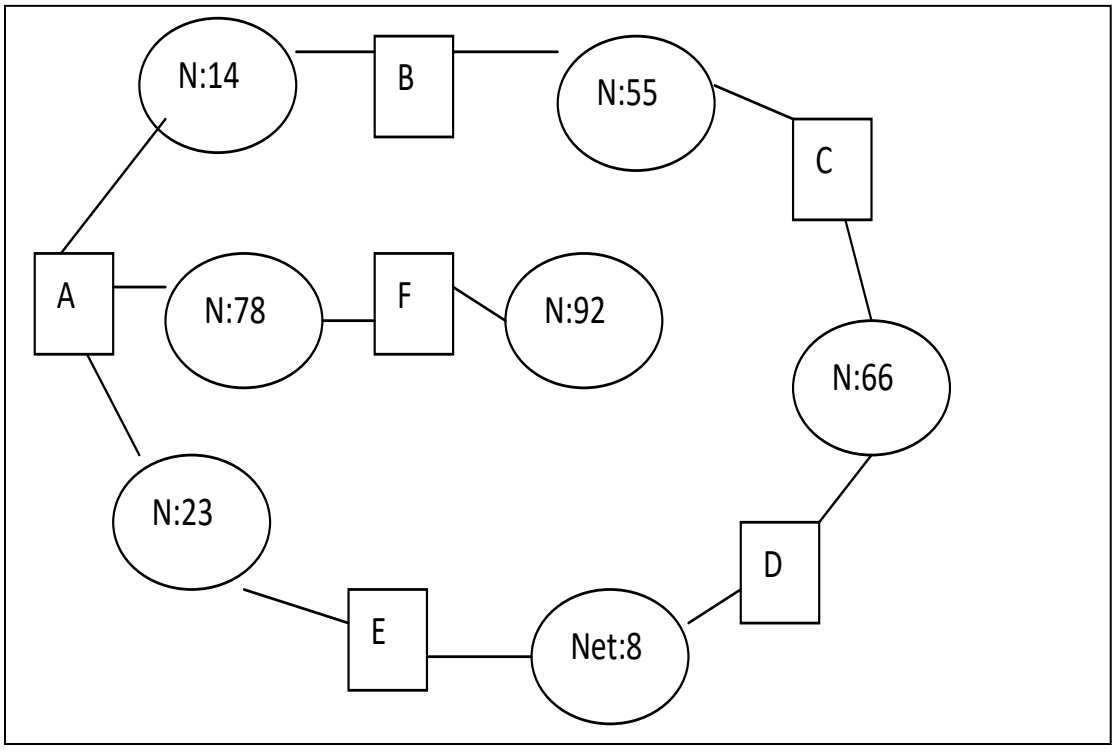
Cost is hops. Cost of link has taken = 1

Cost of link is 1 from router to network

Cost of link is 0 from network to router.

 ➔ Is used to denote router

 ➔ is used to denote network



Step I : Generate the initial routing tables for routers A to F.

For the understanding point of view consider the tables of router A and B only

Routing Table for A

Net id	Cost	Next hop
14	1	-
23	1	-
78	1	-

Routing Table for B

Net id	Cost	Next hop
14	1	-
55	1	-

Add 1 to the cost of B and add B in the next-hop

Net id	Cost	Next hop
14	2	B
55	2	B

Merge the tables

Net id	Cost	Next hop
14	1	-
23	1	-
78	1	-
14	2	B
55	2	B

Remove Duplicate from B's entry with larger cost

Net id	Cost	Next hop
14	1	-
23	1	-
78	1	-
55	2	B

Routing Table for A

Net id	Cost	Next hop
08	2	E
14	1	-
23	1	-
55	2	B
66	3	E
78	1	-
92	2	F

Routing Table for D

Net id	Cost	Next hop
08	1	-
14	3	E
23	2	E
55	2	C
66	1	-
78	3	E
92	4	E

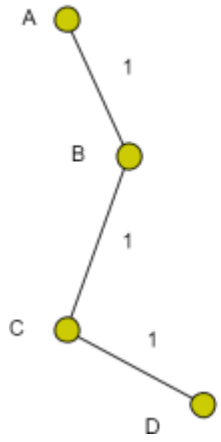
Characteristics of Algorithms

Distributed: as it receives and send back information to neighbors

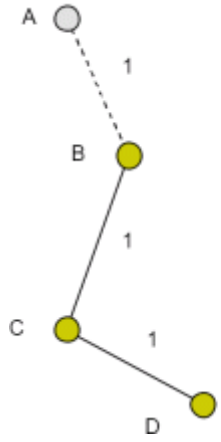
Iterative: it updates table periodically

Asynchronous: all routers need be updated at the same time

Count to Infinity Problem



B	C	D
1	2	3



B	C	D
3	2	3

B	C	D
3	4	3

B	C	D
5	4	5

Shortest Path By Dijkstra's Algorithm

- Computing path from a source node view
- It works on the notion of neighbouring node set
- Need to have the link costs of all links
- Computes shortest path to all the destinations
- Does not depends upon all neighbouring intermediates k
- It always calculates optimal intermediate node and then moves next
-

Link State Routing Algorithm

Distance : delay(time) or Traffic or security

Principle: Each router shares it information with all the routers in the networks.

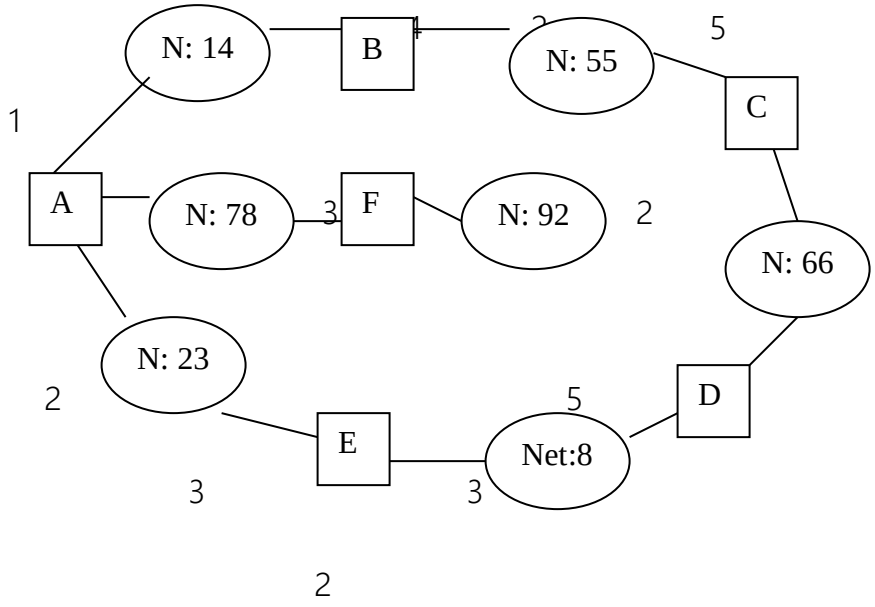
Algorithm:

- Discover the neighbor and learn network address
- Measure the delay or cost
- Construct link state packet
- Send it to all routers in network
- Compute shortest distance path for all routers using Dijkstra's algorithm

Step –I: Sends a special hello packet on each point to point line and get the information about network address.

Step-II: Sends the echo packet to neighbors and calculate the delay by RTT/2

Step-III: Construct the link state packet for each router



Router	Network ID	Cost	Neighbor

A	14	1	B
A	78	3	F
A	23	2	E
B	**14**	**4**	**A**
B	**55**	**2**	**C**
C	55	5	B
C	56	2	D
D	**66**	**5**	**C**
D	**08**	**3**	**E**
E	23	3	A
E	08	2	D
F	**78**	**2**	**A**
F	**92**	**3**	**-**

Step-IV: Each router sends it link state packet to all and hence all router will have same link state database

State V: Apply Dijkstra's algorithm to find shortest path tree for each router

Note A To B cost is 01 and B To A cost is 04

Finding Routing table for A using Dijkstra's algorithm

(iv) Each router sends it link state packet to all hence all router will have same link-state database. as shown in step III.

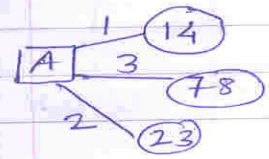
(v) Apply dijkstras to each router and construct individual shortest path tree for each router.

Ex →

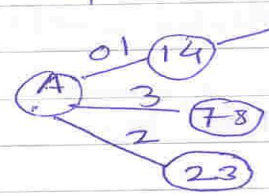
Hole A to B ⇒ 01
& B to A ⇒ 04

Tree for Router A

(i)

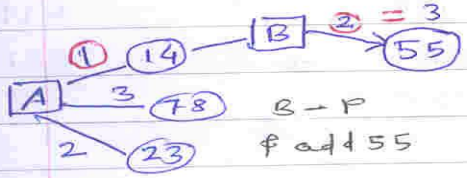


(ii)



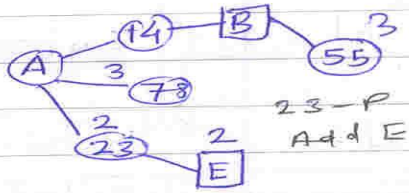
Make 14 permanent & Add B

(iii)



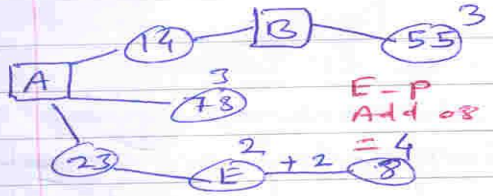
B-P & add 55

(iv)



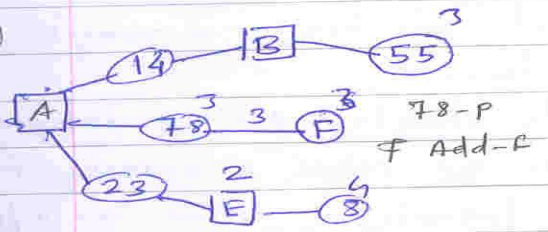
23-P Add E

(v)



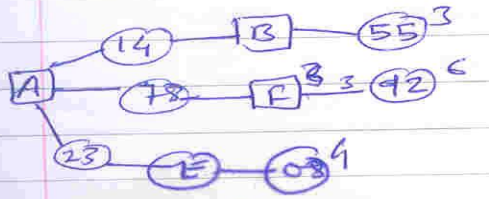
E-P Add 08

(vi)



78-P & Add-F

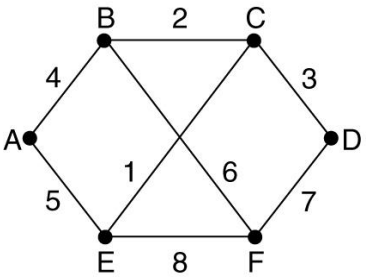
(vii)



∴ Routing Table for A

Net	Cost	Next Router
08	4	E
14	1	
23	2	
55	3	B
66 → 73	5	B
92	6	F

Example From Tanenbaum



(a)

Link State Packets

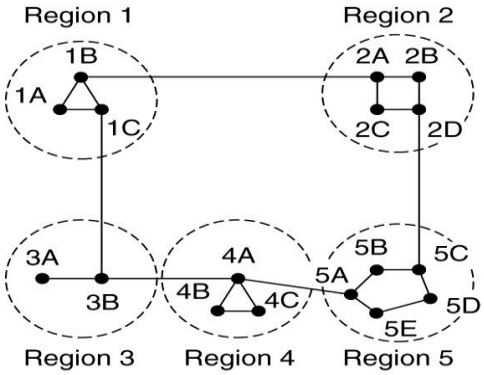
A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

(b)

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Hierarchical Routing

- As network grows in size, the router routing table grows proportionally.
- At certain point the network may grow to the point where it is no longer feasible for every router to have an entry for every other router.
- The solution is hierarchical routing



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Ex. Consider subnet with 720 routers

If no hierarchy, there will 720 entries in the routing table.

Consider two level hierarchy: If subnet is partitioned into 24 regions of 30 routers each, each router need 30 local entries and 23 remote entries so total 53 entries in the routing table.

Consider three level hierarchy: 8 clusters, 9 regions and 10 routers in each region. In this case each router needs 10 local router entries, 8 region entries and 7 clusters entries so total 25 entries only.

Routing in Internet Intra-autonomous: Within AS : RIP,OSPF and IS-IS

Inter-Autonomous: Between different AS: BGP

Scaling and Administration

Routing Information Protocol (RIP)

Developed by Xerox n/w System

Firstly distributed by BSD Unix 1982

Uses Distance Vector Routing Algorithm

Uses Hop as a metric

Cost of each link is 1

Max cost is limited to 15

Information exchange Interval is 30 sec

Request and reply advertisement

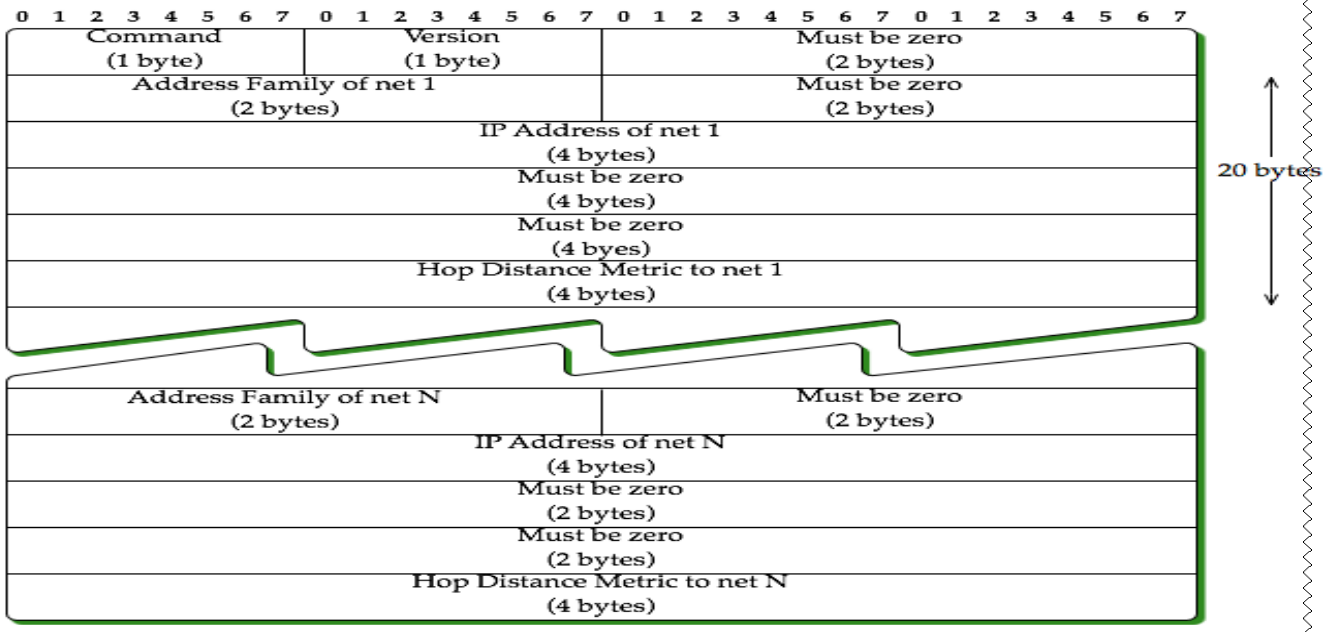
Shares information only with neighbors with fixed interval

Uses Three Timers: Periodic, Expiration and Garbage Collector

Periodic timer: is used for sending the messages for every 30 second

Expiration Timer: If there is no response within 180 seconds, this timer declares the route is dead.

Garbage collector timer: After second timer third timer sets hop=16 for another 120s and finally purge the route and declare another route.



OSPF(Open Shortest Path First) – Interior Gateway Routing Protocol

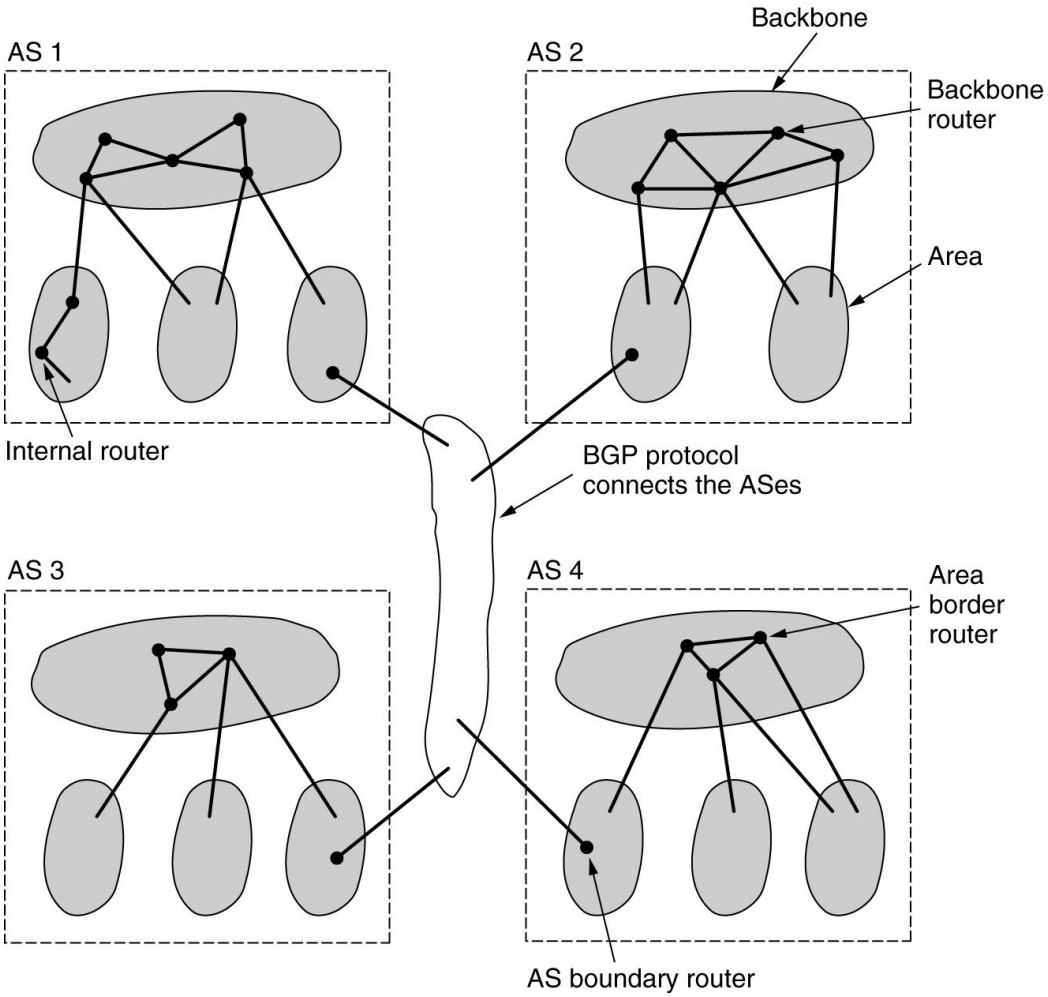
- Specially designed for Intra-domain (Autonomous System) routing in an IP network.
- OSPF is an instance of Link state protocol based on hop-by-hop communication of routing information. Uses Link State Advertisement Types (LSA).
- Locally runs Dijkstra's shortest path algorithm
- Weights can be assigned by administrator
- Ability to cluster the entire domain into several sub domains by introducing hierarchy.
- Network Hierarchy.
- Routing Computation and Equal-Cost Multipath
- Time intervals are: initial flooding 1s, New Packet 5s and Failure 30 min.
- Support for unicast and multicast routing
- Defines four types of link : PTOP, Transit, Stub, Virtual
-

Router Classification:

- Internal Routers: Routers in each low-level area that have interfaces only to other internal routers in the same area

- Area-Border Routers: Each area-border router must have at least one interface to the backbone
- Backbone Routers: These routers are located in Area 0 with at least one interface to other routers in the backbone

- AS Boundary Routers: These routers are located in Area 0 with connectivity to other AS. It handles more than one routing protocol



OSPF Messages:

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

Uses two sub protocols : Hello Protocol and Database Synchronization Protocol

BGP (Boarder Gateway protocol) – Exterior Gateway Routing Protocol

It is inter-autonomous routing protocol (Connecting **boundary routers**)

Default standard for Internet since 1989

Current version is BGP4

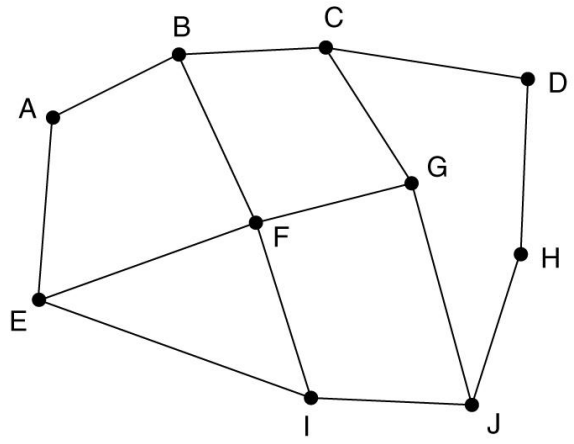
Uses path vector routing algorithm which specifies complete path not only hops.

NW No.	Next Router	Path
N-01	R05	AS14,AS23,AS67
N-02	R08	AS67,AS09,AS34

It uses path vector messages.

Boundary routers share their information with other boundary routers.

Boundary routers are collecting information from their core routers



(a)

Information F receives
from its neighbors about D

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

Divides the network in three groups

Stub network – only one path

Multiconnected network – may be used for transit

Transit network - Backbone

Uses Four Message Types

Open , Update, Keepalive and Notification

Uses Policy based routing

Ex. Never put Iraq on the route of Pentagon.

Path attributes are: weight, Local performance and origin

ICMP

- Internet Control Message Protocol packets are used for various control purposes. Here are some common ones:
- Time exceeded: TTL hit 0.
- Echo request: Can you hear me out there?
- Echo reply: Yes I can hear you.
- Source Quench: Stop sending so much data.
- Timestamp request/reply (as echo but with times).

ICMP: Internet Control Message Protocol

Used by hosts, routers, gateways to communication network-level information

error reporting: unreachable host, network, port, protocol

echo request/reply (used by ping)

Network-layer "above" IP:

ICMP msgs carried in IP datagrams

ICMP message: type, code plus first 8 bytes of IP datagram causing error

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

Type Code description

0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

ARP– The Address Resolution Protocol : IP To MAC

Used to map IP address to MAC Address

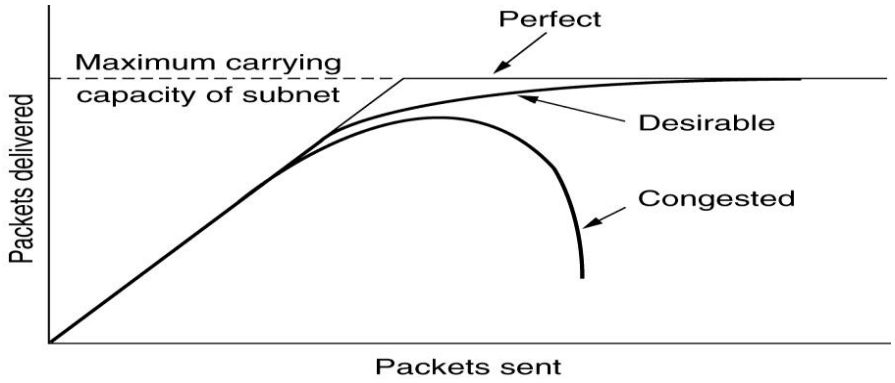
Broadcasts the packet with IP address called ARP request packet

Destination machine matching IP address sends ARP Reply

Congestion Control

Principle: Congestion control has to make sure that subnet is able to carry the offered traffic.

- When too many packets are present in the subnet performance degrades- this situation is called congestion.
- When traffic increases routers are no longer able to cope and begin losing the packets
- At very high traffic, performance collapses completely
-



What Causes Congestion at switching points?

- Three Four input lines, all needed same output line
- Insufficient memory at router looses the packets
- Infinite amount of memory causes timeouts and retransmissions
- Slow Processors at router can lead congestion
- FIFO Policy introduces delay for short packets.

Open Loop Solution

Tempt to solve the problem by providing good design

Early solution and not in middle

Decide whether to accept or not accept given traffic or new connection

When to discard new packet and which one

Closed Loop Solution

Feedback method

Monitor and detect when and where congestion occurs

Pass this information to action taken points

Adjust system operation to correct the problem

What causes Congestion	Solution to it
Retransmission Policy	Use Selective Repeat

Out of Order Packet	Selective Repeat
Acknowledgement	Piggybacking
V/c using Datagram	Queuing and Service policy
Routing	Spreading traffic over all line
Time out	Average time out , not short or long

Policies Affecting Congestion at different Layers

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Congestion Prevention Policies for Virtual Circuit (Connection Oriented)

Admission Control

- Once the congestion has been signaled, no more virtual circuits are setup/allowed until the problem has gone away

- Approach is simple and easy to carry out but it is crude.

- In the telephone system when switch gets overloaded, it also practices admission control by not giving dial tone or feedback message.

- Alternate approach is to **allow new virtual circuits but carefully route** all new virtual circuits around problem areas. That is path should omit the congested router by giving alternate path.

- Another strategy is to **negotiate an agreement** between the host and subnet when virtual circuit is setup. This agreement will specify volume and shape of the traffic, quality of service required and other parameters. In this case **subnet will reserve the resources**.

- Six connection of 1 Mbps each for line of 6 Mbps capacity and mark it full.

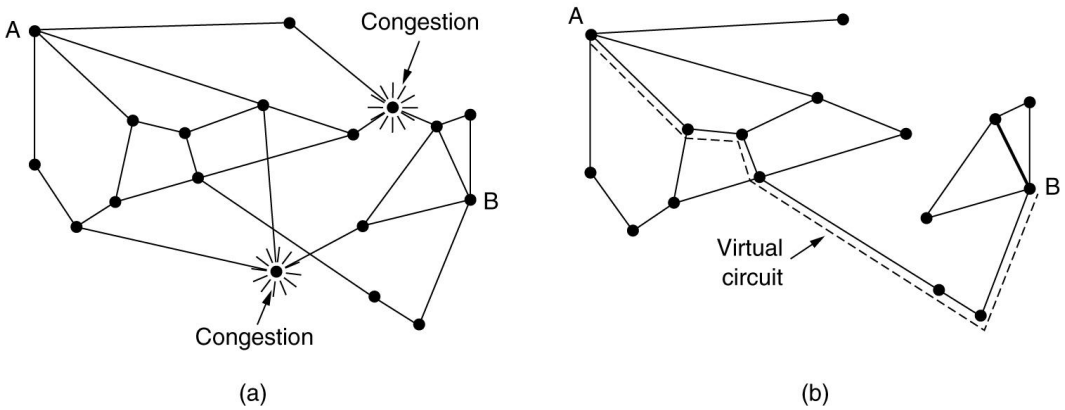


Fig (a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.

Congestion Prevention Policies for datagram Subnets (Connectionless)

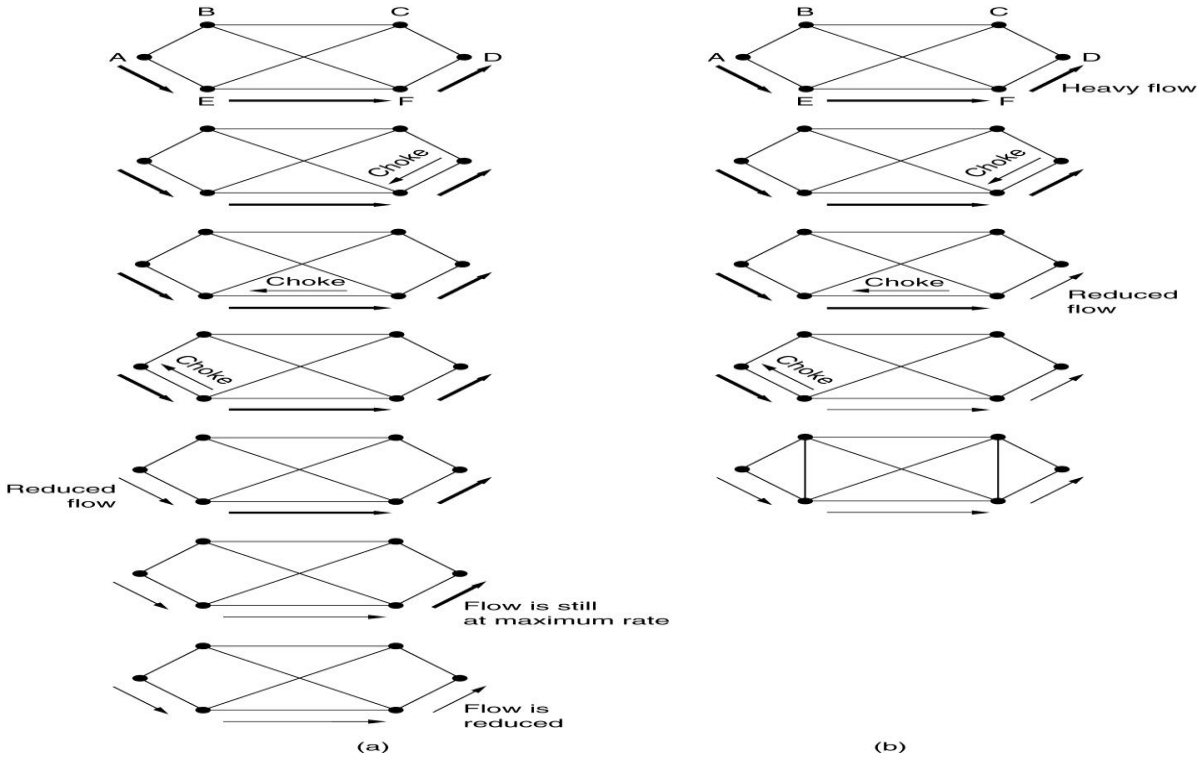
Warning Bit Method.

In the old DECNET and Frame Relay one of the special bit in the header is set by the router and send to destination and destination send it to source through ACK and the source cut back on the traffic.

Choke packet

Router sends a choke packet directly to source along with the packets going to the source without creating new separate packet. Depending on the congestion router sends mild, stern warning or ultimatum. After receiving choke packet source has to reduce the traffic to the specified destination by X percent.

Hop by hop choke packets



Load shading

Just discards the packets randomly. (Blackout)

Needs Intelligent Policy : FTP – new to be discarded Real Time – old to be discarded

Priority Class : Low priority packet will be discarded

Random Early Detection

Start the action when congestion detected first time and not when situation has become hopeless or worst.

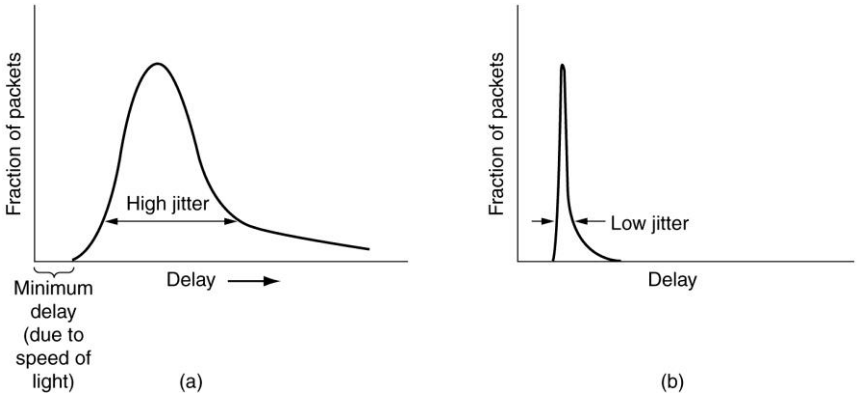
Start the action before router buffer overruns.

Depending on running average of queue length router starts dropping a packet.

Jitter Control

The variation in the packet arrival time is called Jitter.

Expected transit time.
If ahead held up, if behind speed up.
Buffering at receiver is the good solution.



Quality of Service

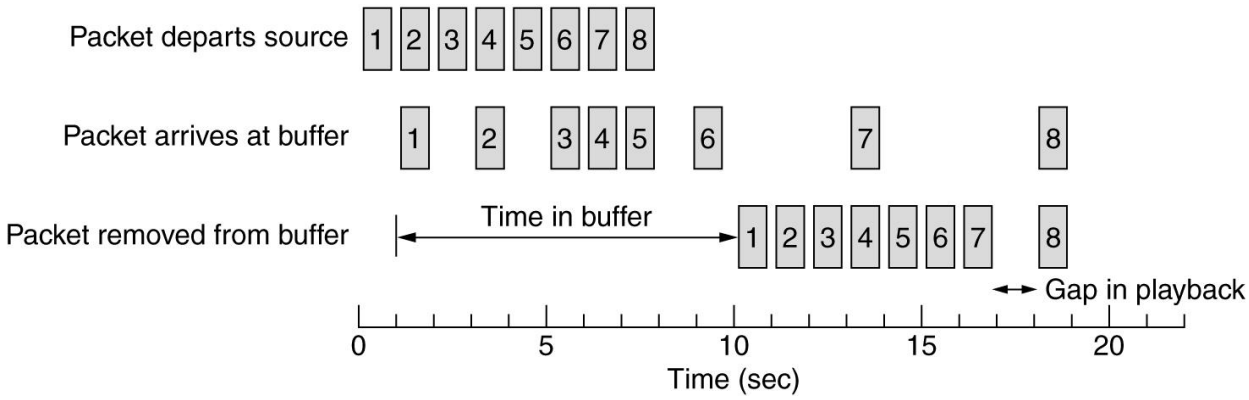
Application	Reliability	Delay	Jitter	B/w
E-mail	H	L	L	L

FTP	H	L	L	M
WWW	H	M	L	M
Rlogin	H	M	M	L
A on demand	L	L	H	M
V on demand	L	L	H	h
Telephony	L	H	H	L
Conferencing	L	H	H	H

Good Solutions

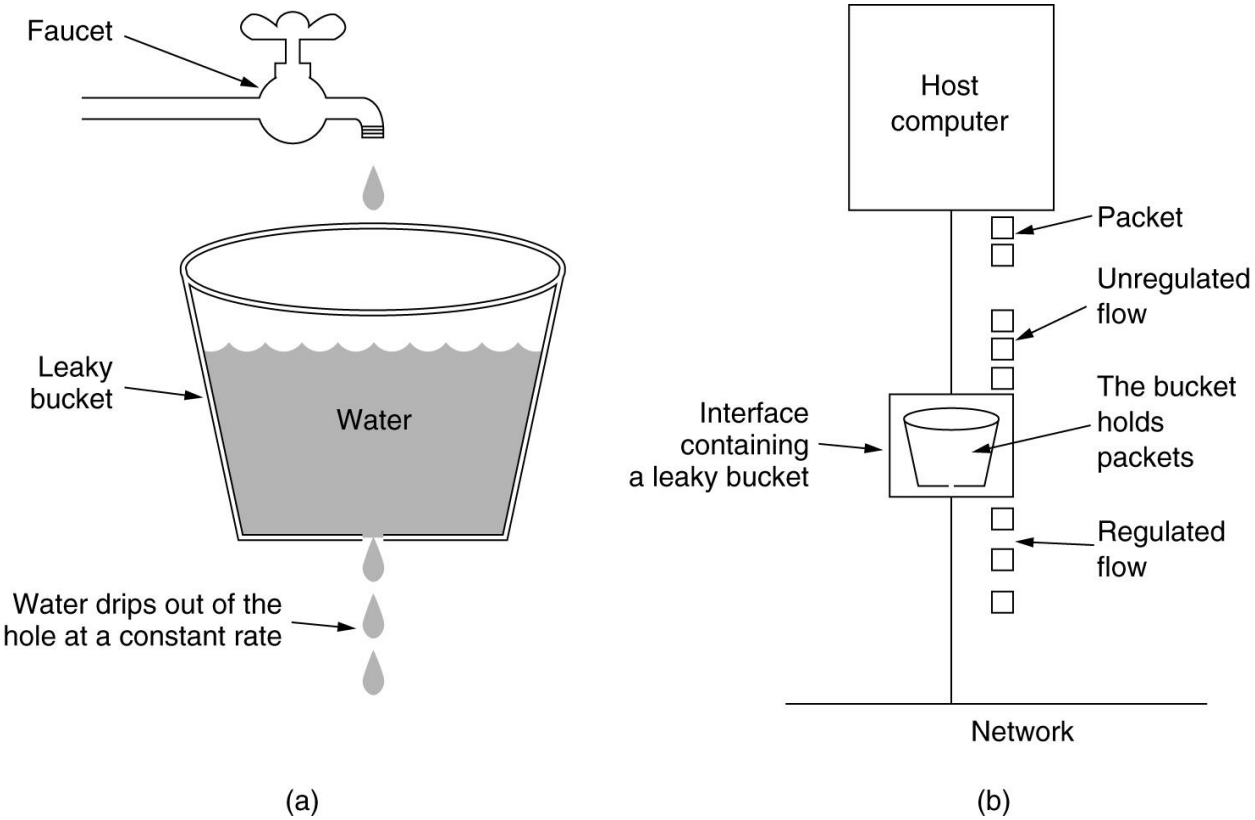
Over provisioning: To provide better router capacity, buffer space and bw.

Buffering: Flows can be buffered at receiver side.

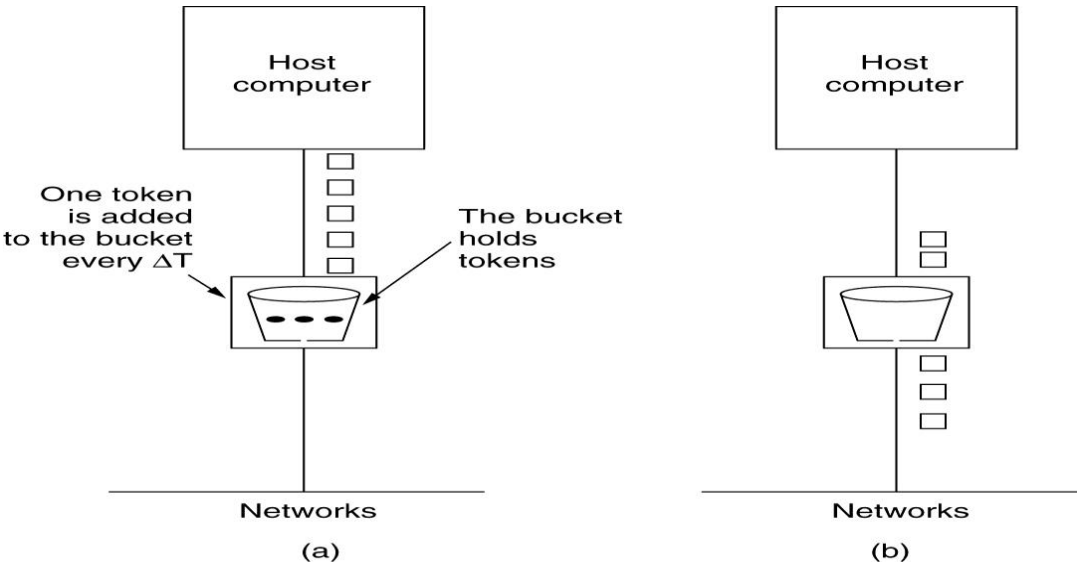


Traffic Shaping: Regulating average rate.

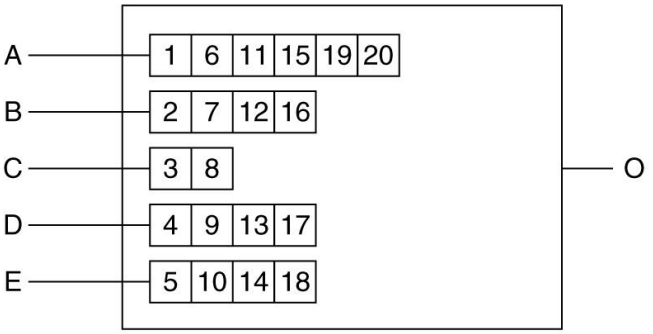
Leaky Bucket : Constant average output



Token Bucket : Capture the tokens



Packet Scheduling

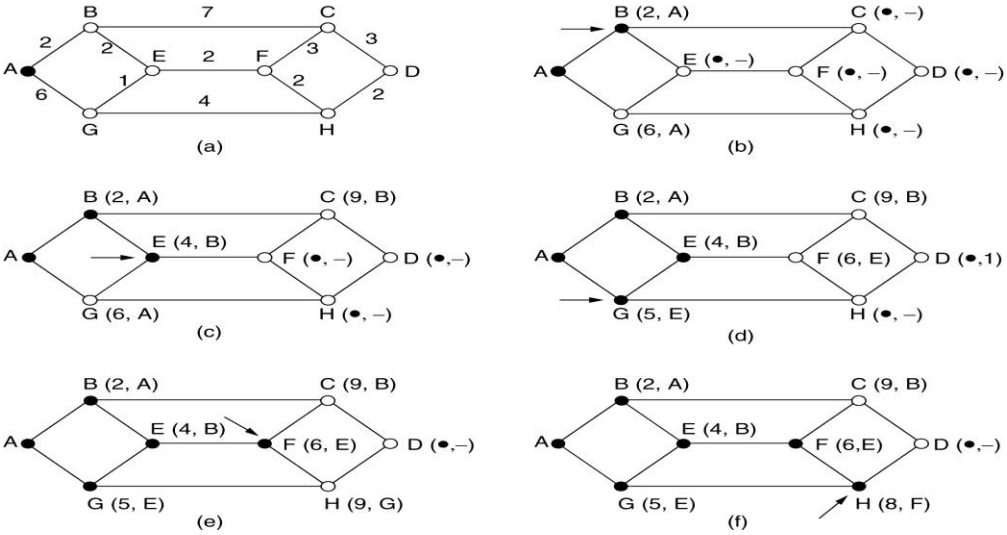


(a)

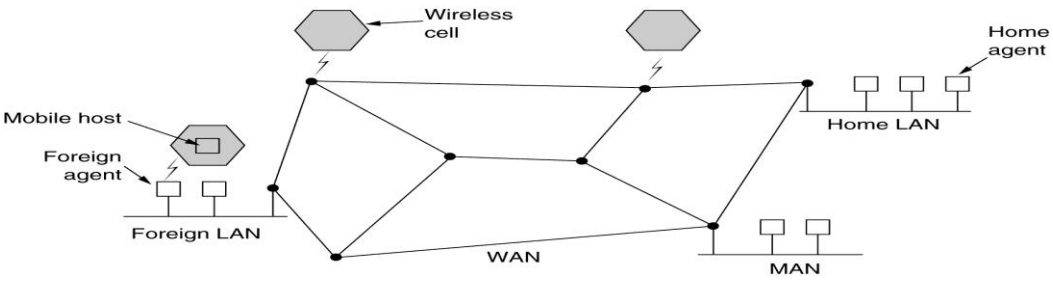
Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

(b)

Example from Tanenbaum

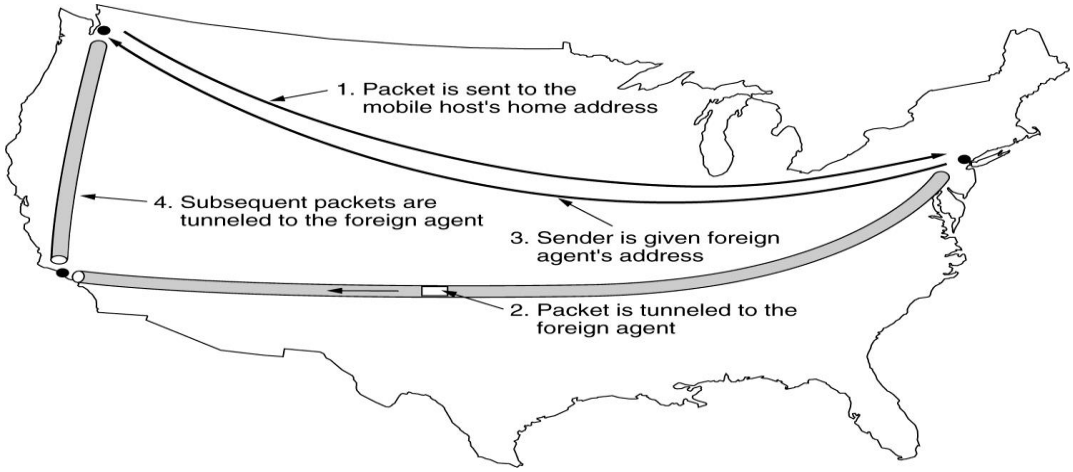


Routing for Mobile Hosts:



- Periodically, each foreign agent broadcasts a packet announcing its existence and address.
- Host enters in new area called foreign area.

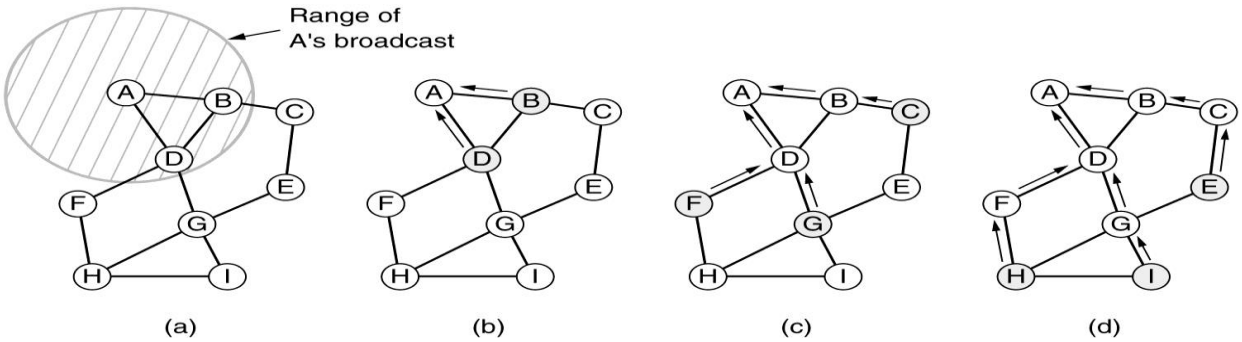
- Mobile hosts registers with foreign agents, giving its home address, current data link layer address and security information.
- Foreign agent contacts the mobile home's agent for cross check examination
- Home agent examines the security information and tells the foreign agent to proceed
- When foreign agent gets the acknowledgement from home agent, it does the registration and offers the network connectivity.



Routing in Ad-hoc networks

Possibilities when the routers are mobile:

- Military vehicles on battlefield -No infrastructure.
- A fleet of ships at sea-All moving all the time
- Emergency works at earthquake-The infrastructure destroyed.
- A gathering of people with notebook computers-In an area lacking 802.11.



One of the popular algorithms is AODV **AD hoc On-demand Distance Vector**

Route request Packet

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

Route reply

Source address	Destination address	Destination sequence #	Hop count	Lifetime

Hop count

Reverse route entry

(a) Range of A's broadcast.

(b) After B and D have received A's broadcast.

(c) After C, F, and G have received A's broadcast.

(d) After E, H, and I have received A's broadcast.

Shaded nodes are new recipients. Arrows show possible reverse routes

IP Addressing Examples

Characteristics of 8-bit block of IP Address

254:1111 1110 = block of 2 addresses

252 : 1111 1100 = block of 4 addresses

248 : 1111 1000 = block of 8 addresses

240 : 1111 0000 = block of 16 addresses

224 : 1110 0000 = block of 32 addresses

192: 1100 0000 = block of 64 addresses

128:1000 0000 = block of 128 addresses

P1	A computer network has 141.14.0.0 IP address. The network has to be divided into four equal sub-networks and each network needs about 16000 IP addresses. Find the subnet mask for subnetted network. How many number of IP addresses will be in each subnetwork? Give the first and last IP address assigned to each block.
Ans	Subnet mask : 255.255.192.0 No. of IP addresses in each subnetwork = 16384-2 Subnet 1 : 141.14.0.1 To 141.14.63.254 (64 x 256) = 16384-2 Subnet 1 : 141.14.64.1 To 141.14.127.254 (64 x 256) = 16384-2 Subnet 1 : 141.14.128.1 To 141.14.191.254 (64 x 256) = 16384-2 Subnet 1 : 141.14.192.1 To 141.14.255.254 (64 x 256) = 16384-2
P2	Suppose that instead of using 16 bits for the network part of a class B address originally, 20 bits had been used. How many class B networks would have been? A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle?
Ans	With a 2-bit prefix, there would have been 18 bits left over to indicate the network. Consequently, the number of networks would have been 218 or 262,144. However, all 0s and all 1s are special, so only 262,142 are available. The mask is 20 bits long, so the network part is 20 bits. The remaining 12 bits are for the host, so 4096 host addresses exist.
	A block of addresses is granted to a small organization. We know that one of the address is 205.16.37.39/28. Calculate the size of block? 16 What will be first IP address? 205.16.37.32 What will be last IP address? 205.16.37.47
P3	An organization has an IP address 192.1.20.0 and need to create four sub networks. Find the subnet mask and give ranges of all sub networks in a decimal dotted form.
Ans	IP 192.1.20.0 Subnet mask 255.255.255.192

	Sub networks are 192.1.20.0 to 63 64 to 127 128 to 191 192 to 255
P4	How CIDR can assigns block of 2,4,8 and16 IP addresses using IP4? Give the prefix and netmask for above four blocks.
Ans	Find the block of addresses from CIDR address 167.199.170.82/27. How many addresses it can support? Show manually the first and last IP address in the block. Number of addresses in the block are 232 – 227 = 25 = **32** = 5-bits for host id IP Address in Binary 10100111 11000111 10101010 01010010 167.199.170.82/27. First address 10100111 11000111 10101010 010**00000** ie 167.199.170.64/27 Last Address 10100111 11000111 10101010 010**11111** ie 167.199.170.95/27 Therefore Number of IP Addresses in Block are=32 Therefore first address will be 167.199.170.64/27 Therefore last address will be 167.199.170.95/27
P5	A block of addresses is granted to a small organization. We know that one of the address is 205.16.37.39/28.
Ans	Calculate the size of block? 16 What will be first IP address? 205.16.37.32 What will be last IP address? 205.16.37.47
P6	You have a class A network address 10.0.0.0 with 40 subnets, but are required to add 60 new subnets very soon. You would like to still allow for the largest possible number of host IDs per subnet. Which subnet mask should you assign?
Ans	40 subnets : needs 6 bits for host id Additional 60 subnets : needs 6 bits for host id Total 40+60 = 100 needs 7 bits for host id Therefore 7 bits will be used from second octant from left 10.0.0.0

	255.**11111111**0.0.0 = 255.254.0.0
P7	What is the network address and host address in IP address 227.77.33.88.
Ans	No network-id or host-id It is class D address
P9	Suppose that instead of using 16 bits for the network part of a class B address originally, 20 bits had been used. How many class B networks would have been?
Ans	2^{18} = 262144-2 =262142
P10	A class B network address 130.50.0.0. is subneted as follows. The last 10 bits of the hosts id are allotted for host number and the remaining 6 bits are reserved for subnet number. How many subnets and hosts are possible with the above addressing scheme?
Ans	6 bits for subnet id = 2^6 = 64-2 = 62 subnets 10 bits for hosts = 2^{10} = 1024 -2 = 1022 hosts per subnet