CN series 2

ASWIN.M.PRABHU

1) Flooding adopts the technique in which every incoming packet is sent in every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. Sequence Numbers, or Hop count and spanning tree maybe adopted to solve these problems.

Advantages situations

1) In military applications, where large numbers of routers may be blown to bits at any instant, the tremendous robustness of flooding is highly desirable
2) As a metric against which other routing algorithms can be compared. Flooding always ~~chose~~ chooses the shortest path because it chooses every possible path in parallel. so no other algorithm can produce a shorter delay.

- When a packet is sent to a mobile host, it is routed to the host's home LAN and is intercepted by the home agent there
- The home agent then looks up the mobile host's new location and finds the foreign agent handling the mobile host
- The home agent does 2 things -
  1) It encapsulates the packet in the payload field of an outer packet and sends the latter to the foreign agent (Tunneling)
  2) It tells the sender to hence forth send packets to the mobile host by encapsulating them in the payload of packets explicitly addressed to the foreign agent instead of just sending them to the mobile hosts home address
- Subsequent packets can be routed directly the host via foreign agent

2) Techniques for achieving good quality of service

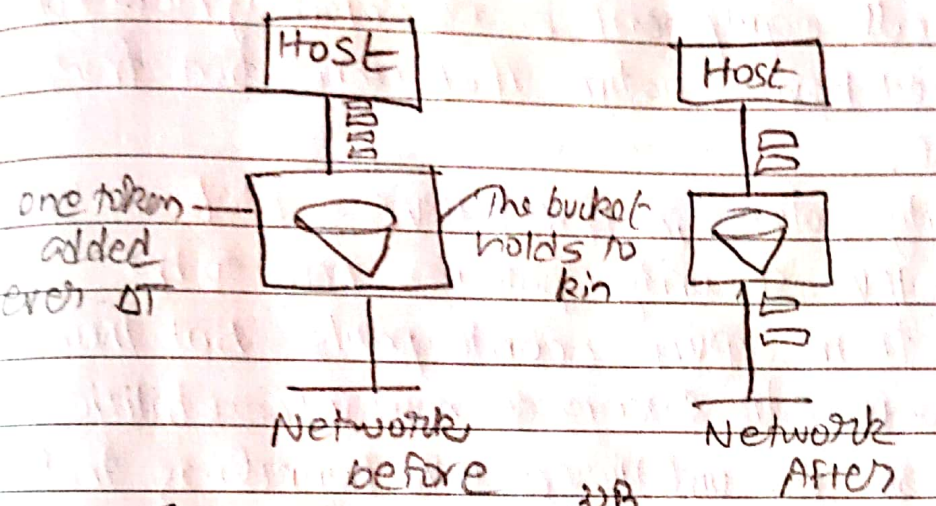
* Overprovisioning - provide so much router capacity, buffer space and bandwidth that the packets flow easily. This is expensive

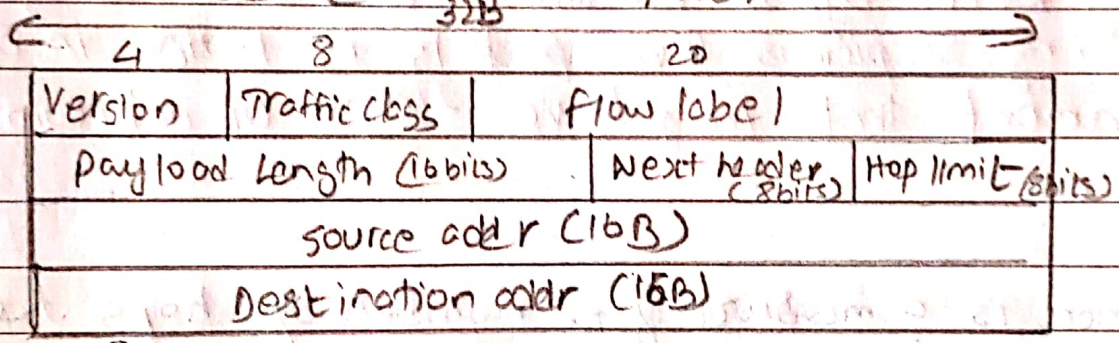
* Buffering - Flows can be buffered on the receiving side before being delivered. Buffering them does not affect the reliability or bandwidth but increases the delay and smooths out jitter. For audio and video on demand, this is the best soln

* Traffic shaping - Make the server transmit at a uniform rate, smooths the traffic at server side than client side.
  - It regulates the avg rate of data transmission. On connection, the user and subnet agree on a traffic pattern which is called service level agreement
  - It reduces congestion. Agreements are important for audio/video which have strict QoS requirements but not file transfer
  - Monitoring traffic flow is called traffic policing. Easier with data gram subnets
  - Algorithms used include
    - Leaky bucket - enforces rigid o/p pattern at avg rate
    - Token bucket - allows output to speed up on burst

4) Tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some busty packets are transmitted at the same rate if tokens are available and thus introduces some flexibility.

for some apps, it is suitable if the app speeds up on large bursts.
1) At regular intervals, tokens are thrown into the bucket.
2) Bucket has a max capacity
3) If there is already a ready packet, a token is removed from the bucket and packet is sent.
4) If there is no token in bucket packet cannot be sent.





* Version (4 bit) - 6 for IPv6
* Traffic class (8 bits) - to distinguish between packets with different real time delivery requirements
* Flow label (20 bits) - will be used to allow a source and destination to setup a pseudo connection with particular properties and requirements
* Payload length (16 bits) - tells how many Bytes follow the 40B header
* Next header (8 bits) - tells which of the 6 extension (optional) headers follow this one. If this last header, it tells which transport protocol handler to pass packet to
* Hop limit field (8 bits) - used to keep packets from living forever
* Source addr (16B) - addr of sender
* Destination addr (16B) - addr of recepient
written as 8 groups of 4 hex digits with colons in between

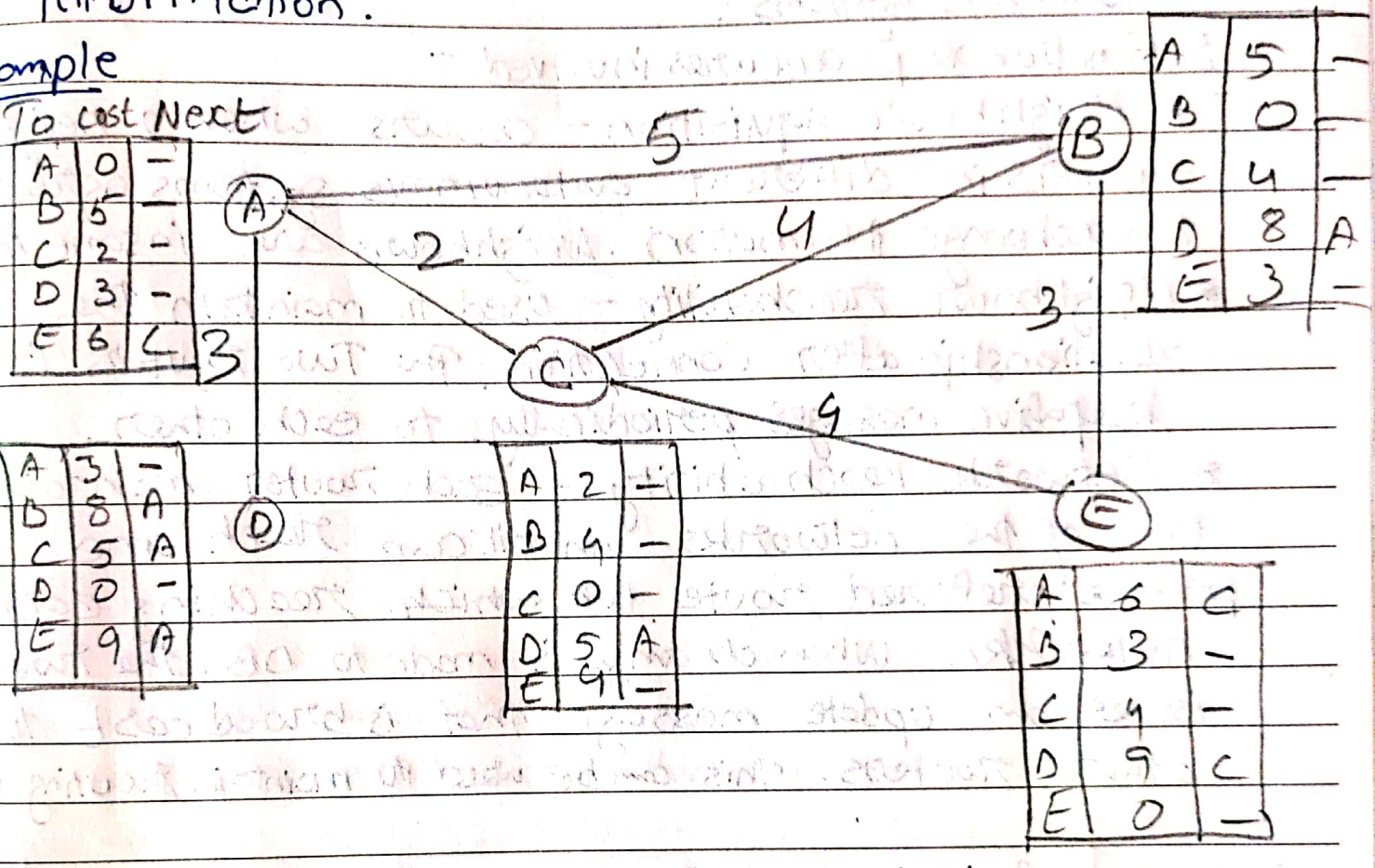
6) * Lack of IPV6 security training/education - Enterprises must invest time and money in IPv6 from security training upfront before deploying. Network security is more effective as a part of planning than after deployment.
* Lack of IPv6 support at ISPs and vendors. - A test network and test plan for all protocols involved must be developed to test all equipment - especially new tech from vendors. Not having native IPv6 connection from provider is an issue.
* Congruence of security policies in IPV4 & IPV6 - Not only do the depth of the IPV6 security policies need to be equal to that of their IPV4 counterparts but their breadth must be wider to encompass new vulnerabilities
* Security device bypass via unfiltered IPV6 tunneling traffic - Recognizing suspicious IPV6 packets is hard in an environment that may have rogue or unknown tunnel traffic.

7) a) Distance is a measure of the number of hops the packet requires to reach the destination. Here vector is defines as (Distance, Direction) of next hop router to which packet is forwarded. Also known as Bellman Ford algorithm. In DVR, each node shares its routes in the network only to the neighbours and does not broadcast it. whenever any node receives the routing information it updates its own routing table and informs its neighbours.
working
1) Firstly each node enters the cost of the neighboring node
2) A link that is down is assigned a cost is assigned to infinity

3) Every node that sends a message directly connected to the adjacent node about the adjacent neighbours and their cost.

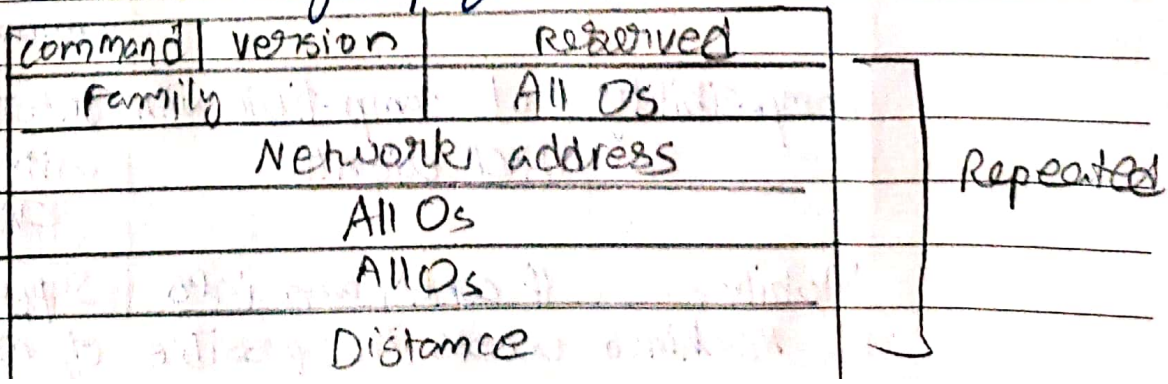
4) After exchanging the nodes information it will find the ~~bases~~ least cost to reach the other nodes information.

Example



b) Routing Information Protocol is an intradomain routing protocol used inside an autonomous system. RIP is a distance vector protocol that uses hop count as its primary metric. RIP defines how routers should share information when moving traffic among and interconnected group of LANs.

Message format



9)a) Broader Gateway protocol is the protocol underlying the global routing system of the internet. It manages how packets get routed from network through the exchange of routing and reachability info among edge routers. It directs packets between autonomous systems.

3 Functional procedures involved -

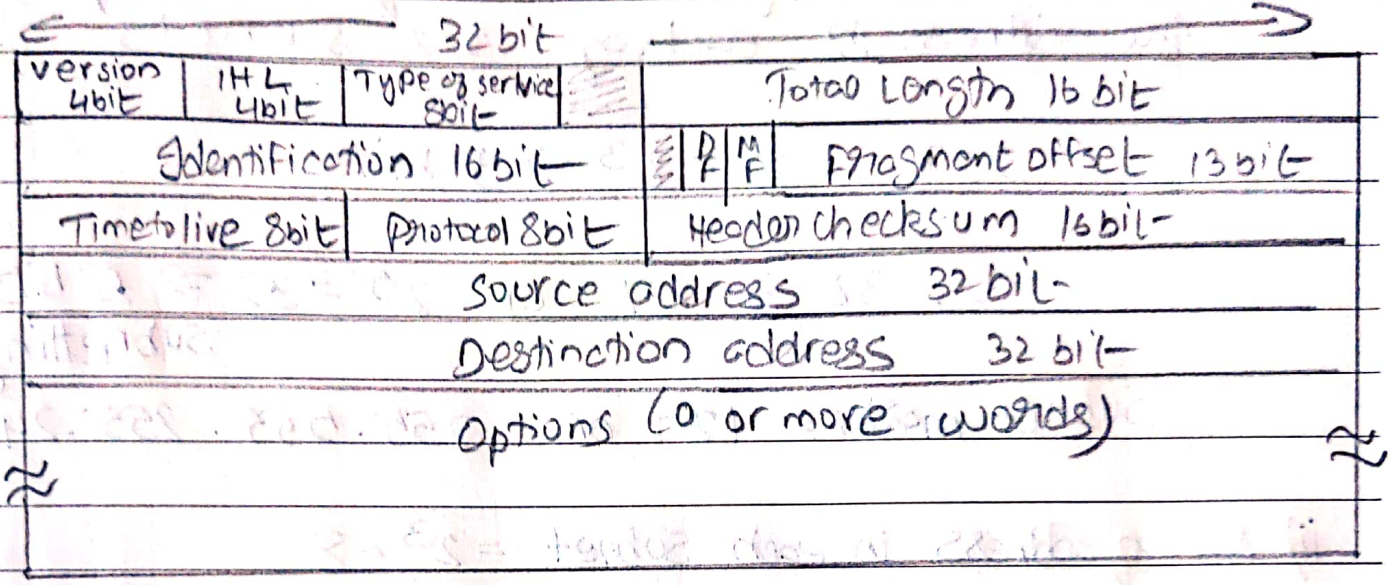
* Neighbour aquisition - occurs when 2 neighbouring routers in different autonomous systems agree to to exchange information. Neighbours are in same network
* Neighbour reachability - used to maintain the relationship after connection. Two routers issue keepalive messages periodically to each other.
* Network Reachability - Each router maintains a DB of the networks that it can reach and ~~prefers~~ preffered route for ~~which~~ reaching each network. When change is made to DB, the router issues an update message that is broadcast to all other routers. This can be used to maintain routing info

b)

Basis	BOOTP	DHCP
Autoconfig	Not possible, only manual	It automatically obtains and assigns addresses
Temporary IP addressing	Not provided	Provided for a limited amount of time
compatibility	Not compatible with DHCP clients	Interoperable with BOOTP clients
Mobile machines	IP config and info access not possible	Supports mobility of machines

	Error occurrence	Manual config prone to errors	Auto config immune to errors
	usage	Provides the information to the diskless computer or workstation	It requires disks to store and forward the information

8) a)



- version - indicates version of protocol
- IHL - IP Header length, in 32 bit words. Min is 5
- Type of service - distinguish between classes of service
- Total length - Len of header and data. Max is 65,535 B
- Identification field - to allow destination host to determine to which datagram does a fragment belongs to
- DF - Dont Frag Fragment flag
- MF - More fragments flag. All except last have this bit set
- Fragment offset - where in datagram the fragment belongs
- Time to live - is a counter used to limit packet lifetimes
- Protocol field - tells it which transport process to give to
- Header checksum - verifies header only
- Source and destination address - for sender and receiver

- options field - to allow subsequent versions of the protocol to include info not in original design.

8)b) Block of 211.17.130.0/24 subnetted into 32 subnets

i) ~~Given block~~ Only 3 bits require to represent the address in each of 32 subnets

$$\frac{256}{32} = 8 = 2^3 \Rightarrow 3 \text{ bits}$$

$\therefore 32 - 3 = 29$ or $2^5 = 32 \Rightarrow$ 5 bits for subnetting

Subnet mask = 129 or 255.255.255.248

ii) No of address in each subnet $= 2^3 = 8$

iii) Subnet range - 00000yyy

First address

00000000 :- 211.17.180.0/29

Last address.

00000111 :- 211.17.180.7/29

iv) Subnet range = 11111yyy

First address

11111000 - 211.17.180.248/29

11111111 : 211.17.180.255/29