first 64 bits → network

second 64 bits → Interface ID

14/12/2023

→ Header size
  - → TCP: 28 bytes
  - → UDP: 8 bytes

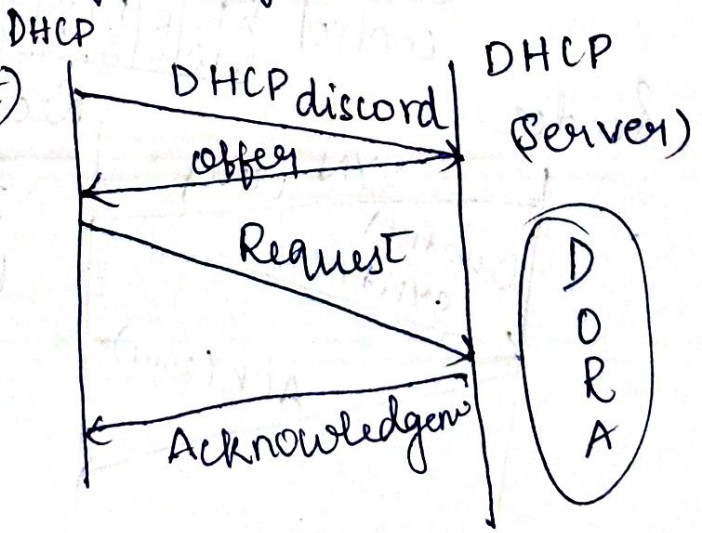
* → TCP: end to end processing connection
* → Establishing a network takes 3 steps.
* → Removing a network connection takes 4 steps.

21/12/2023

→ ARP: Address Resolution Protocol
  - → resolves IP to MAC
    length of MAC = 48 bits

→ DHEP: Dynamic Host Configuration Protocol.

→
  - → provides: IP address, Subnet Mask, default gateway, DNS server address.

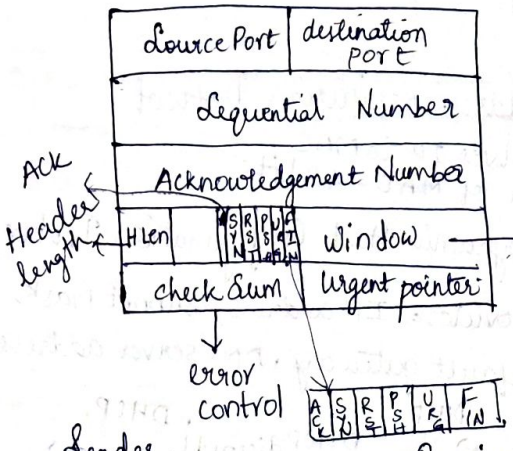


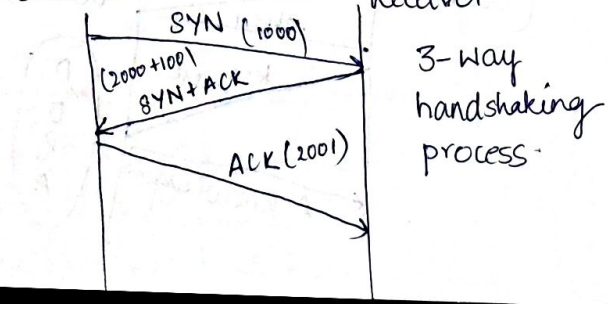
→ Elements of ~~TCP protocol~~ Transport/TCP protocol

- → Addressing
- → Flow control & Error Control.
- → Connection Establishment / Release
- → Multiplexing & ~~De~~ Demultiplexing.
- → Crash / Error recovery.

→ Flow ~~and Error~~ control are not possible in UDP protocol.

*→ TCP header: (20 byte) Max (60 bytes) ⇒ Can be extended.



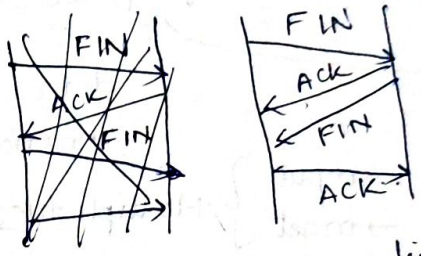


→ RST is set; if the connection is lost suddenly; ~~the~~ the connection can be RESET to 1.

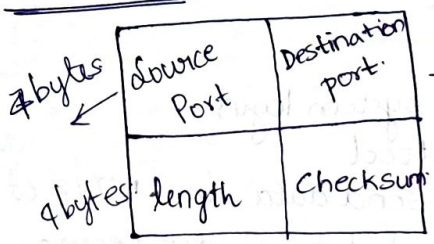
→ PSH, URG.

→ FIN

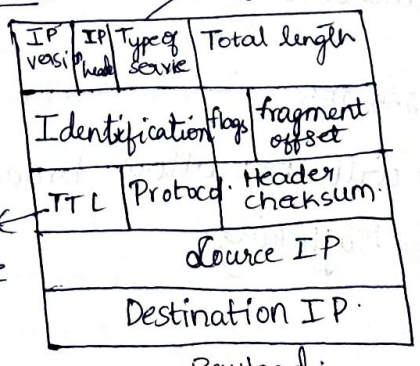
&



*→ UDP header: → video & audio streaming.



*→ IP header: → gives the priorities of requests.



Flags

- unused
- more fragment
- no more fragment

X10 → tells the receiver that more packets are arriving.

X01 → tells the receiver to close the connection

* → Default port no. of ftp: 20 & 21
  - 20 → data connection
  - 21 → control connection

functions

- → put | → mput } Multiple files
- → get | → mget } Multiple files

Single file.

* → telnet: (23)
  - → remote system login
  - → TCP protocol
  - → Do not send data in encrypted form and data is not secure.

* → Limited and direct broadcast addresses.
  - ↓
  - 255.255.255.255.
  - → routers will not allow broadcast address trafficking.

→ What are the fields required to reassemble the fragments at receiver in IP address?
  - → flags & fragments.

→ Application Layer Protocols.

* ICMP: Internet Contrd Msg protocol
  - → Network layer
  - NAT

* → DNS: Domain Name Server / System
  - → resolves domain name to IP address
  - → 2 ways: iterative & recursive

resolver is used to find the IP address. to resolve domain to IP in systems.

* 5 tuple of DNS
  - → Domain Name
  - → Time to leave
  - → Class (IPv4 | IPv6)
  - → Type
  - → Value

* → Telnet & FTP uses TCP protocol.

* 200.40.50.60 /24

255.255.255.0

200.40.50.0 → Network.

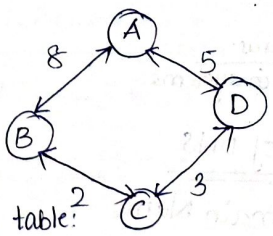
200.40.50.255 → Broadcast.

* Tcp connections needed in FTP: 3-way hand shaking.

* 3 Main divisions of DNS:

  - → Generic Domains
  - → Country domains
  - → Inverse domains

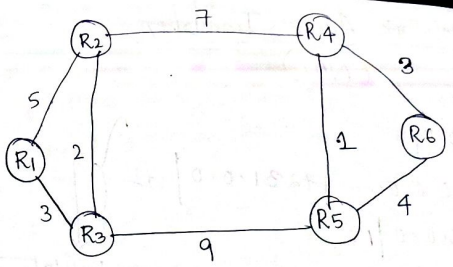
* Problem:



A's routing table:

destination address	Distance	next hop
A	0	A
B	8	B
C	8	D
D	5	D

B ↔ C ⇒ unused



R1 → R6

R1 — R3 — R2 → R4 — R6

→ Take the unused links and reduce the distances by 2 (or) any value

* 172.16.0.0/20 ⇒ * Subnet into 8 subnets
255. ↓ for network * Subnet Mask
* ~~Subnet weight~~
* Calculate range of each subnet.

→ 20 bits are there for network.

→ 11111111.11111111.1111 0000.00000000/20

1111 1111.1111 1111.1111 1111.0000 0000/20

→ Subnetmasking

* Network Address Translation (NAT)

10.0.0.0/8
172.16.0.0 — 172.31.0.0/12
192.16.0.0/16

} private addresses

22/12/2023

→ Given IP address: 10.15.20.60

Address class:

class A: 10.0.0.0 to 126.255.255.255

class B: 128.0.0.0 to 191.255.255.255.

class C: 192.0.0.0 to 223.255.255.255.

∵ 10 is given ∴ IP address will be in class A.

In class A; first octet represents network and remaining 3 represent host

⇒ Network IP address : 10.0.0.0

Direct Broadcast address:

↳ In class A; direct broadcast address is obtained by setting all host bits to 1 in host portion of the address.

⇒ 10.255.255.255.

Limited broadcast address:

↳ is always 255.255.255.255. regardless of IP address class.

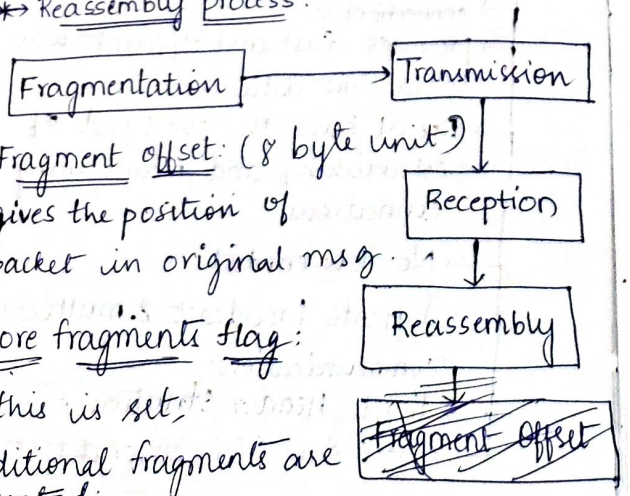
→ Key features of UDP:

- → Transport layer protocol.
- → connectionless.
- → provides fast and efficient way to transmit data.
- → Doesn't have the overhead of establishing and maintaining connections.
- → No flow control.
- → Supports broadcast & multicast communication.
- → Simple Header structure.
- → Check Sum for error detection.

★→ Real-time applications:
- → Voice over Internet Protocol
- → Online Gaming
- → Streaming media
- → DNS queries
- → Internet of things.

→ IP header – Reassembly of fragments:
- ↳ IP protocol allows for the fragmentation of packets when the payload size exceeds the Maximum Transmission Unit (MTU) of the underlying network.

★→ Reassembly process:



★→ Fragment offset: (8 byte unit?) gives the position of packet in original msg.

★→ More fragments flag: If this is set, additional fragments are expected.

★→ Time out mechanism is often employed to manage the reassembly process.

* Complete packet is formed when all fragments are received & reassembled.

★→ Identification field is used to uniquely identify a set of fragments belonging to same original packet.

→ FTP: 3-way hand shaking
- → File Transfer Protocol
- → transfer files b/w client & server on TCP-based network
- → SYN packet: Synchronize signal is sent by the client. Packet also includes the client's initial sequence number (ISN).
- → SYN-ACK packet: On receiving the packet, server acknowledges the request by sending a TCP packet with both SYN and ACK flags set to 1.
- → ACK packet: FTP client acknowledges the server's response by sending a TCP packet with the ACK flag set.

* 3 way handshake ensures that both the client and the server agree on initial sequence number & establishes reliable connection before data transfer.

→ FTP uses 2 separate channels for communication:
- Command channel (Control connection)
- Data channel (additional connections)

* Default port numbers of FTP:
- Data Channel: Port no - 20
- Control channel: Port no - 21

* Default port number for TELNET: port 23

Telnet uses TCP for reliable connection.

TCP SYN → TCP SYN-ACK → ACK.

* Once TCP connection is established, the user is prompted to log into the remote system.

* After successful connection, user enters an interactive session with the remote host.

* TELNET connection allows the user to execute commands & receive responses from the remote host.

* IP address: 220.100.1.1
- to send a packet to all hosts in same network, we use broadcast address.
- Specific broadcast address depends on network's subnet mask.

Network address: 220.100.1.0.

Broadcast address: 220.100.1.255.

⇒ Source IP address: 220.100.1.1

Destination IP address: 220.100.1.255.

* Working of following protocols:

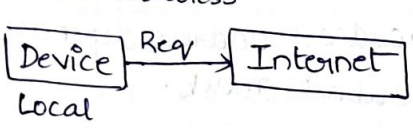
→ DHCP: Dynamic Host Configuration Protocol
- dynamically assigns IP addresses & other network configuration parameters to devices in a network. (diagram)

→ SMTP: Simple Mail Transfer Protocol:
- sending emails b/w servers.
- Client —SMTP→ email server.

- Server —SMTP→ recipient's email server.
- Recipient's email server stores the message until the recipient retrieves it.

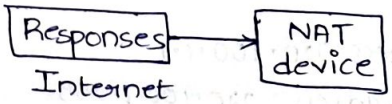
→ **NAT: Network Address Translation:**

- Map private IP addresses within a local network to a single public IP address.



Replaces local source IP addr with its own public IP addr.

→ NAT device maintains a table to track connections.



→ **TCP:** Transmission Control Protocol.

- Reliable, connection-oriented, ordered delivery.
- Establishes connection through 3-way handshake.
- Manages flow control, error checking, congestion control.

→ **ICMP:** Internet Control Message Control:

- used for Network error report & diagnostic
- provides error messages such as ping replies
- used for network testing and troubleshooting

→ **FTP:** File transfer protocol:

- transferring files blw client and server.
- Opens a separate data connection for actual file transfer.
- Supports both active & passive models for data transfer.

→ **TELNET:**

- provides remote access to the system.
- provides terminal emulation over the network.
- Allows user to log into remote host & interact directly.

* **3 Main divisions of DNS:**

- translates the domain name to IP addr
- **Generic Domains:**
  - registered hosts
  - 3 character labels; describes organization type.
  - Ex: aero, biz, com, gov etc.

- Country Domain:
  - 2 character country abbreviations.
- Inverse Domains:
  - Mapping address to a name.

* Address Resolution Protocol:

- Maps IP addr to MAC addr.
- ARP request is a message sent by a device to request the MAC addr. associated with a specific IP addr.

ARP Request Packet

- If required mapping is not found in cache; the device sends an ARP request.
  - Includes: Sender's MAC, IP addresses & target IP & MAC address.
- Broadcasting ARP request:
  - sends this request to all devices.
- Receiving and Responding:
  - device with IP addr mentioned in ARP request responds to request.
  - response; ARP reply: contains MAC addr.
- Updating the ARP cache
  - Requesting device, updates its ARP cache with newly obtained MAC addr.
  - Subsequent data packets destined for that IP addr are encapsulated in Ethernet frames using correct MAC addr.

* Role of Domain Resource Records: (DNS)

- In DNS; Resource Records are fundamental elements that provides various types of information about domain names; mappings, server info.
- Each RR has a specific format and is associated with a particular type.
- Commonly used RR:
  - Address Record (A):
    - Maps domain name to IPv4 addr
    - Ex:
      example.com. IN A 192.168.1.1
  - AAAA (IPv6 addr) record:
    - Maps domain name to IPv6 addr

↳ example.com IN AAAA 2001:

→ (MX) Mail Exchange Record:

↳ Specifies mail servers responsible for receiving email on behalf of the domain.

↳ Ex:

example.com IN MX 10 mail.example.com.

→ (CNAME) Canonical Name record:

↳ creates an alias for existing domain.

↳ Ex:

www.example.com IN CNAME example.com.

→ TXT (text) record:

↳ holds human-readable text associated with domain.

↳ Ex:

example.com IN TXT "This is a text record".

→ NS (Name Server) record:

↳ Specifies authoritative DNS servers for domain.

↳ Ex:

example.com IN NS ns1.example.com.

* WAN link = 2Mbps

RTT b/w source & destination - 300msec.

optimal TCP window size needed to fully utilize the line = ?

Ans: Bandwidth delay product

= Link bandwidth x Round Trip Time (RTT)

= 2 Mbps x 0.3 sec.

⇓

$2\,Mbps = \frac{2\,Mbps}{8} = 0.25\,MBps$

∴ BDP = 0.075 MB.

⇓

convert to bytes

= 0.075 MB x 1024 KB/MB x 1024 bytes/MB

TCP window size = 78,643 bytes.

* Transport layer protocol - transmitting data using FTP/TELNET:

↳ Transport layer protocols: TCP/UDP.

↳ When transmitting data using FTP/TELNET; TCP is primary protocol employed.

* FTP: Role of TCP:

- Reliable and ordered delivery.
- Establishes connection through 3-way handshake before data transfer.
- While data transfer process; commands & responses are exchanged over the control channel; while actual file data is transferred over data channel using TCP.

* TELNET: Role of TCP:

- Reliable; bidirectional communication b/w client & server.
- Ensures commands and responses are delivered in correct order & handles retransmission of lost or corrupted data.
- User I/Ps and O/Ps are transmitted over the TCP connection in text-based format.

* → Given subnet mask: 255.255.255.124

Class C Subnet mask: 255.255.255.0

→ Hence; given subnet mask falls b/w 2 class C Subnets

→ Binary form:

11111111.11111111.11111111.01111100

In this 5 bits are for host addresses.

No. of hosts per subnet $= 2^n - 2$

n = no. of bits for host addresses

$\Rightarrow 2^5 - 2 = 30$

⇒ Each subnet can have 30 hosts.

⇒ No. of bits borrowed for subnetting = 3 bits

$2^3 = 8$ Subnets

* → Leaky Bucket Algorithm:

- Flow control mechanism often used in networking to control the rate at which data is transmitted.
- Primary purpose:
  - Smooth outbursts of traffic and network operates at a steady rate.

* Leaky Bucket Algorithm

- Incoming data is poured into a bucket with a leak.
- bucket has a fixed capacity; if incoming data is too high, it spills out.
- prevents bursty traffic and policing to control the rate of data transfer.
- prevents network congestion
- Quality of service in TCP typically involves factors like latency, packet loss.

* window size = 65538 B.

1Gbps channel

10 ms one way delay.

max throughput = ?

BDP = Link Bdw * Round trip time.

$$\text{Throughput} = \frac{\text{TCP window size}}{\text{RTT}}$$

window size = $65538 \times 8 = 524304$ bits

RTT 1Gbps = 10^9 bits per sec

BDP = 10^9 bps $\times$ (20msec) = 20×10^6 bits

$$\text{Throughput} = \frac{524304}{20 \times 10^6} = 0.026/\text{sec}$$

= 38,044,948 bps.

= 38.04 Mbps.

* CIDR block : 245.248.128.0/20.

→ Subnet sizes = 2^{12} addresses.

→ Divide the CIDR block into 2 parts for organisation A and organisation B

→ Allocate addresses:

- Half of the addresses = 2^{11} = 2048 addr
  - Subnet : 245.248.128.0/21
  - Range: 245.248.128.0 to 245.248.135.255
- Quarter of the addresses = 2^{10} = 1024 ad
  - Subnet: 245.248.136.0/22
  - Range: 245.248.136.0 to 245.248.139.255

→ ISP:

Subnet: 245.248.140.0/21

Range: 245.248.140.0 to 245.248.147.255.

* Header fields in TCP that contribute to reliable and ordered data.
  - → Sequence Number.
  - → Acknowledgement Number.
  - → TCP flags.
  - → Window size.
  - → Check sum.

* Minimum Window size:

Channel utilization >80%.

$$\text{Throughput} = \frac{\text{Window size}}{\text{RTT}} \times \text{Link BW}$$

$$U(\text{Channel utilization}) = \frac{\text{Throughput}}{\text{Link BW}}$$

Link BW = 1×10^9 bps.

RTT = 40 msec = 0.04 sec.

Packet size = 1000 bytes

$U > 80\%$.

Throughput = U x Link BW

$$\text{Window size} = \frac{\text{Throughput}}{\frac{1}{RTT}}$$

$$= U \times \text{Link BW} \times RTT$$

$$= U \times 10^9 \times 0.04$$

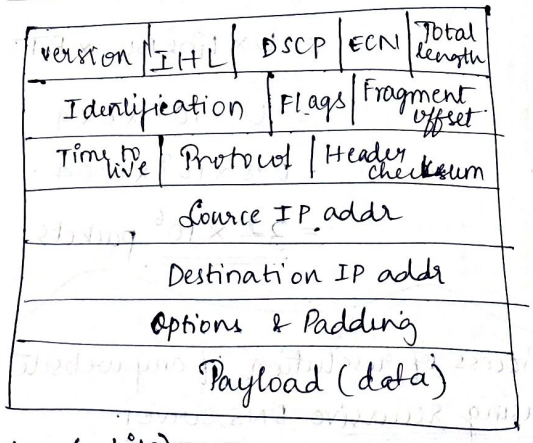
$$= 0.8 \times 10^9 \times 0.04$$

$$= 32 \times 10^6 \text{ packets}$$

* Process of resolution of any website using recursive DNS server.
  - → Understand ethical hacking.
  - → Recursive resolution is a process where the DNS server will continue to search for an answer in lower-level domains.

- Recursive DNS server receives the DNS query from the user's device.
- Cache check: to determine if it has the mapping of the requested domain name to an IP addr.

* IPv4 format:



- Version: (4 bits)
  - Version of protocol (IPv4 / IPv6)
- Internet Header length (IHL): (4 bits)
  - 32 bit words.
  - Starting point of the data.
- Total length (16 bits)
  - header + Payload.
  - Assists routers in processing & forwarding packets.
- Protocol: (8 bits)
  - protocol used.
  - enables routers to determine how to process payload.

* SMTP: Sending and Receiving emails:

→ Sending Email:

- User composes Email
- Email client initiates connections
- SMTP handshake
- Sender authentication
- Email transmission.
- SMTP server routing
- SMTP relay
- Email delivery

→ Receiving Email:

- Email retrieval
- Authentication
- Email download.
- Display & Management.

Characteristics:

- Text-based protocol
- Reliability
- Connection-oriented.

* IP addr: 10.0.0.0/16.

500 hosts per subnet.

$2^x \geq 500 \implies x = 9$.

9 bits for host.

→ No. of bits for subnet = 32 − No. of bits for hosts

= 32 − 9 = 23

→ Subnet mask for the new subnets will be /23.

→ Subnet range = Network Addr. + Incr x Subnet No.

$Incr = 2^9 = 512$

* Subnet 1
  - N.A = 10.0.0.0
  - Range = 10.0.0.1 to 10.0.1.254
  - BA = 10.0.1.255.

* Subnet 2
  - NA = 10.0.2.0
  - Range = 10.0.2.1 to 10.0.3.254
  - BA = 10.0.3.255

* Key Components of DNS:
  - Server, Resolver.
  - Record.
  - Root DNS Servers.
  - Cache.
  - Top-level domain servers.

* Process of domain Name resolution:
  - User initiates request.
  - DNS query sent to resolver
  - Resolver checks cache.
  - Recursive DNS query
  - Root DNS servers.
  - Response sent to resolver.
  - Response sent to user

* Significance:
  - Human-readable names
  - Distributed
  - Navigation
  - Email delivery
  - Dynamic IP addr assignment
  - Global accessibility

* Link State Routing Algorithm:

↳ optimal path for data transmission b/w nodes.

Steps
- Router creates a Link State Advertisement (LSA) containing info about its directly connected links and states.
- Router floods its LSA to all other routers in the network.
- Each router collects LSAs from all other routers in the network and builds its link state database.
- Using LSDB each router runs Dijkstra's algorithm to calculate the shortest path to every other router in network.
- Shortest path tree is used to determine the next-hop router for each destination in the network.
- Routing Table.