Lecture #01 CN 7-9

- Introduction to CN
- Layers
- Protocols
- Performance Measure : Loss , Delay, Throughput
- Security : ISP → Internet Service Provider

SEA - ME - WE

- Packets : Data + Address

① Access Link
② Edge devices
③ Network Core

Packets = 2 L

Link Speed = R (bps)

2R

No. of bits in each packet = L

Packet Transmission delay = $\frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$

→ RJ 11 – ethernet

→ RJ 45 – Telephone (Landline)

→ Routing Algorithm

→ Store & Forward

→ Arrival > Transmission Rate then this cause queue

CN

→ Packet loss

• Time out message - waiting time exceeds ~~from~~ For the server responce.

→ Packets stored in buffer (queuing delay)

① ~~Straus~~ Transmission delay ② Queuing delay

• L → Packet length (bits)

• R → Link transmission rate (bps)

$$d_{trans} = \frac{L}{R}$$

• Type and physical media of transmission

③ Propagation delay

• d → length of physical link

• S → propagation speed ($\approx 2 \times 10^8$ m/sec)

• $d_{prop} = \frac{d}{s}$

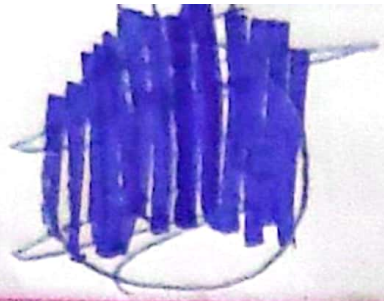
• Length of the media

④ Node delay

• Processing speed in the router

→ Queuing delay

$$\frac{L \cdot a}{L} = \frac{\text{arrival rate of bits}}{\text{service rate of bits}}$$ "traffic intensity"



This is dual damage ⚠

work ⇒ La/R > 1 < La/R → Not Good

=

0

Then Good

→ Security

→ DoS

→ Layers

Principles

Book Pg#133

- P2P
- Client Server

No data loss / Reliable

↑

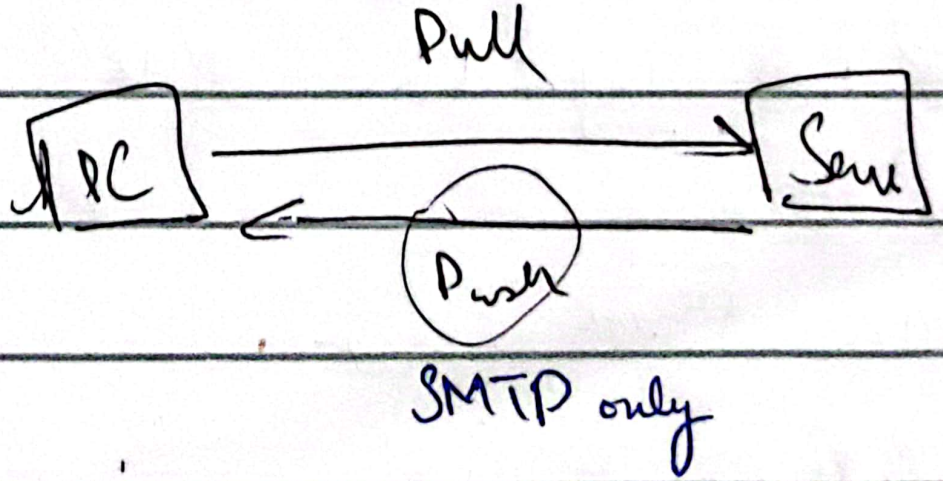
→ Packets => TCP → 100% Packets (Skype)

↓↓ UDP → (whatsapp video call)

TCP → Reliable → Skype Vide Calling

UDP → Not reliable → Whatsapp Calling

- Protocol
- TCP vs UDP
- HTTP
- Presistant HTTP and non-Presistant HTTP
- Cookie



- **Electronic mail**
- **SMTP Protocol** → Use TCP → Complete meal
  - TCP → Reliable → transfer 100% or not
  - UPP → Not reliable → transfer in parts
  - → Use Presistant connections

HTTP → Pull request SMTP → Push request

- **POP3 Protocol**

① Authorize Phase

② Transaction Phase

- **DNS**

CN

19-10

DNS

AQ: how to map between IP address and name, and vice versa?

AQ: When to use cname, record, alias and URL

Attacking DNS

CN

1. TCP Connection Management
- Three way handshake
  (1) Step 1 No data transfer
  (2) Random number is assigned for security purpose (ISN - initial server no.)
  (3) Termination FIN bit
- Life cycle
- ICMP - Internet control menege protocol
- If the ip address does not match then it sends RST (reset segment)

established
↑
0 → stop
1 → start
fin → termination bit

2. TCP
- TCP/IP
- TCP Segment structure

CN

16-11

Switch – Connect multiple devices on the same network (Multiple access points)

Repeater – Retransmit the signal at higher level

Router- Connet two big networks

- OSI Model (7 Layers)

CN

7-12

Simple encryption scheme

→ DES: Data Encryption Standard

→ 3DES

→ AES

→ RSA

→ Digital Signature / Public Signature

Must for desktop application

CN

- Encryption & Decryption
- Modular Arithmatic

CN

19-12

Messege digest - Hash function
- Use to encrypt messege with hexadecimal
- Not so good because change in structure of words doest change in encryption
- Hash function algo
- 5 authentication protocol

Message Security
- Symmetric key - only have one key
- Asymmetric key - 2 keys (one for encryption one for decryption)
- TLS
- 3RTT that makes it slow
- For securing from man in the middle - TLS seq #

CN

$n = pq$ and $z = (p-1)(q-1)$

e $d < n$ d $(ed-1)$ $ed \bmod z = 1$

public key (n, e), private key (n, d)

$c = m^e \bmod n$

Hash function

$m \Rightarrow H(m)$

$m+s \Rightarrow H(m+s) \Rightarrow$ MAC

$H(m+s) = h \Rightarrow$ HMAC

$KB^+(KB^-(m)) = m$

Digital signature

Passive – Becon Active – probe

BTS 2G

BSS → BSC → MSC → MSC Gateway – Telephone

3G

MSC — MSC Gateway

BSS — RNC — SGSN → GGSN → GGSN Gateway

Two main nodes

SGSN and GGSN

Packet Data network Gateway

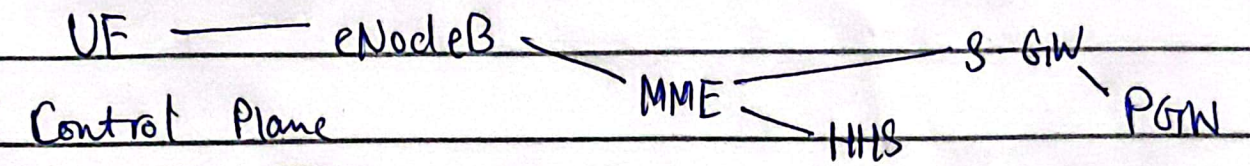
4G - all IP

① → An all IP core network

② → Enhanced radio access network

P-GW Data Plane: Transfer IP-Datagram from UE to P-GW

Control Plane: Involves the coordination of multiple components within the network



eNodeB - Enhanced NodeB

MME - Mobility management entity

HSS - Home Subscriber Server

~~Packet~~ LTE - Long Term Evolution