* Network Access Control (NAC)

Goals

- Prevent zero-day Attacks
- Enforce Security Policy throughout the network
- Use identities to perform Access control

NAC refers to an automated detection & response system that can react in real-time to stop threats as they can occur & before they cause damage or a breach.

NAC = preventive, detective, corrective

NAC Implemented as

Preadmission Philosophy

- Requires systems to meet all security requirements before allowing communication with the network

Security Posture

Postadmission philosophy

- Allows / Denies based on predefined Authorization matrix.

* Firewalls

i) Static packet Filtering Firewall

- 1st generation, layer 3 @ OSI
- filters traffic by examining data from message header.
- No user authentication
- Rules revolve around src, dst & port

Note — firewall provide protection for traffic b/w subnet, not within subnet (no protection behind the firewall)

ii) Application-level Gateway FW

- 2nd generation, layer 7 @ OSI
- Filter traffic based on Application/ Internet Service
- A.K.a = Proxy FW → changes src & dst address to protect identity of private network
- Negatively impact performance as each packet must be examined & processed as it passed through Firewall

iii) ~~Circuit-level Gateway~~ Stateful Inspection FW

- 3rd Gen, layer 3 + 4 @ OSI
- A.K.a = Dynamic packet filtering / stateful inspection
- Evaluate state or context of network traffic such as previous packet of the same session

stateful

v) Deep Packet Inspection Fw (DPI)

- Layer 7

PAYload = deep

- filter payload content of communication along with the header values
- A.k.a = complete inspection / information extraction (IX)
- Block malware, spam, block domain names
- often integrated with App. Fw.

vi) Next-Gen Firewalls

- IPS / IDS, TLS / SSL proxy
- Antivirus
- Bandwidth throttling
- VLN Anchoring
- QoS Mangent
- Web filtering

(iii) circuit-level Gateway Fw

- layer 5 @ OSI
- Used to establish communication session b/w trusted partners.
  (E.g SOCKS (socket secure))
- A.k.a = circuit proxy - they merge comms based on circuit, not content of traffic
- 2nd Gen

Multi / Dual-Homed Firewalls

- At least has two interfaces to filter traffic
- IP forwarding should be disabled, which automatically forward traffic from one interface to another one

Bation Host ——— screened host

- host exposed to internet with hardening
- Sacrificial host that will receive all inbound attacks
- Act as a proxy for all trusted systems within private network

Firewall Deployment Architecture

Single Tier
- Minimum protection

Two Tier
- Moderate level of routing & filtering complexity

Three / multi Tier
- Seperated by multiple subnets
- Eg DMZ as subnet
- More secure
- More complex

* Endpoint Security

The end device is responsible for its own security.

* Secure Operation of Hardware

↳ Repeaters, concentrators & Amplifiers
- ↳ Layer 1 of OSI
- ↳ Hubs = same collision domain + broadcast domain
  - collision domain: Seperated by Layer 2 device
  - broadcast domain: Seperated by Layer 3 device
- ↳ Modems = WAN technology | 1960 - 1990

Bridges — Layer 2 @ OSI

- Same broadcast domain, different collission domains
- Store-and-forward device

Switches

layer 2 @ OSI

- one broadcast domain
- seperate collision domain

layer 3 @ OSI

- vlan, routing
- seperate broadcast & seperate collission domain

Routers — layer 3 @ OSI

- Systems on either side of router are part of different broadcast & collision domain

Brouter — first attempt to route, if fails, it defaults to bridging

- layer 3 @ OSI

- seperate broadcast + collission domains

- layer 2 @ OSI

- one broadcast + seperate collision domain

Gateways

- connects networks that use different protocols.
- A.K.A = protocol translators
- different broadcast domains + different collision domains.

Proxies

- NAT / PAT servers
- Cache servers
- Provide Internet access to private network & hide/protect identity of clients

LAN Extenders

= creates WAN! weird.

- is remote access, multi-layer switch used to connect network over WAN links.

✡ CABLING

Transmits one signal at time → Baseband and Broadband cables

Transmits multiple signals

10 BaseT
XX YYYY ZZ

- XX = maximum speed cable type offers (10)
- YYYY = baseband or broadband
- ZZ = maximum distance the cable can be used or to present technology

Coaxial Cable

- Thinner: 10Mbps, 10Base2, 185 meter
- Thicker: 10Mbps, 10Base5, 500 meter

↳ Support high bandwidth, offers longer cable than twisted pair & fairly resistant to electromagnetic interference (EMI).

Best: lower cost + ease of installation

Conductors

- copper
- Alternate to conductor-based network cabling is fiber optic (copper alternative) → +2Gbps speed

Twisted pair

- unshielded twisted pair (without foil)
- most common: UTP: Unshielded Twisted-pair
  - 10BaseT — 100 meter
  - 100BaseT
  - 1000BaseT → 1Gbps

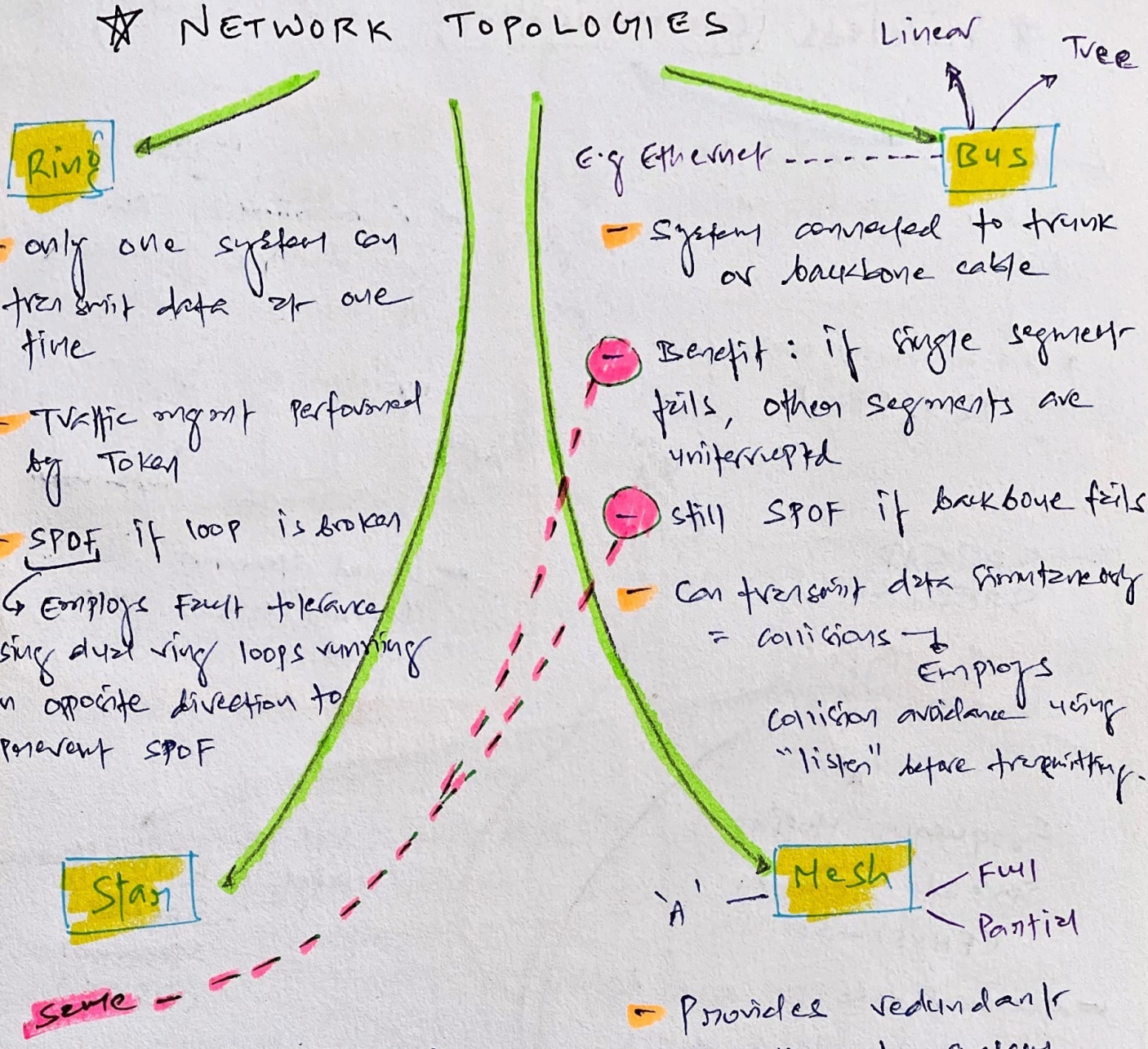
- Copper problem = Attenuation
- more speed = more Attenuation
- Solution = use shorter cable for high speed transmission.

Coaxial cable	distance	Twisted pair cable
	>	

data transmitted over one set of wire picked up by another wire due to electromagnetic field.

Tighter the twist = more resistant to internal & external interference & crosstalk, greater throughput

✡ NETWORK TOPOLOGIES



- only one system can transmit data at one time
- Traffic mgmt performed by Token
- SPOF if loop is broken
  ↳ Employs Fault tolerance using dual ring loops running in opposite direction to prevent SPOF

- System connected to trunk or backbone cable
- Benefit : if single segment fails, others segments are uninterrupted
- still SPOF if backbone fails
- Can transmit data simultaneously = collisions → Employs collision avoidance using "listen" before transmitting.

- Centralized connection device such as switch / hub
- Logical bus and logical ring can be implemented as physical star

- Provides redundant connections to system, allowing multiple segment failure without affecting connectivity.

Note — Gateway → only useful if network protocols are changing.

Cat 7 → Appropriate for 10 Gbps network at much longer distance.

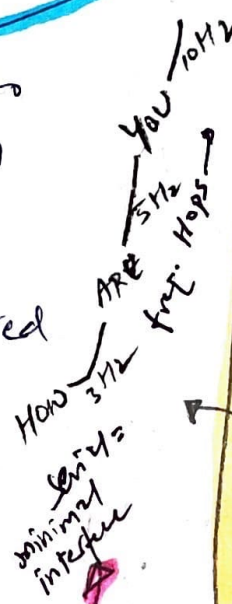
STP Cable → limited to 155 Mbps & 100 meters.

✱ Wireless Communications and Security

Employ radio waves to transmit signals over a distance

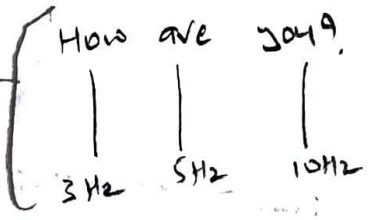
↓

Radio spectrum measured with Hertz (Hz)



Spread Spectrum

- Communication occurs over multiple frequencies at the same time



- spread spectrum is parallel comms, not serial.

SPREAD SPECTRUM'S

3 Types

Frequency Hoping Spread spectrum (FHSS) – Serial

- transmit data in serial fashion (not parallel) while constantly changing frequencies in use

Also helped to minimize interference

- Entire range available but only use one frequency at a time

Direct Sequence Spread Spectrum (DSSS)

Parallel

Employs Available Frequency

- transmit data using parallel
- Occurs same way as parity of RAID-5 allows data on missing drive to reserved

Orthogonal Frequency-Division Multiplexing (OFDM)

- Employs digital multicarrier modulation scheme that allows tightly compacted transmission.
- Perpendicular modular signal = No interference with each other.

Cell phones

- Provider's tower can be simulated to conduct MITM attacks

Bluetooth

- IEEE 802.15 / Personal Area N/w (PAN)

* Attacks → Bluejacking
  - Bluesnarfing
  - Bluebugging

RFID

- Radio frequency identification
- tracking technology
- RFID Reader can collect information transmitted by activated chips in the area

NFC

- Near field comms.
- Smartphones: device to device data exchange
- Radio based tech.

* Attacks → MITM
  - Eavesdropping
  - Data Manipulation
  - Replay

Cordless phones

- Designed to use unlicensed frequencies (900 MHz, 2.4/5 GHz)
- Eavesdropping

✱ LAN Technologies

Ethernet

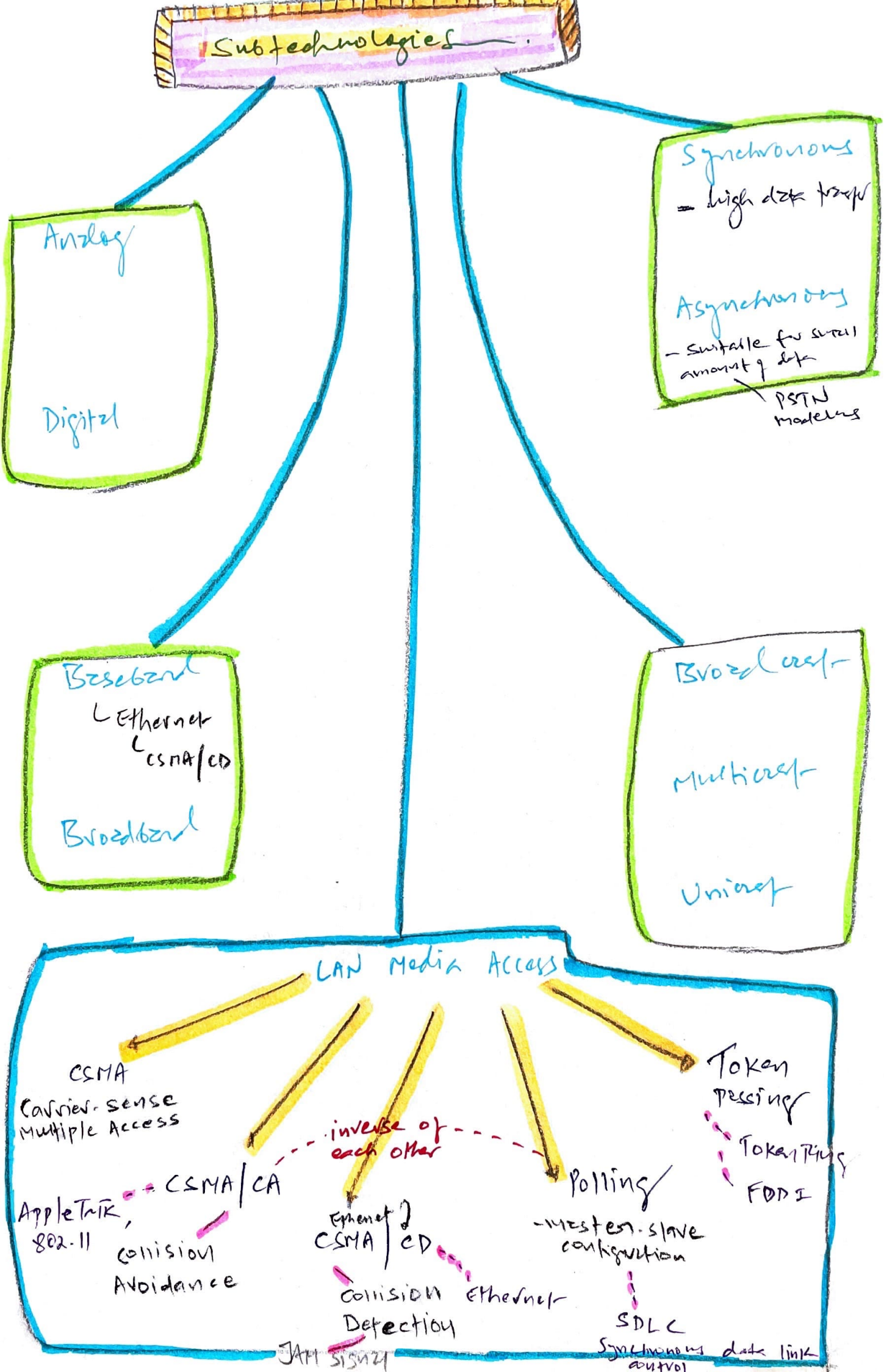
- Full-duplex, twisted-pair cabling
- Employs broadcast and collision domain
- IEEE 802.3 standard
- A.k.a: Shared-media LAN technology / broadcast technology

Token Ring

- token travels in a logical loop in LAN
- Employed in ring or star topologies.
- Deployed as physical star using Multistation Access unit (MAU)

FDDI (Fibre Distributed Data Interface)

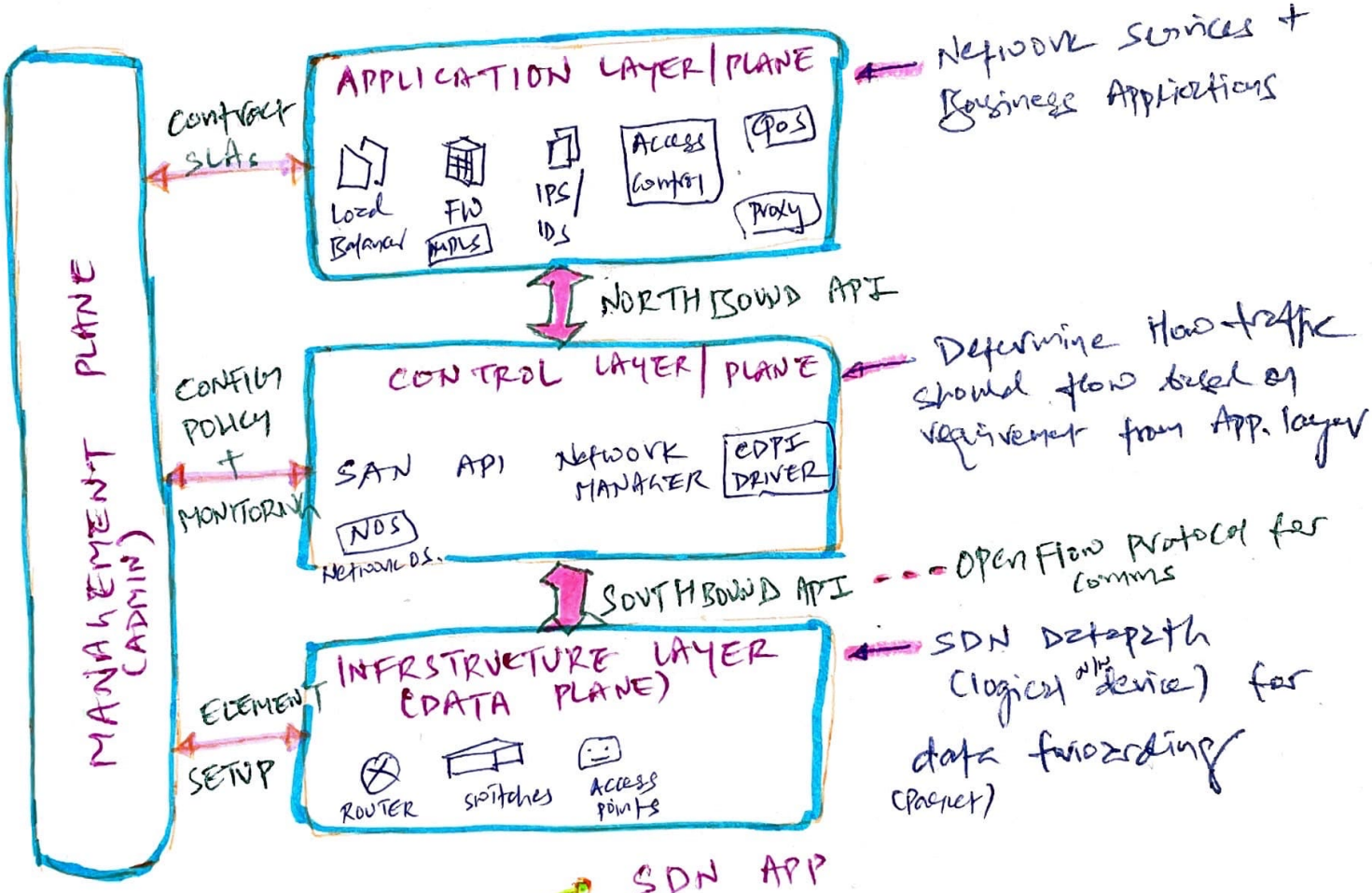
- high speed token passing technology
- $ $ $ $ $ $
- Used as backbone for large enterprises
- Dual ring design = self healing by removing failed segment
- Two rings: traffic flowing in opposite direction


Subtechnologies
Analog
Digital
Synchronous
- high data transfer
Asynchronous
- suitable for small amount of data
PSTN modems
Baseband
Ethernet
CSMA/CD
Broadband
Broadcast
Multicast
Unicast
LAN Media Access
CSMA
Carrier-sense Multiple Access
CSMA/CA
inverse of each other
AppleTalk, 802.11
collision Avoidance
Ethernet
CSMA/CD
Collision Detection
Ethernet
Jam signal
Polling
-master-slave configuration
SDLC
Synchronous data link control
Token passing
Token Ring
FDDI

SDN - SOFTWARE DEFINED NETWORK

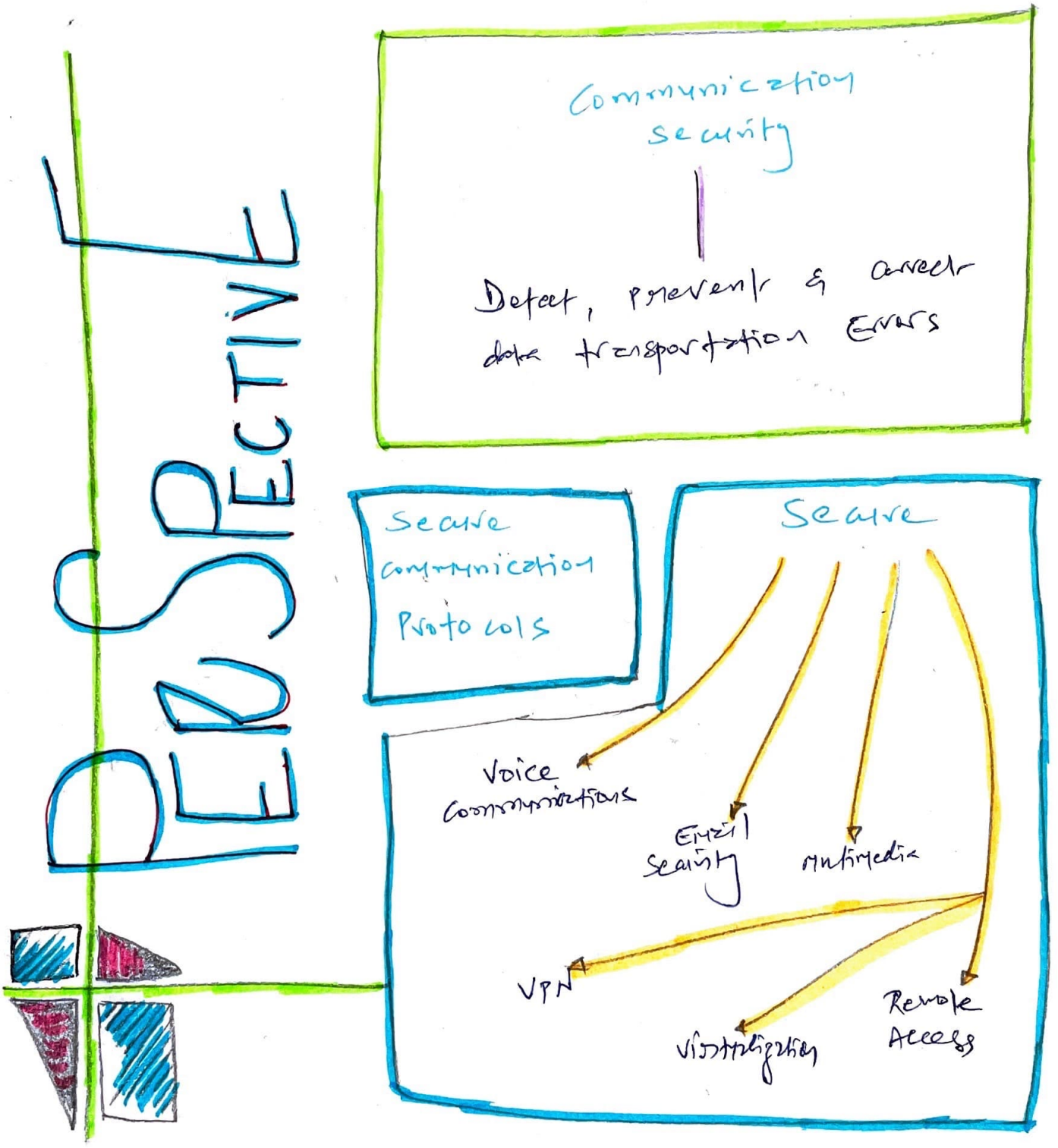
- SDN seperates routing & forwarding decisions of networking elements from Data plane

SDN Architecture
- APPLICATION PLANE
- CONTROL PLANE
- DATA PLANE



SDN CORE COMPONENTS
- SDN APP
- SDN CONTROLLER
- SDN DATAPATH
- SDN control to Data-Plane Interface (CDPI)
- NBI - NORTH BOUND INTERFACE
- SBI - SOUTHBOUND INTERFACE
- Mgmt + Admin

12. SECURE COMMUNICATIONS AND NETWORK ATTACKS



✱ Secure Communication Protocols

IPSec

- Uses PKI to provide Encryption, Non-repu. + msg auth.
- IP based protocol

Kerberos

- SSO
- Hybrid ~~authentication~~ Encyption + authentication protocol

SSH

- End to end Encryption

(S-RPC)

Secure Remote Procedure call

- Authentication service
- Prevents unauthorised execution of code on remote system

Signal Protocol

- End-to-end encyption for voice / video / messaging Apps

SSL

TLS

Secure Socket layer

- 40-bit | 128-bit key

Transport layer security

both

Prevents spoofing, tampering + eavesdropping

- Both can be implemented to lower lyr (layer 3) to operate as VPN, called Open VPN

* Authentication Protocols

~~(MORE)~~ Move on
~~BOSON~~ BOSON coffee
~~NOTES~~

(CHAP) Challenge Handshake Auth. Pro.

- Used over point-to-point (PPP) links
- Authentication using challenge-response dialog that cannot replayed
- Periodic reauthentication of established session

Protection against Replay attacks

(PAP) Password Auth. Pro.

- Transmits username & password in clear text
- No Encryption

(EAP) Extensible Authentication Protocol

- This is framework of authentication instead of actual protocol

Allows customized authentication Security solutions

- EAP-TLS
- PEAP
- LEAP

* Secure Voice Communications

Important to implement
- Authentication
- Integrity
- Confidentiality

PBX / POTS Vunerable to + PSTN
- Eavesdropping
- Tapping
- interception

VoIP
Encapsulates Audio into ip packets to support telephone calls over TCP/IP network.

VoIP problems
- MITM
- DS + DOS Attacks
- Vishing (VoIP phishing)
  - Caller ID can be falsified
  - A.K.A = SPIT Attack (Spam over Internet Telephony)
- 802.1x Authentication falsification (vlan Hopping)
  - Risk where VoIP phone & servers are on the same switches
- VoIP traffic Unencrypted = risk

Social Engineering

Exploits human characteristics

Attackers bypass physical and logical (technical) security controls punching holes in security perimeter.

Tools p.t.o

Phreakers — They gain unauthorised access to personal mailboxes, redirect messages, block access, redirect inbound/outbound calls.

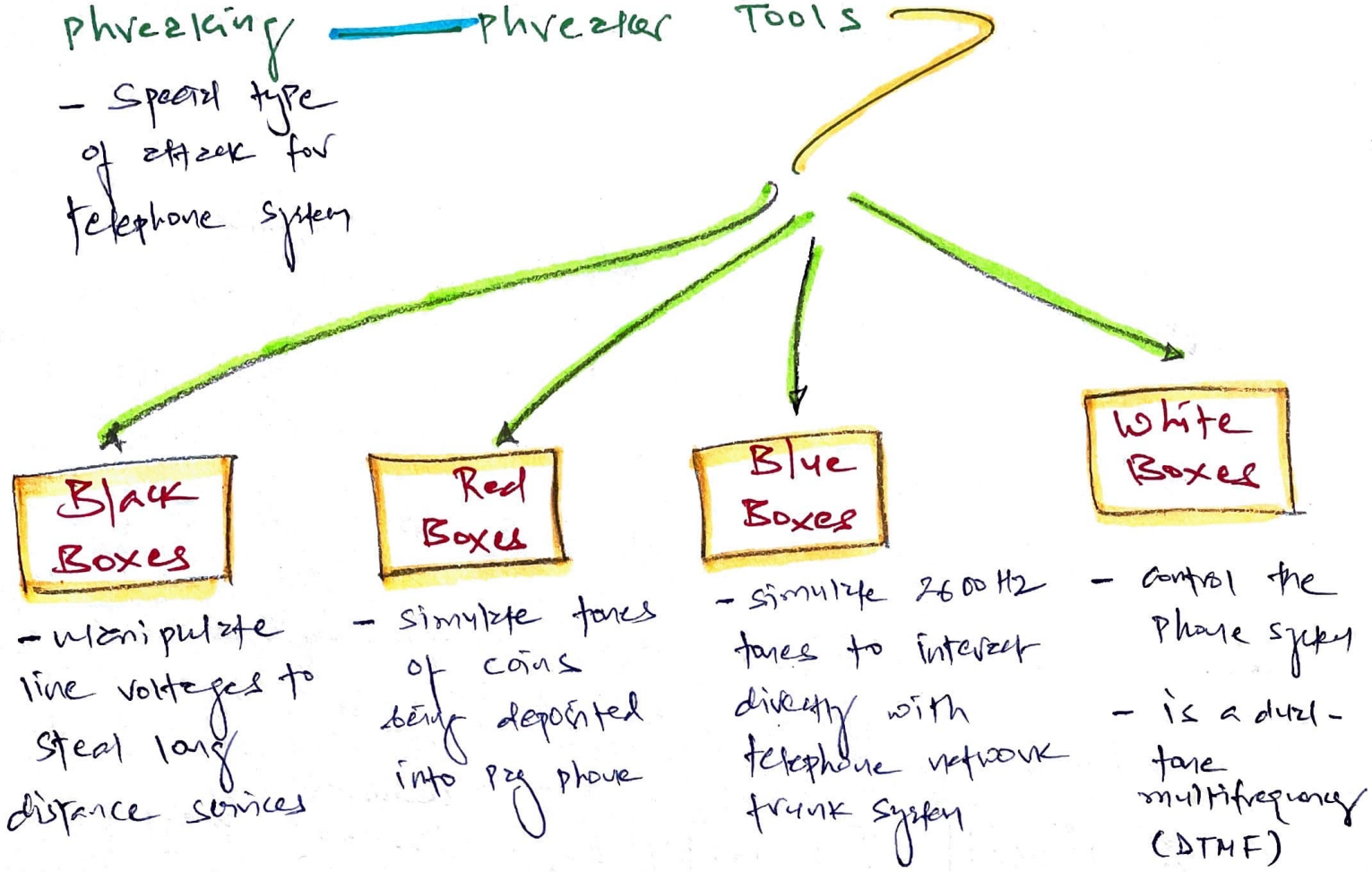
They are threat to PBX (private branch exchange)

Reduce PBX fraud with DISA (Direct Inward System access)

- DISA is designed to help manage external access and external control of PBX by assigning access codes to users.

Phreaking — Phreaker Tools

- Special type of attack for telephone system



☆ Multimedia Collaboration

- Remote Meeting
- Instant Messaging (IM)
  - susceptible to packet sniffing
  - No protection for Policy

☆ Email Security ---- security issues (P.T.O)

- Email server – SMTP
- Email clients – POP3, IMAP

Careful! SMTP server should not turn into Open Relay
- means SMTP server doesn't authenticate senders before accepting and relaying mail

Note - Many internet-compatible Email system rely on X.400 standard for addressing and message handling.

Note - Email security begins in a security Policy approved by upper mgmt.

protocols: IMAP, POP & SMTP do not employ encryption natively.

Email Security Issues

- POP3, IMAP, SMTP = don't employ encryption natively + modify email in transit (integrity issue)
- Delivery of trojan, virus, worms
- Spoof source email = spamming
- Mail Bombing (DDoS Attacks)

Email security solutions — PGP

PGP: download common

PGP: 2 type of messages

S/MIME — Security Multipurpose Internet Mail Extensions

- Auth & C to email via public key encryption and digital signatures
- Uses X.509 → PKI for clients

MIME object Security Service (MOSS)

- Uses MD2, MD5, RSA, DES for Encryption & Authentication
- provides C, I, Auth, NP of email messages

Privacy Enhanced Mail (PEM)

- Use of RSA, X.509, DES
- Provides C, I, Auth & NP

DomainKeys Identified Mail (DKIM)

- Ensure valid email is sent through verification of domain identity.

SPF — Sender Policy Framework

- Protection against spam & email spoofing
- check inbound msg originate from authorised SMTP server.

opportunistic TLS for SMTP Gateways

- Encrypted connection with every other email server
- protects from sniffing of email

Pretty Good Privacy (PGP)

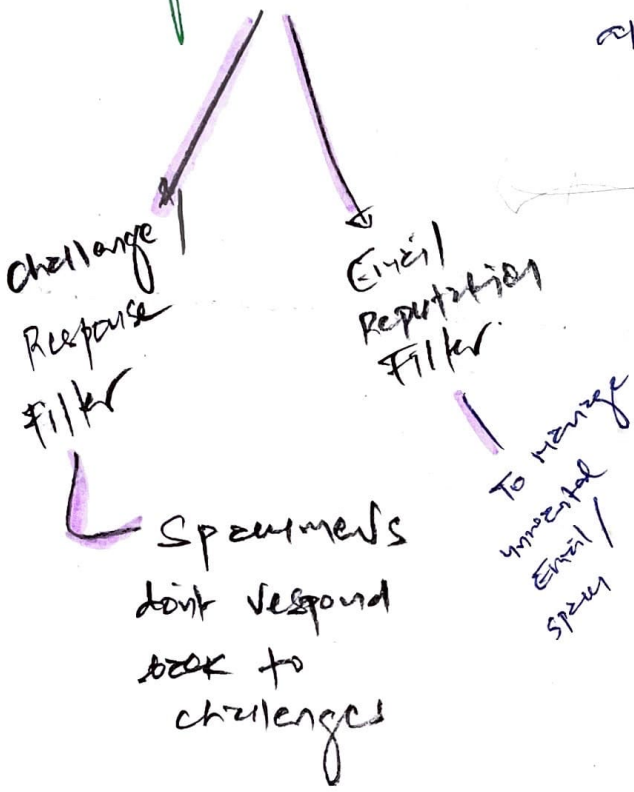
- Public private key system used in IDEA

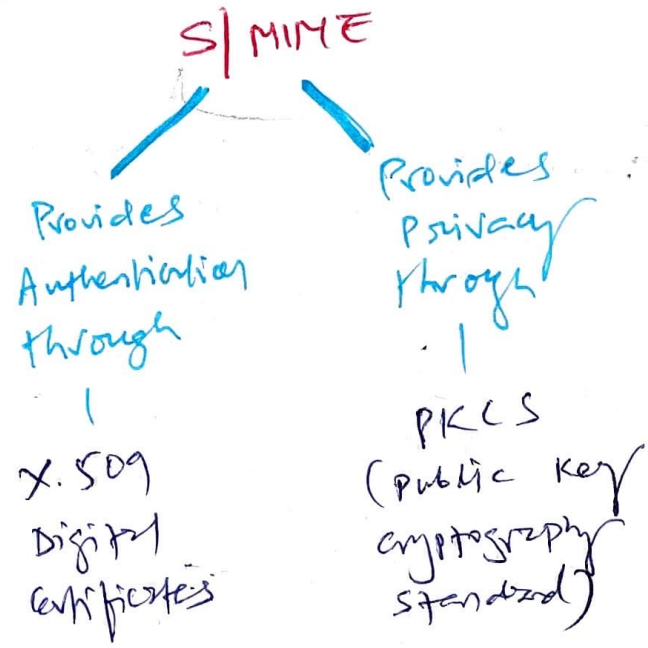
Email security at Glance

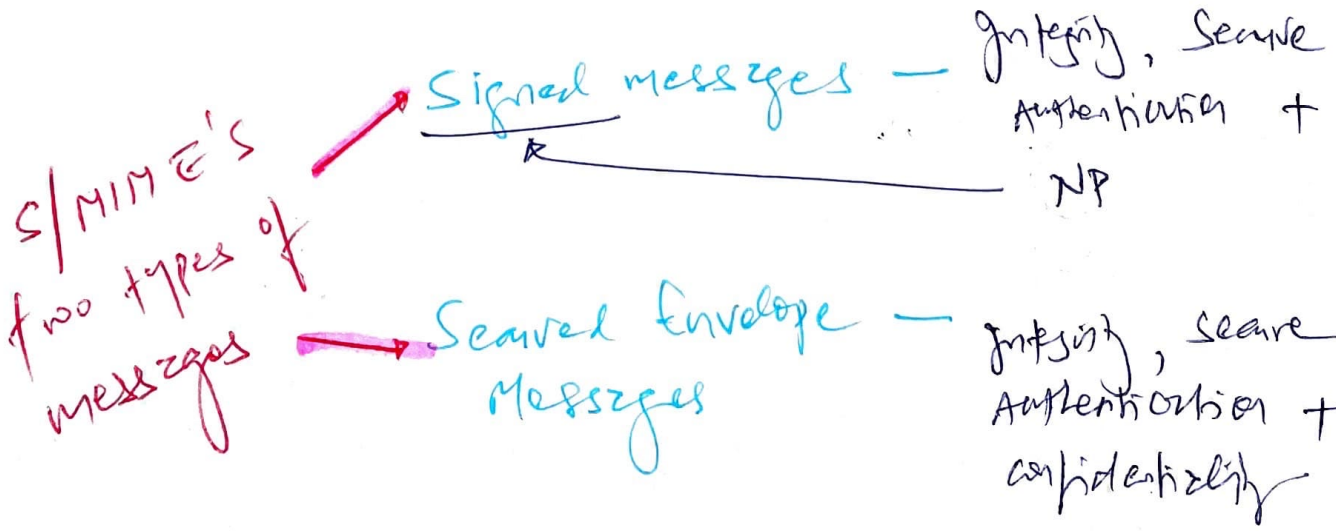
Digital Signatures → Eliminate impersonation

Encryption of messages → Reduces Eavesdropping.

Use of Email Filters → Keeps spamming & mail-bombing at minimum.







Telephony then →

- Plain Old Telephone Service (POTS)
  or
- Public Switched Telephone Network (PSTN)

Combined with modems

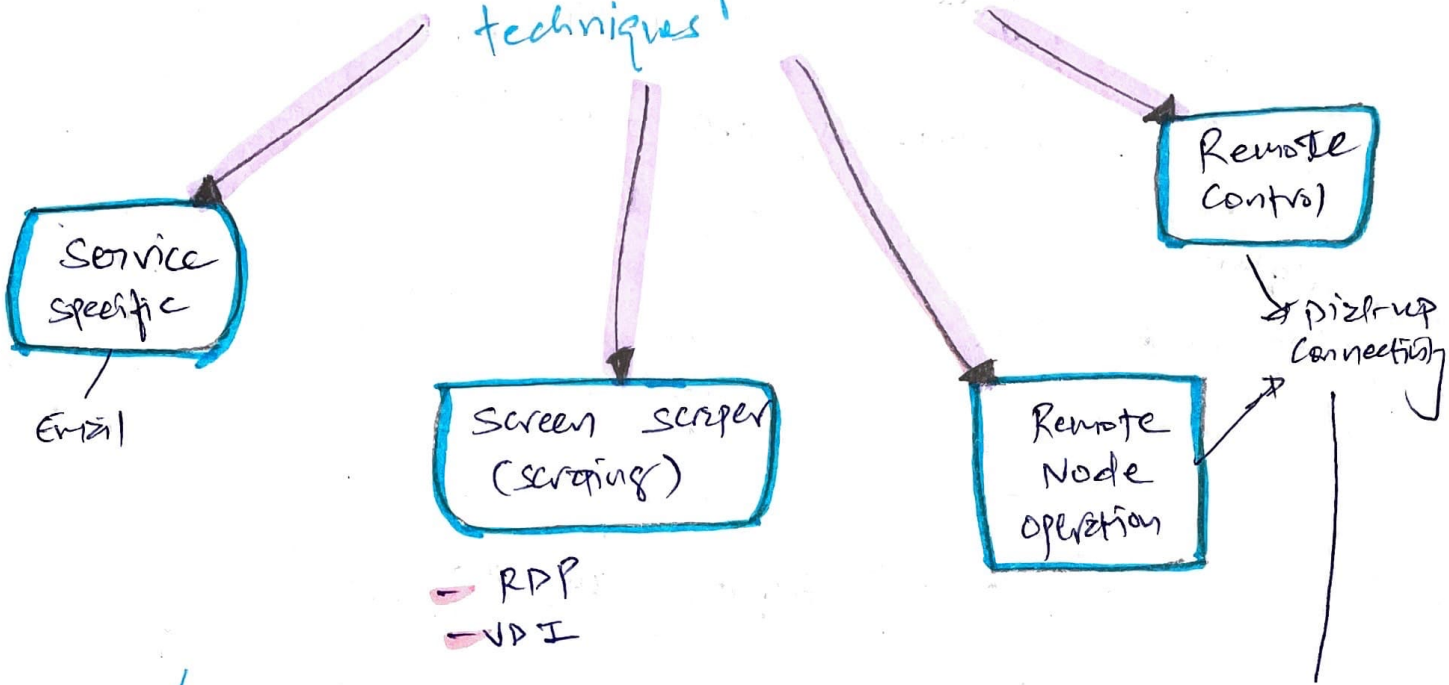
Telephony Now →

- Private Branch Exchange (PBX)
  VoIP
  VPN

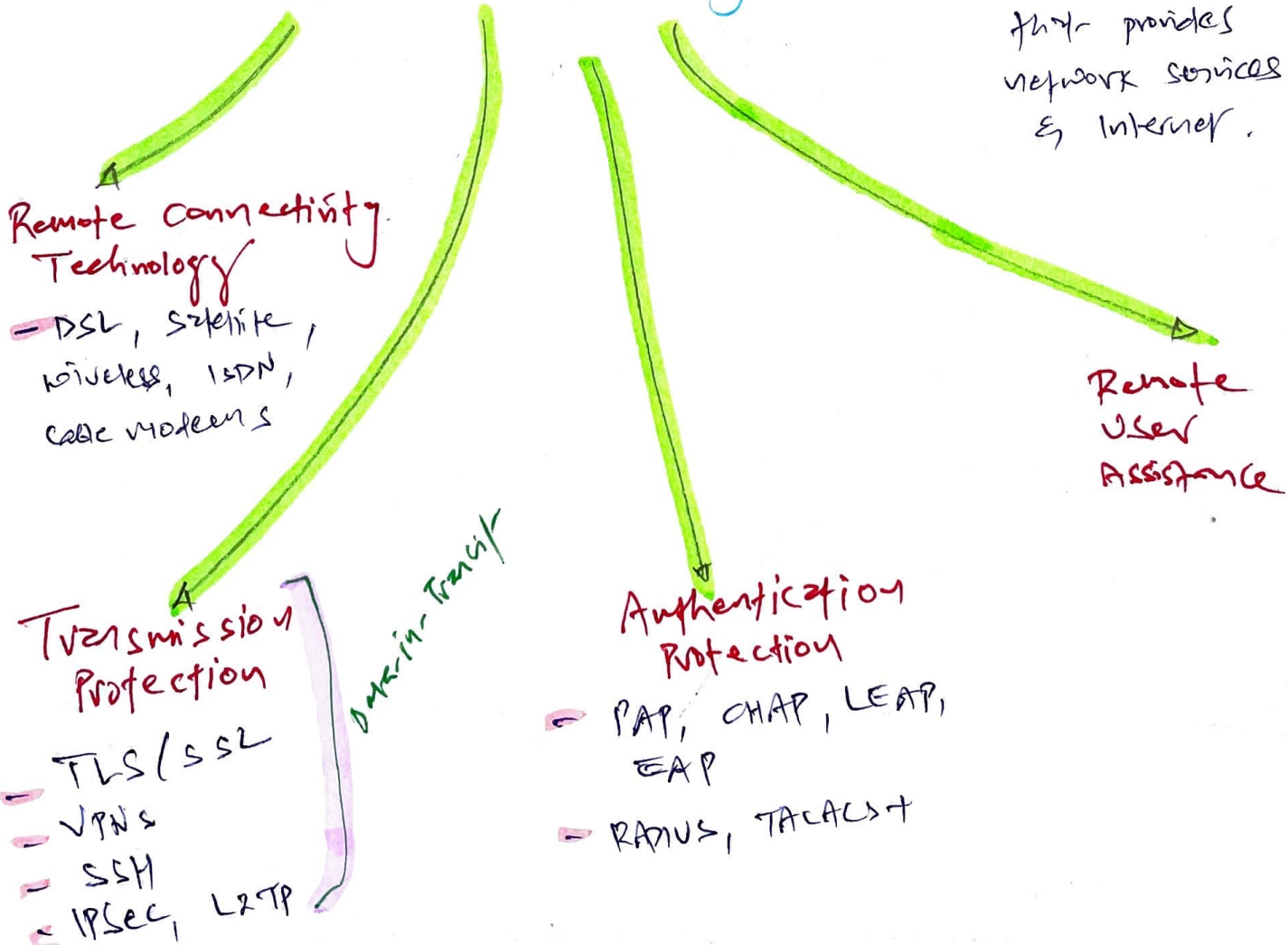
For telephone comms

✱ Remote Access Security Management

Four types of remote access techniques



Plan / Address Remote Access Security Issues



Dial-up Protocols

Provides link governance for dial-up & VPN links

LCP uses encapsulation when two devices wants to connect

LCP

NCP make sure PPP can integrate with other protocol

NCP

PPP

Not an authentication protocol. It's dial-up

older technology

SLIP

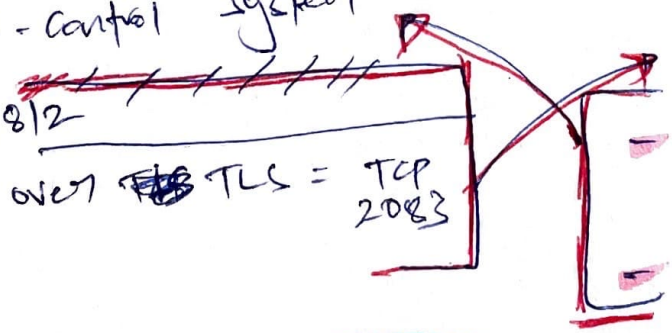
- Point-to-Point protocol
- Transmits TCP/IP packets over non-LAN connections such as: ISDN, VPN, Frame Relay
- choice for dial-up Internet connections
- Protected with CHAP & PAP
- PPP works on layer 2

- Serial line Interface protocol
- Support TCP/IP comms over asynchronous serial connections such as Serial cables, modem dial-up.
- Support only IP, require static IP, offers no error detection/correction, does not support compression.

Centralized Remote Authentication Service

TACACS+

- Terminal Access-controller Access-control System
- UDP 1812
- RADIUS over ~~TLS~~ TLS = TCP 2083



RADIUS

- Remote Authentication Dial-in User Service
- TACACS, XTACACS & TACACS+
- TACACS+ port TCP 49

2FA

RADIUS & TACACS provides seperation of authentication & authorization for remote clients, so if it's compromised, only remote connectivity is affected.

☆ Multi-homed Firewalls ☆

(Dual-homed)

has at least two interfaces to filter traffic

Note — All multi-homed firewalls has IP forwarding which automatically send traffic to another interface should be disabled

Bastion Host / sacrificing host

- Exposed to internet that has been hardened by removing unnecessary services/ programs/ protocols & ports

Screened Host / proxy host

- firewall protected system typically positioned just inside private network.
- All inbound traffic routed to screened host, it act as a proxy for all trusted system, responsible for filtering traffic + protect the identity & internal client.

Note — All inbound traffic is directed to bastion host, and only authorised traffic can pass through router/ firewall to private n/w.