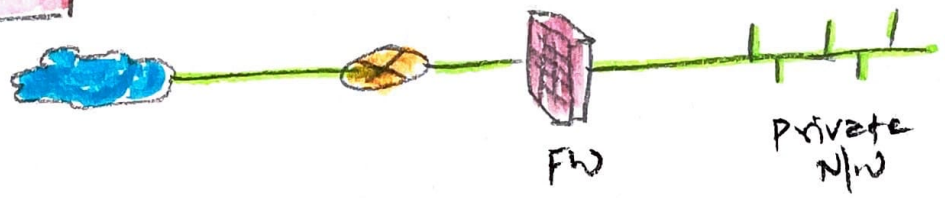
☆ Firewall Deployment Architectures ☆

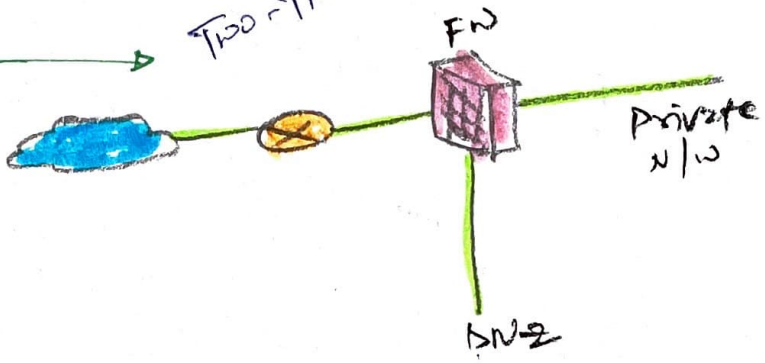
Single Tier



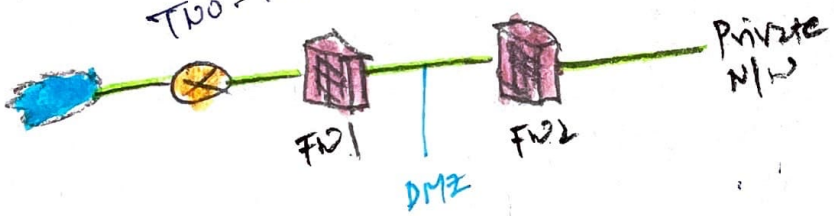
- minimal protection
- Useful against several Attacks

Two-Tier

Design 1 → Two-Tier I



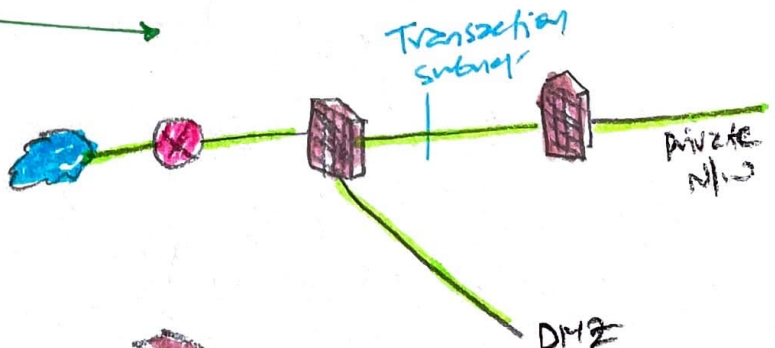
Design 2 → Two-Tier II



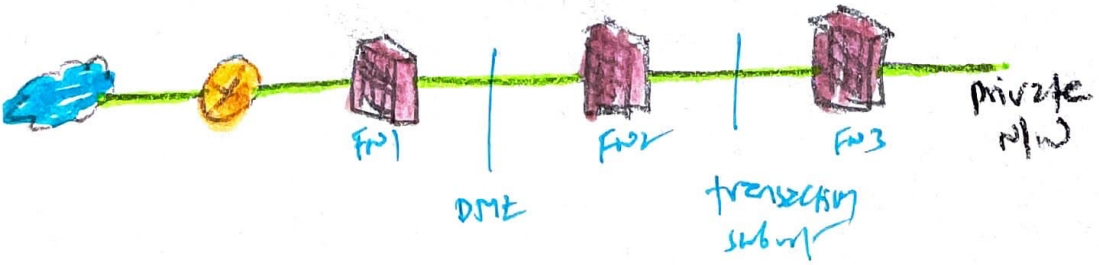
- moderate level of routing & filtering complexity.
- DMZ is used to host information for external users such as web/file servers

Three-Tier

Design 1 (Tier II)



Design 2 (Tier I)



- Most Secure

याद रखो

Cabling Types

- 10 Base 2 — Distance 185 meter
  - Speed → 10 mbps
- 10 Base 5 — 500 meter
  - Speed → 10
- 10 Base T (UTP) — 100
  - Speed → 10 — 100
- STP — 155
- 100 Base T / 100 Base Tx — 100
  - → 100
- 1000 Base T — 100
  - → 1 Gbps
- Fiber Optic — 2+ km
  - → 2+ Gbps

UTP Categories

	Throughput
Cat 1	voice only
Cat 2	4 mbps
Cat 3	10 mbps
Cat 4	16 mbps
Cat 5	100 mbps
Cat 6	1000 mbps
Cat 7	10 Gbps

Teardrop — Use of fragmented TCP packets to target flaw in TCP / tcp stack fails resulting DoS.

Attacks

Christmas — Set all possible TCP flags on packet

↳ Challenge for Endpoint security = sheer volume of data

↳ Data leakage or anything that bypasses security like data loss prevention = covert channel

↳ PPP has replaced SLIP. PPP is the answer for legacy service.

↳ Firewalls can filter Non-IP protocols (IPX / SPX, NetBEUI, AppleTalk)

12. SECURE COMMUNICATIONS AND NETWORK ACCESS CONTD.

✡ VPN

Tunneling problems

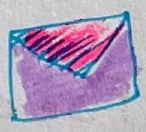
DAMN GOOD INTERVIEW QUESTION - What is tunnel in Internet?

Encapsulation = creates logical illusion of communication tunnel

- Use larger packets = bandwidth saturation
- Not designed for broadcast as tunneling use point-to-point comms

SNAIL MAIL

letter = primary content protocol packet

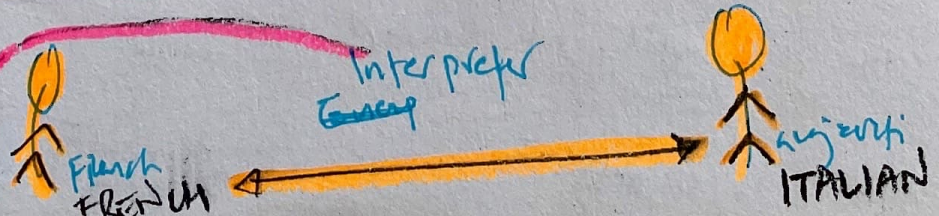


Envelope = tunneling protocol

- Hard to monitor content of the traffic

this creates security issue

VPN TRIVIA — Most VPN use encryption to protect encapsulated traffic, but encryption is not necessary for connection to considered a VPN.



* Common VPN Protocols

PPTP → Encapsulation protocol

- Operates @ Data link layer 2 @ OSI
- Doesn't support RADIUS & TACACS+
- Supported protocols: CHAP, PAP, EAP, SPAP, MS-CHAP
- Initial PPTP session = Not Encrypted
- PPTP used on VPN, replaced by L2TP that uses IPSec for Encryption
- Most modern PPTP adopt Microsoft P2P Encryption that supports data Encryption.

offers Authentication

L2TP

- Provides point-to-point tunneling
- No in-built encryption, relies on IPSec for Encryption
- Supports RADIUS & TACACS+

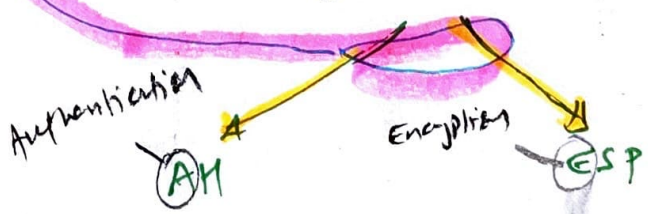
L2F

- Mutual authentication tunneling mechanism
- No Encryption
- Replaced by L2TP
- layer 2 @ OSI

AH & ESP requires 2 security Associations each = total 4 SA

IPSec

- layer 3 @ OSI
- only for IP networks
- Provides secure authentication + encrypted data transmission



- Auth, NP, I
- Encryption + limited Auth

Transport mode

Tunnel mode

ESP provides Encryption & limited authentication

only IP packet data is encrypted, not header

Entire IP packet is encrypted

VPN characteristic Table P544

VPN PROTOCOL	Native Authentication Protection	Native Data Encryption	Protocols Supported	Dial-up Links Supported	Number of Simultaneous Connections
PPTP	yes	No	PPP	yes	Single Point-to-point
L2F	yes	NO	PPP/SLIP	yes	"
L2TP	yes	No (can use IPsec)	PPP	yes	"
IPSec	yes	yes	IP only	No	Multiple

Vlan Notes

Vlan works like subnets. But, they are not actual subnets.

Vlan used for → Traffic mgmt

Vlan Mgmt → Control Vlan traffic for Security or performance

- Vlan restricts broadcast traffic
- Reduce network's vulnerability to sniffers with isolation / segmentation
  - Isolated private vlan
- Layer 3 switch prevents broadcast storms
  - Flood of unwanted Ethernet broadcast network traffic.
- Define no routing b/w vlan or deny filter b/w certain vlans.

✱ Virtualization

Security

- Easy Backup (A)
- Safer testing

VM Escaping

- when software within guest OS is breached

To minimize Risk

1. Have physical isolation (servers) for sensitive Data
2. Monitor
3. Patch hypervisor software up to date

✱ Virtual Software

running windows Application on Linux host or USB

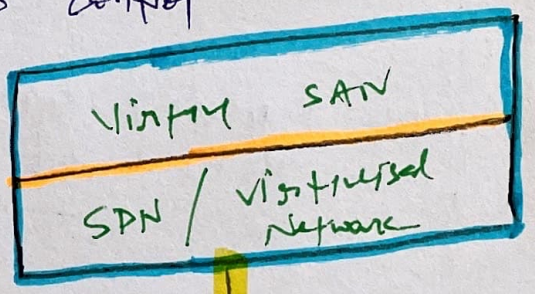
Virtual Desktop refers to

- Remote Access Tool
- Extension to virtual App
- Expanded Desktop

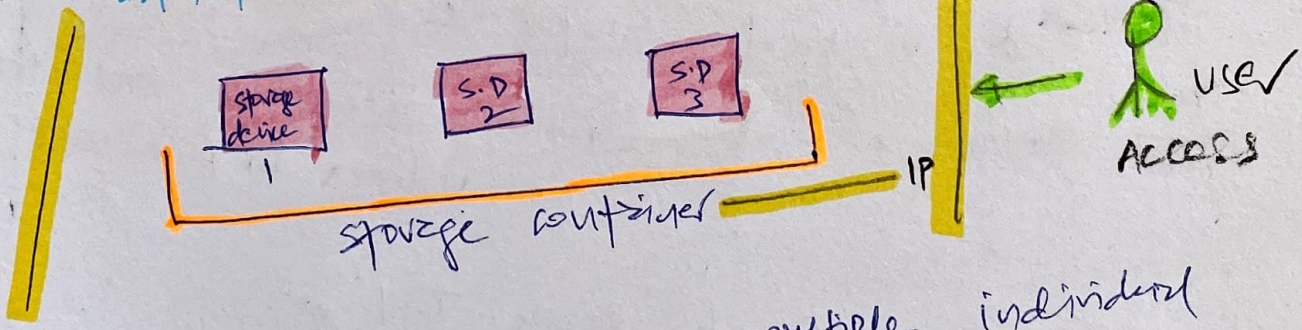
* Virtual Networking

Software Defined Networking (SDN)

- Vendor neutral + independence
- From IP to programming + routing
- SDN seperates infrastructure / hardware layer from control layer
- Allows data transmission paths, communication decision trees & flow control



* Virtual SAN



A technology that combines multiple individual storage devices into single consolidated network accessible storage container.

→ Virtual SAN is software-defined shared storage system, is a virtual overlay of SAN, on top of virtualized network or SDN.

✱ Network Address Translation (NAT) --- layer 3 @ OSI

NAT : Internal IP → External IP

PAT : Internal IP → External IP + port number

Multiplexing of or NAT overloading

NAT

Private IP Range

10.0.0.0 – 10.255.255.255 — A

172.16.0.0 – 172.31.255.255 — B

192.168.0.0 – 192.168.255.255 — C

You can never route a traffic on private IP Address (RFC 1918). Routers in Internet will drop data packets containing source or destination for RFC 1918 ranges.

NAT → Static

NAT → Dynamic

→ P.t.o (more detail)

NAT-Traversal (RFC 3947) - designed to support IPsec VPN through UDP encapsulation of IKE.

Automatic Private IP Addressing (APIPA)

169.254.0.1
to 169.254.255.255

Assign IP if DHCP fails

APIPA = problem

- Power failure on DHCP
- Bad cable
- Malicious attack on DHCP server

Note – APIPA & loopback (127.x.x.x) are not private IPs.

Stateful NAT → Maintains information about the communication sessions b/w internal clients & external systems.

NAT & IPSec – NAT is not directly compatible with IPSec as NAT modifies packet header, And IPSec too rely on encrypting packet header for security. Thus, we have to use NAT-Traversal.

Read Table 12.2 (p555)

✡ Switching Technologies.

p.t.o End for list

Circuit switching

- Telephone network
- Permanent physical connections
- Fixed transmission times, uniform level of quality, little to no loss of comm interruptions.
- once path is disconnected, diffrent path may assemble after reconnection.
- offers Exclusive use of communication path → Nope.

Packet Switching

- Connectionless
- sensitive to data loss
- Message broken into smaller segments.
  - Each segment has its own header, src, dst IP that routes from hop to hop.
- Unlike circuit s/w, if path is broken, it's easy to find alternate path but have to encrypt packet to prevent from data disclosure.

Virtual Circuits

← multiple path exists b/w point A & B

- logical pathway or circuit created over packet-switch network b/w two endpoints.

2 types

Have to create

predefined

PVC = Walkie Talkie

Permanent VC (PVC)

- Two-way radio or walkie-Talkie
- Predefined VC, always avilable, Press button & start talking.

SVC = DIAL-UP

Switched VC (SVC)

- Shortwave radio = requires tuning
- Like dial-up connection, VC to be created, best path chose from multiple routes, disassembled after use

* WAN Technologies

2 types of WAN links:

Dedicated line (leased line / point-to-point link)

- Dedicated line is always open & waiting for traffic to be transmitted over it. (Eg. customer LAN to WAN)
- T_1
- T_3
- E_1
- E_3

Nondedicated line

- Requires connections to be established before transmission can occur.
- DSL, ISDN & standard modems

For Exam

DSL - digital subscriber line

- A technology that exploits the upgraded telephone network to grant customer speeds from 144 Kbps to 20Mbps & more

DSL formats:

- ADSL
- xDSL
- CDSL
- HDSL
- SDSL
- VDSL
- IDSL
- RADSL

- Max. DSL line distance = 5000 meters

* ISDN
(Integrated Services Digital Network)

- ISDN is fully digital telephone network that supports both voice and high-speed data communications.

ISDN Formats

(BRI)
Basic Rate Interface

- 144 Kbps as total throughput
- offers customer connection with
  - two B channel & one D channel
    - 64 Kbps throughput
    - used for Data trans.
  - one D channel
    - used for call establishment, mgmt & tear down
    - bandwidth 16 Kbps

(PRI)
Primary Rate Interface

- 192 Kbps to 1.54 Mbps as bandwidth, not throughput
- multiple 64-Kbps B channels (2 to 23)
- single D chan 64 Kbps

WAN Notes

↳ CSU/DSU (channel service unit / Data service unit) device converts LAN signals to WAN carrier info & v.v

↳ CSU/DSU contains DTE/DCE (Data terminal equipment/ Data circuit-terminating Equipment), that provide actual connection point for LAN router (DTE), WAN carrier info switch (DCE)

* WAN Technologies for connection

X.25
- older packet-switching technology
- Uses PVC for P-2-P connection
- lower throughput + performance

SMDS
- Switched multimegabit Data Service
- Connectionless packet-switching
- Connect MAN, remote LAN
- Fragment data into small fragmentation cells

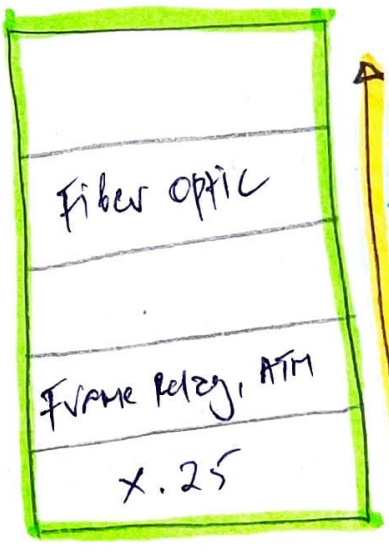
FRAME RELAY
- layer 2 @ OSI, Packet-switching
- Use of multiple PVCs, Connection-oriented
- CIR (committed Info. Rate)
- Requires use of DTE / DCE
  - DTE : LAN
  - DCE : WAN

ATM
- Asynchronous Transfer mode
- Connection-oriented
- Cell-switching WAN Technology
- Fragments comms into fixed-length 53-byte cells
- Use PVC &/or SVC
- offers high throughput

SDH
- Fibre
- ITU
- Synchronous Digital Hierarchy

Both use time-division multiplexing (TDM) with minimum control & mgmt overhead.

SONET
- Fibre
- American — (ANSI)
- Synchronous optical Network
- * SONET + SDH use time division multi. (TDM) to high-speed duplex communications.
- SDH+SONET support mesh & ring topologies. often implemented as Backbone for Telcos
- SDH+SONET interception point is ADM (Add-Drop multiplexers) - allows addition and removal of low rate bit stream connections.



* Specialized Protocols

Synchronous Data Link control

SDLC

upgraded version

High-Level LC

HDLC

- Use of permanent physical connection of dedicated leased lines to provide connection to mainframe such as IBM system

- Refined version of SDLC for serial synchronous connections

- supports full duplex, P-2-P, P-2-M

- SDLC uses polling @ layer 2 OSI, and is bit-oriented synchronous protocol

+ Flow control, Error correction & detection

HSSI

High-speed LC

- layer 1 @ OSI

- HSSI is DTE/DCE interface standard that defines how multiplexers and routers connect to high-speed network such as ATM/ Frame Relay.

* Dial-Up Encapsulation Protocols

PPP

- Encapsulation protocol designed to support transmission of IP traffic over → dial-up
→ point-to-point links

Replaced SLIP

- All dial-up & P-2-P connections are Serial in nature.

✡ PREVENT OR MITIGATE NETWORK ATTACKS

p.t.o

p.t.o for prevention

DoS

- resource consumption attack

2 forms

- Attack exploiting vuls. in H/w & S/w
- Flood victim's pipeline with garbage

Result: computer unable to process legitimate requests.

DDoS

- DDoS Attack that use intermediary system as secondary victims using Zombie, bots, agents = DDoS

→ this entire thing/ deployment is called BOTNET

Replay

- Attack using captured traffic via eavesdropping
- Reestablish comm session against the system
- Prevent using onetime Auth. mechanism and sequence session identification

Eavesdropping

- Dangerous for data in transit than data at rest
- Passive attack that requires physical access to IT infra
- wireshark, sniffer, ZAP (zed Attack proxy)

Impersonation / Masquerading

when username & password is captured

- Pretending to be someone (@hacktivist) ← :(
- Different from Spoofing: false identity without proof
- Use onetime pad / token Auth. using kerberos

Modification Attacks

- this attack bypass this
- Captured packets are altered and then played against the system
- Prevention: Digital signature verification & packet checksum verification

DNS poisioning & DNS spoofing are called RESOLUTION ATTACKS.

ARP Spoofing

- Provides false MAC address for requested IP Address, then system redirect traffic to alternate destinations.
- ARP Attacks are often elements in MITM Attacks.
- Prevention:
  - Use static ARP mapping for critical systems
  - Monitor ARP caches for MAC-to-IP Address mapping
  - Use IDS to detect anomalies in traffic and change in ARP traffic.

DNS poisioning

- When Attacker alters domain name to IP Address mapping to redirect traffic to rogue system

DNS Spoofing

- Exploitation of Race conditions
- When Attacker sends false replies to requesting system, beating the real reply from valid DNS server

DNS Hijacking

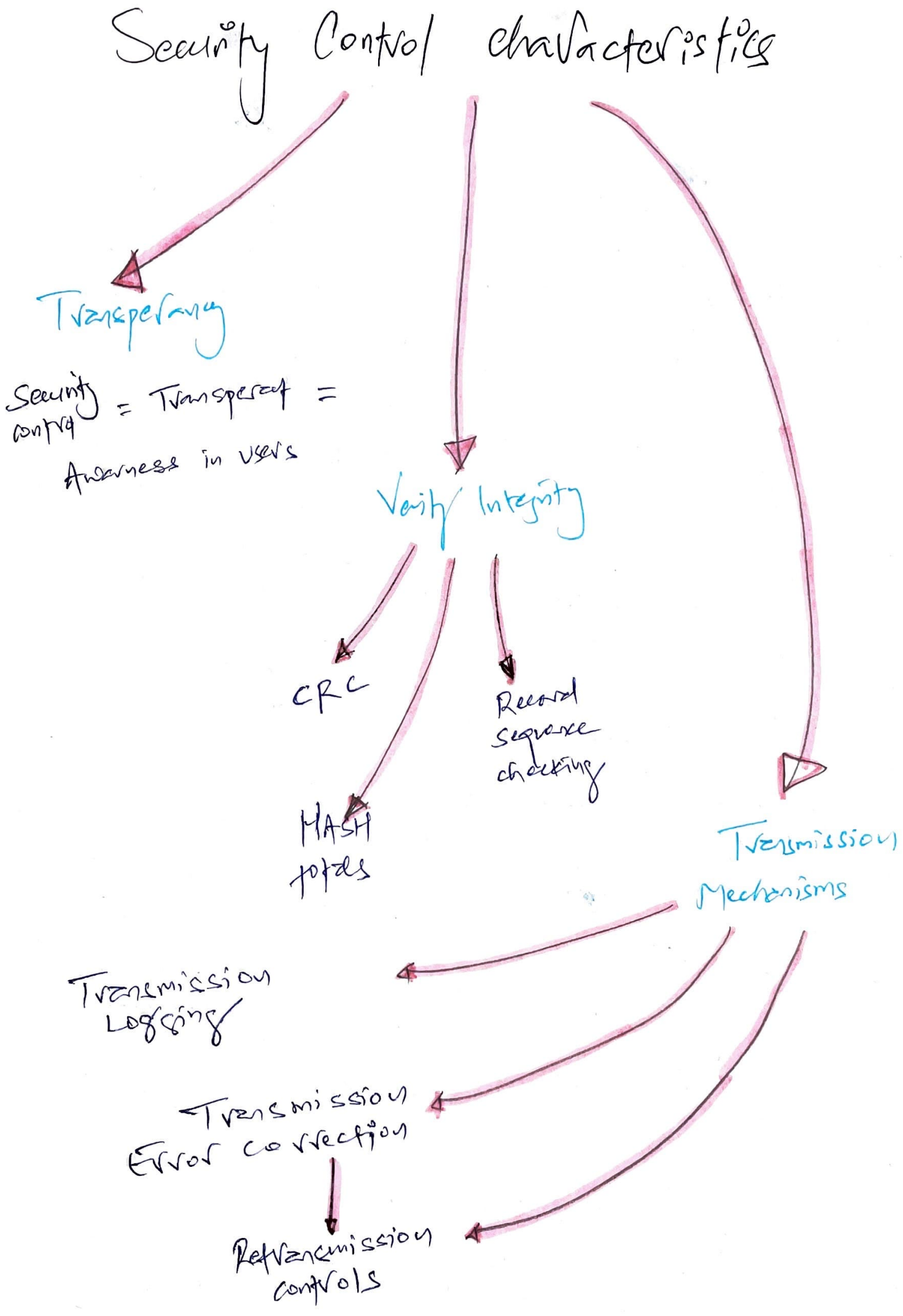
- Sending false reply to caching DNS server for nonexistent subdomains, attacker can hijack entire domain resolutions details.

Note - only solution for DNS hijacking is to upgrade DNS to DNSSEC

Hyperlink spoofing

This attack

- Can take the form of DNS Spoofing or simply an alternation of hyperlink URL in HTML code of domain Send to client
- Who see the URL anyway - this attack is usually successful ~~successful~~ — click, click, click


Security Control characteristics
Transparency
Security control = Transparent =
Awareness in users
Verify Integrity
CRC
Record sequence checking
HASH totals
Transmission Mechanisms
Transmission Logging
Transmission Error correction
Retransmission controls

Network Attack Preventions

DoS / DDoS

- Add FW / Router / IDS that detect DOS Traffic
- Disable & block broadcast features, ICMP / Echo reply & spoofed packets
- Upto date system patch
- Consider commercial DOS protection or Response like Cloudfare / Prolexic

Eavesdropping

- Onetime Authentication methods (token devices)
- Use of Encryption (SSH, IPsec)
- Physical control to prevent access from unauthorised personals
- Software installation policy (not everyone should be able to install Wireshark)
- IAM / Leastprivilege on System access

Impersonation / Masquerading

- Use of onetime pad, authentication token, Kerberos, encryption

PBX Notes

DISA (Direct Inward System Access)

↳ Uses access codes assigned to users to add a control layer for external access & control of the PBX..

Compromise of access codes = Attackers can make calls through PBX & even control.

- ATM — Cell — WAN Technologies

Packet Switching
- Frame Relay
- X.25

Circuit Switching
- T1
- POTS
- ISDN
- PPP