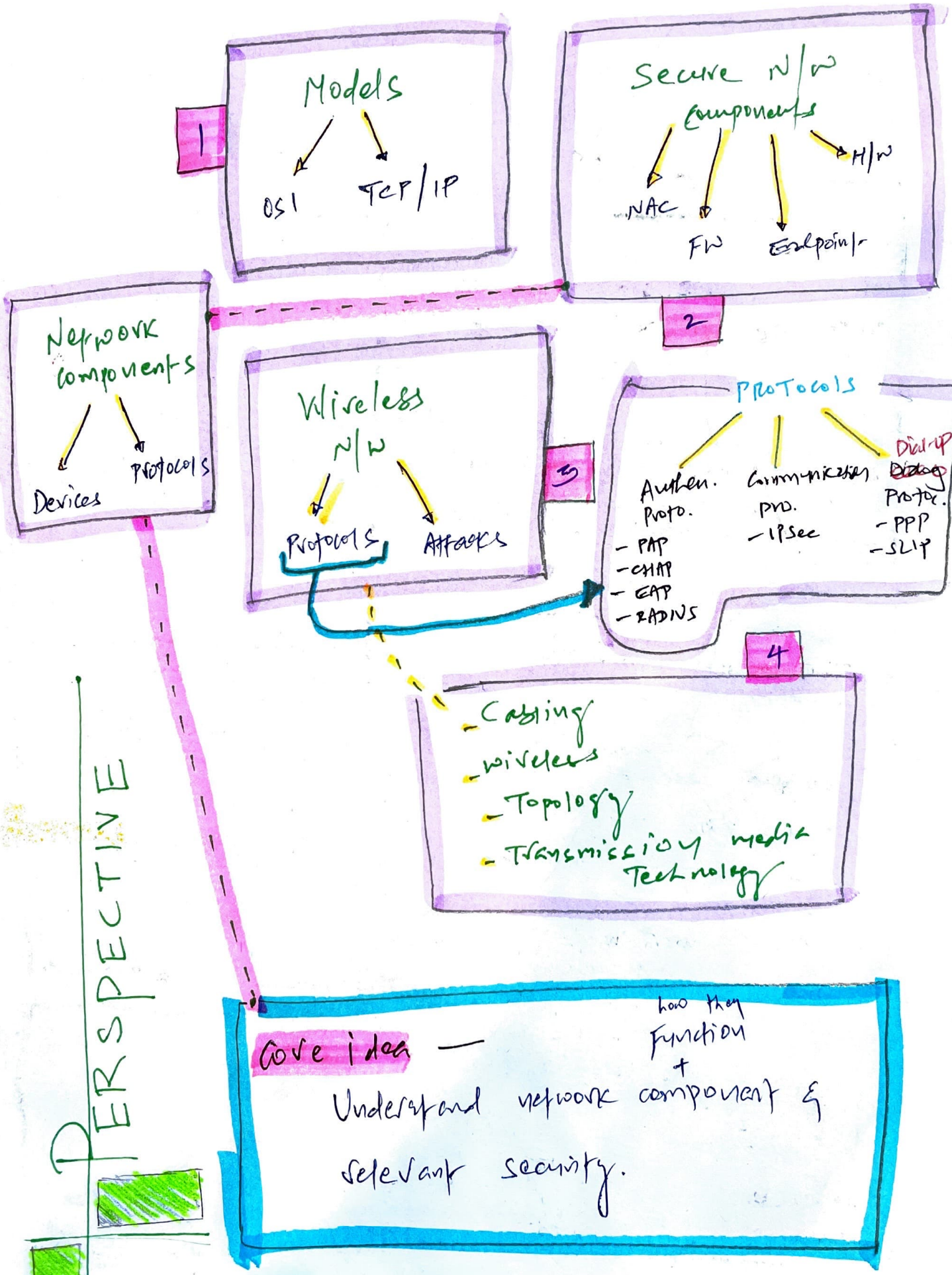
11. SECURING NETWORK ARCHITECTURE & SECURING NETWORK COMPONENTS



✱ OSI Model

Benefit

It's an expression of how networking actually functions.

CRITICAL

↳ Layer 7 is application & Layer 1 is physical

↳ Data streams associated with layer 7, 6, 5, from layer 4 they become segments, then packet-frame-

Application (7)

HTTP, FTP, LPD, SMTP, Telnet, EDI, TFTP, POP3, IMAP, SNMP, NNTP, S-RPC, SET

Presentation (6)

- Encryption & compressions
- Acts as interface b/w Network & Application
- Format types: JPEG, MPEG, ASCII, TIFF, EBCDIC, MIDI

(5) Session — comms mngmt.

- NFS, SQL, RPC
- simplex / full & half-duplex
- Retransmission failed PDUs

Transport (4)

- Integrity of connection & controlling session
- TCP, UDP, SSL, TLS, SPX

Network (3)

- ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP

(2) MAC → LLC

Datalink = Ethernet

SLIP, PPP, ARP, L2F, L2TP, PPTP, ISDN

Physical (1)

SONET

EIA/TIA-232 — V.24

EIA/TIA-449 — X.21, HSSI, V.35

PDU - protocol data unit

Segment - TCP, Datagram - UDP

Packet

Frame

Bits

TCP/IP Model

Application

= 1 + NFS + Windows

Transport

- host to host layer

TCP, UDP

Internet

IP, ICMP, IGMP

Link

Ethernet — FDDI

Fast Ethernet

Token Ring

Routing protocols

- Distance Vector
  - RIP
  - IGRP
  - EIGRP
- Link-state
  - OSPF
  - IS-IS

MAC = H/W Address

6 Byte / 48-bit binary address

00-13-02-1F-81-53

- 3 byte / 24 bits → Vendor of physical network interface (OUI) → organizationally unique identifier
- Unique number assigned to interface by mfg.

ARP

- Resolves IP to MAC
- Dependent on Ethernet's source & destination MAC
- not true layer 2 or 3 protocol — 2.5?

TCP/IP - How to use securely?

P.f.o TCP vulnerability

VPN

- For C, I & Authentication
- To establish VPN
  - PPTP
  - L2TP
  - IPSec
  - SSH
  - Open VPN (SSL/TLS)

TCP wrappers

Port based Access control

- Port based Access control
- An application that can serve as a basic firewall by restricting access to ports and resources based on user or system ID.

TRANSPORT LAYER PROTOCOLS < TCP / UDP

IP Address + Port = Socket

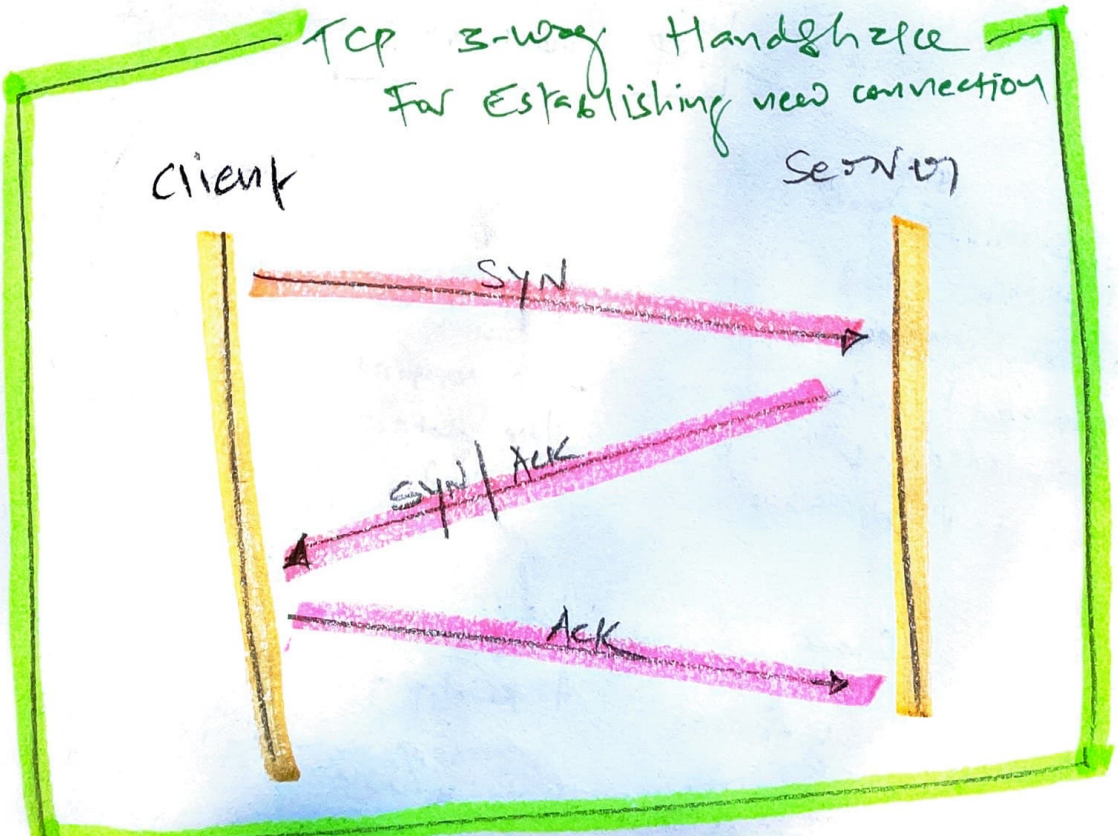
0-1023 = well known ports (service)

1024-49151
Registered s/w ports] - For client attempting to connect to their products

49152-65535
Random / dynamic / ephemeral ports / private ports

- used randomly - temporarily by client as a source port.

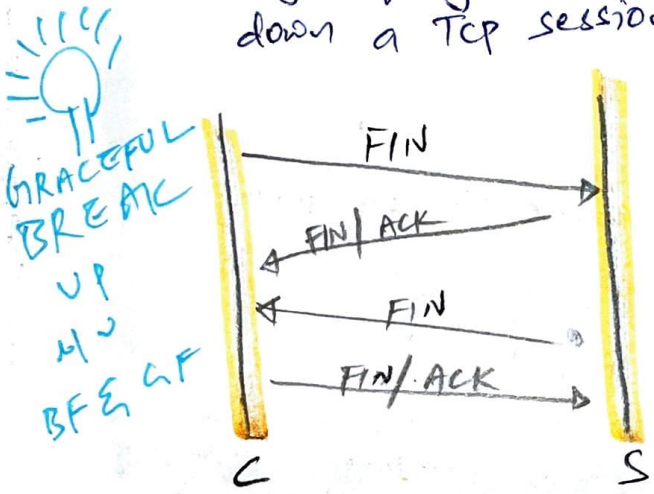
TCP 3-way Handshake For Establishing new connection



2 methods to disconnect TCP SESSIONS

FIN (finish) flagged packet

Three exchange of four packets for gracefully tear down a TCP session



RST (reset) flagged packet

cause immediate and abrupt session termination

GRACEFUL BREAK UP AND BFD GF

IP header protocol field value for UDP is 17

IP header protocol field value for TCP is 6

TCP concepts

Transmission window

- Number of packets transmitted before acknowledgement packet is sent

Sliding window

- To control the data flow

Stop small window = Use when comm is unreliable

Large window = Faster data transmission = Use when connection is reliable

REMEMBER FOR EXAM

TCP Header Flags

PSH
- Need to push data immediately to application

RST
- Reset: cause immediate disconnect of TCP session

CWR / ECE
- Explicit congestion notification
- Congestion window reduced — to manage transmission over congested links

SYN
- Request synchronization with new sequence numbers.

FIN
- Request graceful shutdown of TCP session

URG
- Indicates urgent data

ACK
- Acknowledges synchronization or shutdown requests

TCP header = 6 value

UDP header = 17

UDP --- IP also connectionless datagram service

Doesn't provide
- Reliable delivery
- Sequence no.
- Pre-establish session
- No error detection / correction
- No flow control

Employ TCP on IP for reliability & controlled communication sessions.

* IP ~~PROTOCOL SUITE~~ NETWORKING BASIC

CIDR (Classless Inter-Domain Routing)

└ Can combine multiple noncontiguous sets of address into a single subnet

class C subnet 1
class C subnet 2
class C subnet 3
→ one large subnet

IP classes — 255 = x

A — 1.0.0.0 to 126.255.255.255 — 255.0.0.0 /8

B — 128.0.0.0 to ~~222~~191.x.x.x — 255.255.0.0 /16

C — 192.0.0.0 to 223.x.x.x — 255.255.255.0 /24

D — 224.0.0.0 to 239.x.x.x — Reserved for multicasting

E — 240.0.0.0 to 254.x.x.x — Experimental

127.0.0.0 ← Loopback

255.255.255.255 ← Broadcast

IPv4 — 32-bit addressing

IPv6 — 64-bit addressing.

✱ NETWORK LAYER PROTOCOLS — ICMP, IGMP

ICMP
(Internet Control Message Protocol)

Purpose
- To check remote systems online / responding / check intermediate systems to remote end & to measure performance efficiency

Utilized by
- Ping
- Traceroute
- Pathping
-

Problems
- DDoS Attack
  - Bandwidth consumption
  - Ping Flood
  - Smurf Attack

Solution
- limit ICMP
- Block ping on FW
- limit throughput rate

Ping of Death
Sends larger Ping >65,535 bytes

Ping Flood
DoS Attack, consumes all bandwidth

Spoofing Broadcast pings → Smurf Attack
- Form of distributed DDoS Attack
- Exploits vulnerabilities of → ICMP → IP

Smurf attack generates enormous amount of traffic on target network by spoofing broadcast pings.

ICMP - Important Stuff
ICMP Header Protocol field = 1

ICMP Types

0 - Echo Reply	8 - Echo request
3 - Dest unreachable	9 - Router Advertisement
5 - Redirect	10 - Router Solicitation
	11 - Time exceeded

IGMP
(Internet Group Management Protocol)

IP Header Protocol field value

1

2

Purpose

Multicasting

Used By

- IP Hosts to register their dynamic multicast group membership.
- Connected routers to discover multicast groups.

ARP
(Address Resolution protocol)

Core operations

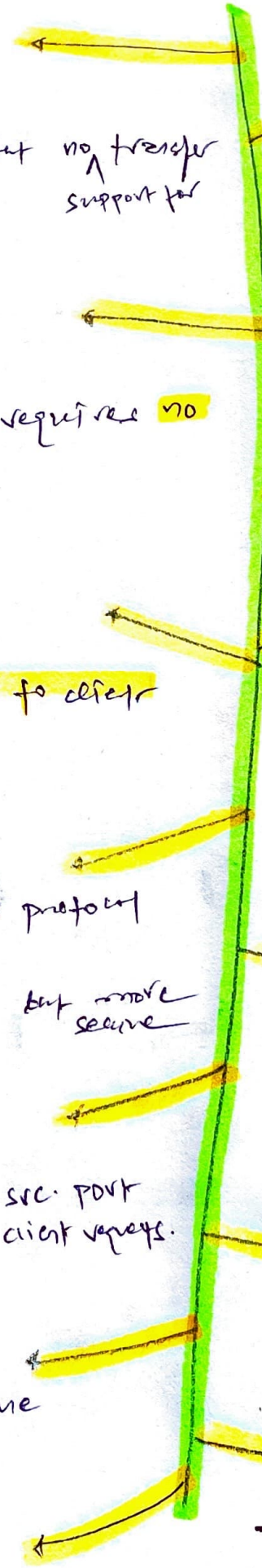
- Broadcast
- caching

Resolve IP to MAC

ARP cache poisioning

- Attackers insert bogus information in ARP cache

Common Application Layer Protocols



Telnet
- 23
- Remote connectivity but no transfer of files
support for

FTP
- 20 (TCP)
- Exchange of files requires specific authentication

TFTP
- UDP 69
- Exchange of files requires no authentication

SMTP
- TCP 25
- Email b/w 'c' & 's'

POP3
- TCP 110
- pull Email from server to client

IMAP > POP3

HTTP
- TCP 80
- Transmit web page elements from web server to web client

IMAP
- Internet message Access protocol
- TCP 143
- Same operation as pop 3 but more secure

SSL, HTTPS
- TCP 443
- Use TLS encryption
- VPN like secure protocol

DHCP
- UDP 67 & 68 → As src. port for client requests.
As dst port on server to receive client comms

LPD
- Line print Daemon
- TCP 515
- N/W service for spool print jobs

X window
- GUI App for command line operating system

SNMP → P.T.O
- UDP 161 used by SNMP Agent
- UDP 162 for Trap messages

NFS
- Network file system
- N/W file sharing.

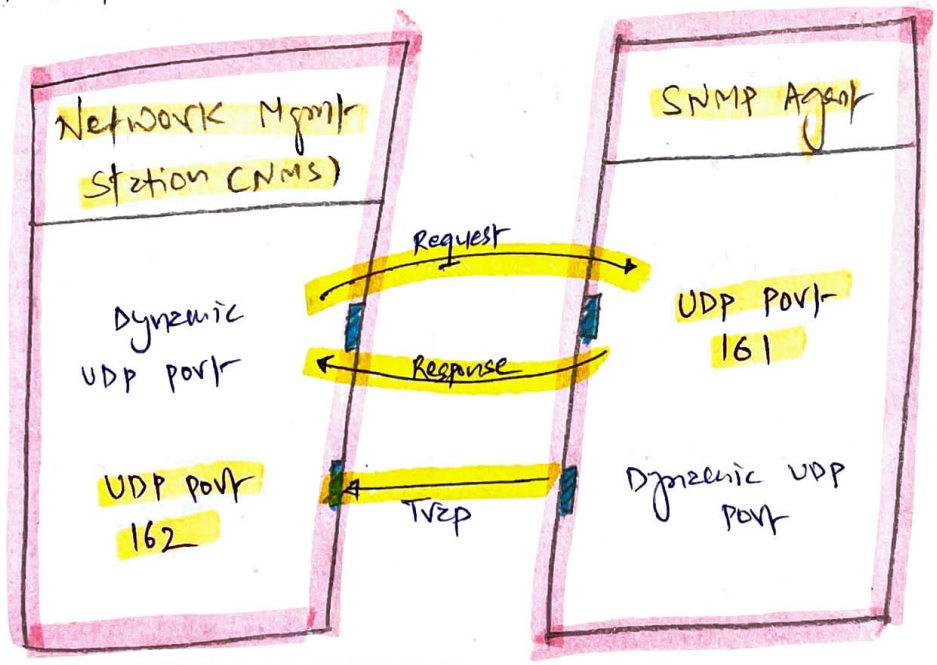
SNMP — is a network service used to collect health & status information by polling monitoring devices from a central monitoring station.

Early versions

- Plaintext transmission of community strings as authentication

latest versions

- Encrypted comms b/w device & mgmt console + Robust authentication factors



TCP/UDP ICMP IGMP ARP

TCP/IP is multilayer protocol

→ there are implications (P.T.O)

Application of multi-layer protocols

Introduction to encapsulations

Encapsulations

Pros

- wide range of protocols can be used at higher layers
- Encryption can be incorporated into various layers
- Flexibility & resiliency in complex network structure is supported

Cons

1. Covert channels are allowed - we can hide unauthorised protocol inside authorised one

[TCP [HTTP [FTP]]]
← Unauthorised protocol / Not secure

2. Filters can be bypassed

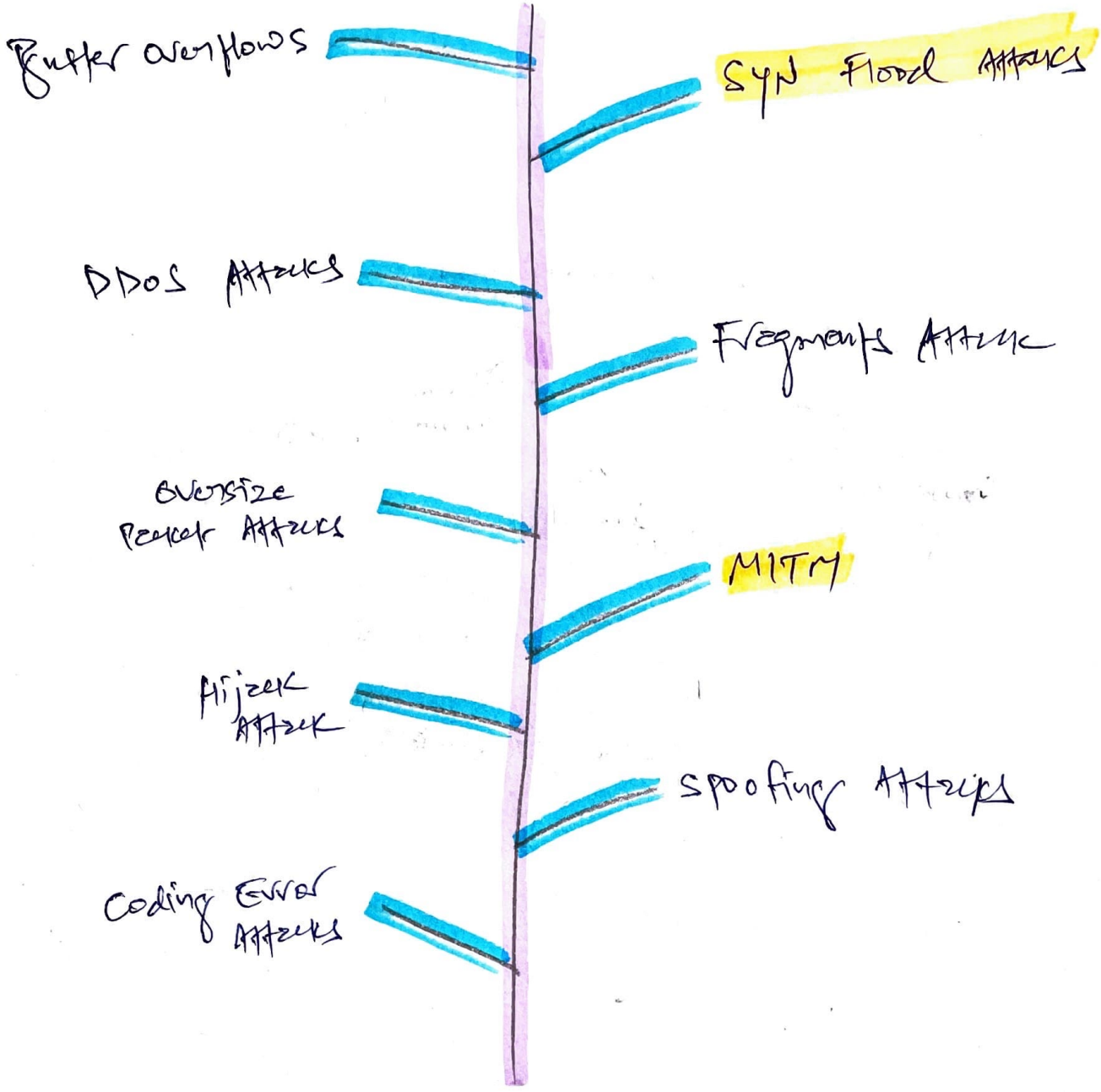
3. False Encapsulation -
E.g ICMP is only used to check health but with utilities such as LOKI, ICMP is transformed into tunnel protocol to support TCP comms.

4. logically imposed network segment boundaries can be overstepped.

5. Vlan Hopping -
Double Encapsulation where one switch remove outer tag for vlan 10 but next switch process traffic for hidden vlan 20

logically imposed network segment boundaries can be overstepped.

TCP/IP Vulnerabilities



Improper TCP/IP implementation in OS is vulnerable to above attacks

Name to IP **DNS** davekmurl.com → 46.1.2.3

A Record

DNS operates over TCP & UDP 53

IP to Name **Reverse DNS** → uses PTR DNS Record

46.1.2.3 → davekmurl.com

Need PTR Record

www.davekmurl.com

TLD = top level Domain

Subdomain / Hostname

Registered Domain Name

DNS Records

A
Address Record
FQDN to IPV4

AAAA
FQDN to IPV6

PTR
IP to FQDN (Reverse lookup)

SOA
Start of Authority Record
- Specifies authoritative information about zone file such as primary name server

CNAME
Canonical name
FQDN alias to another FQDN.

MX (Mail Exchange)
mail & messaging related FQDN to IP

NS
- Authorised Name Server Record

Then: DNS were handled by static HOST file.

Now: Dynamic DNS query (mostly for large N/W & Internet)

P.T.O more security methods

DNS security = DNSSEC

- DNS security Extensions
- function: To provide validate authentication b/w devices during DNS operations
- Use of digital cert to perform mutual Auth.

DNS poisoning

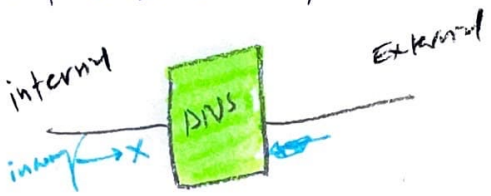
- Act of falsifying DNS information used by user to reach a desired system
- Trick → corrupt HOST file or DNS (zone file) server query.

Other ways to Exploit DNS

- Alter HOST file
  - Putting false DNS data on client machine to redirect to false location
- Corrupt IP information
- Deploy Rogue DNS Server
  - (DNS Spoofing)
  - (DNS pharming) — modify HOST file
  - Rogue DNS server respond to client with false IP Address before real DNS server
- Use Proxy falsification
  - only for web comms
  - Attacker plants false web proxy ~~server~~ data into client browser — then modify HTTP Packets
  - Rogue proxy server
- DNS poisoning.
  - Pro Placing incorrect info into Zone file → Real DNS server send false data to server

DNS SECURITY MEASURES

- Use DNSSEC
- Deploy NIDS
- Harden DNS server
- Limit zone transfer from internal DNS server to External DNS server



Block inbound

TCP 53 (zone transfer requests)

+

UDP 53 (queries)

Require internal clients to resolve all domains through internal DNS

Block outbound

UDP 53 (queries)

+

Keeping open outbound

TCP 53 (zone transfers)

Domain Hijacking

Sketch idea → Research Domain theft story for Fox-IT.com, sep 2017

CONVERGED PROTOCOLS

Software-Defined Networking (SDN)

TO DO FOR MORE

- Separated infra. layer from strategy to one vendor
- No concept of IP Address + subnets
- vendor neutral
- cfg. & mgmt of h/w controlled via centralized mgmt interface.

MPLS

- Directs data across network based on short Path labels rather than IP-based routing's longer network Addresses

Fibre channel over Ethernet (FCoE)

- N/w data storage / SAN operate over fibre optic cable
- Fibre channel operates on OSI Layer 2 (s/w)
- $$$$, need separate infra (cables)

Internet Small Computer System Interface (iSCSI)

cheaper option

- Networking storage standard based on IP
- Low cost alternative to fibre channel
- Enables location independent file storage, transmission & retrieval over LAN, WAN & Internet

VoIP

- transport voice / video / data over TCP/IP network
- VoIP as s/w + h/w

Content Distribution Network (CDN)

= low latency + high quality throughput + high availability + high performance of hosted content

WIRELESS NETWORKS

historically insecure
- defect insecure config from device mfg.

Data Emanation
- transmission of data across electromagnetic signals
- Hackers can re-create electron stream of magnetic field to reproduce data

802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 mbps	2.4 GHz
802.11n	200+ mbps	only 2.4 & 5 GHz
802.11ac	1 Gbps	5 GHz

* Securing Wireless Access Point

Deploy

Ad-hoc Mode
- Two wireless device with their own NIC can communicate with each other without centralized control authority

Infrastructure mode
- AP is required
- Wireless NIC on system can't connect directly

Four variation under Infrastructure mode

P.T.O

Infrastructure Mode

Stand-alone

AP to wireless clients but not wired

Wired-Extension

AP connects wireless clients to wired n/w

Enterprise Extended

Multiple AP connect to large physical area to serve wired n/w

Bridge

Wireless connection links two wired networks

linking n/w b/w floors or buildings

Myth Debunked – Service set identifier (SSID) is not a name of wireless network

SSID

Extended SSID (ESSID)

– Name of wireless n/w when WAP is used

Basic SSID (BSSID)

– MAC address of the Base station hosting ESSID

→ this helps to differentiate b/w multiple base stations

* Securing SSID - - - - - SSIDs are broadcast by WAP via special transmission called beacon frame.

We can hide SSID broadcast but wireless sniffer can discover it.

Don't disable broadcasting SSID instead use WPA 2 instead

* Important factors for site survey

- Ensure sufficient strength is available in all locations / (especially in TOILET :))
- Eliminate wireless signal from areas where access shouldn't be permitted (public area / outside the building)
- Planning + future deployments

cyber security

SECURE ENCRYPTION PROTOCOLS

There are two methods that wireless clients can use to authenticate to WAP before normal n/w comms. can occur across the wireless link.

Open System Authentication (OSA)

- No real Authentication required
- OSA transmits everything in cleartext = NO SECURITY

Shared key Authentication (SKA)

- Some form of authentication required before comms
- WEP → WPA → WPA 2 PTO

WEP (Wired Equivalent Privacy)

- can crack in 60 seconds
- Provides C & I using pre-shared key
  - key used to encrypt packets before transmission
- WEP Encryption employs Rivest Cipher 4 (RC4) → symmetric stream cipher
  - RC4 does 128-bit encryption
- Poor implementation of Initialization vector (IV)
  - Refer to wireless Attacks

WPA (Wi-Fi Protected Access)

- 802.11i was developed to replace WEP.
  - defines cryptographic solutions
- Uses MIC (message integrity check) / prevents MITM + replay attacks
- Based on LEAP & TKIP = not good, crackable
- Also, use of single passphrase for Authentication = downfall of WPA

WPA 2 = for IPsec level Encryption

- Amendment known as 802.11i
- New encryption scheme - CCMP (Counter Mode cipher Block chaining Message Authentication code protocol)
  - CCMP based on AES encryption scheme → provides 256-bit encryption

2017 KRACK ATTACK — Key Reinstallation Attack

Able to corrupt the initial four-way handshake b/w client & WAP into reusing previously used key

802.1X / EAP

Port-based Access control

- Client can't communicate with resource until proper authentication has take place

Extensible Authentication Protocol

- Not authentication mechanism but framework

EAP allows authentication technology to be compatible with existing wireless or P-2-P connections.

EAP-TLS
EAP-MD5
EAP Chaining

PEAP

- Protected EAP
- Usually EAP is not encrypted. PEAP can provide encryption for EAP methods
- Provides Authentication & Encryption

uses TLS

LEAP

- Vulnerable to ASLEAP ATTACK
- Lightweight EAP
- Cisco prop. to TKIP for WPA
- Avoid LEAP, use EAP-TLS

MAC Filter → Used by WAP to block access to non-authorised devices.

- MAB (MAC Authentication Bypass)

TKIP

TKIP improvement included key-mixing function that combines initialization Vector (IV) with secret root key before using that key with RC4 to perform encryption.

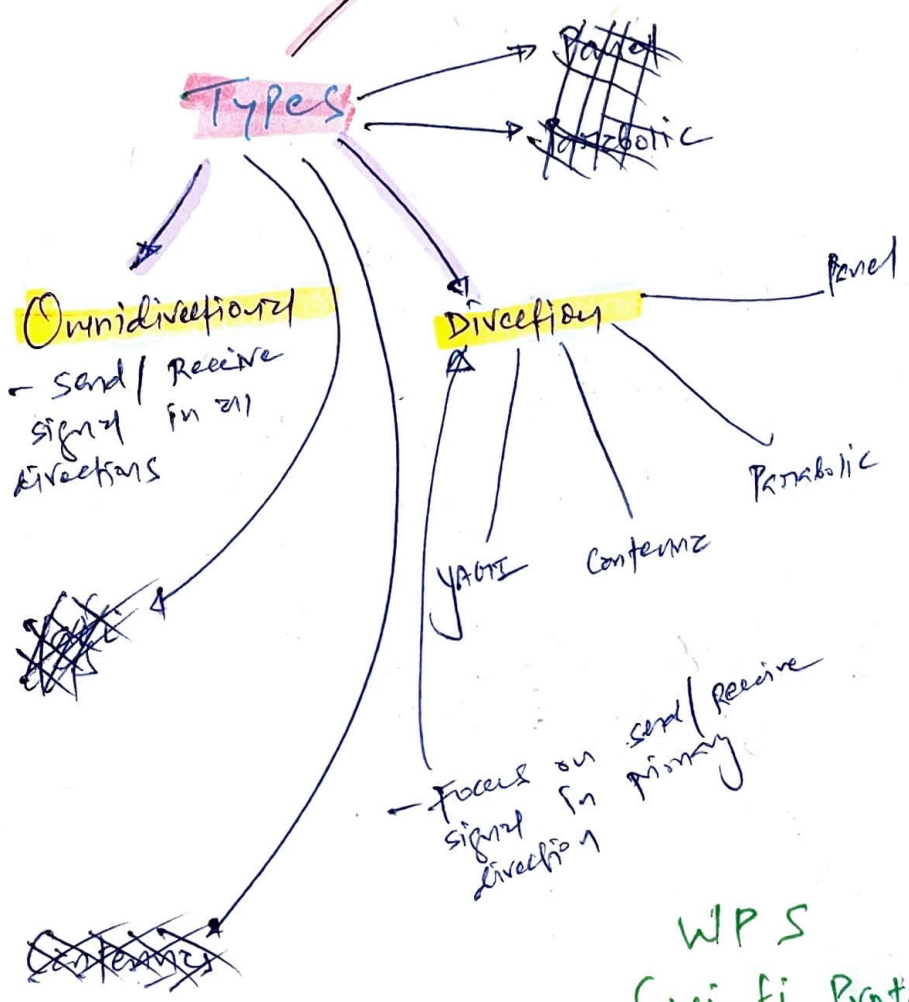
- Temporal Key Integrity Protocol
- Replacement of WEP
- Used with WPA but replaced by WPA2

CCMP

used by WPA2

- Uses AES with 128-bit key.
- No attack as yet.
- Created to replace WEP and TKIP / WPA

ANTENNA



Power levels

- Do it minor adjustment if wireless signals are not good after site survey & adjusting antenna
- Sometimes lowering Power level can enhance the performance

WPS
(wi-fi Protected setup)

- Security standard for wireless n/ws
- Simplifies effort for adding new clients to secured n/w
- Either press WPS button or call PIN (code) to trigger WPS remotely
- Leave it off unless you have to add numerous clients to wi-fi n/w.

Wireless Attacks

War Driving

- Use of dedicated handheld detector (PED - Personal Electronic Device) to crack wi-fi network
- Kind of performing malicious site survey for unauthorised purpose

War chalking

- Thief that make circle in dog on selected house

- → closed / secure n/w
- → open n/w

- It's faded.

Replay

- Focus: initial Authentication Abuse
- Retransmission of captured comms to gain access to target system

- Mitigation: Updated firmware of base station + W-IDS / W-NIDS

Reconnect request includes base station's MAC Address + SSID

IV (Initialization Vector)

- WEP's primary weakness = poor implementation IV

WEP IV is only 24bit long & transmitted in plaintext

- IV is a cryptographic random number
- IV is based on RC4

Rogue AP

- Usually discovered during site survey
- Rogue WAP duplicates valid WAP's MAC, SSID, channels
- Rogue WAP = social engg. Attack with look like SSID
- Sol: Use wireless IDS for rogue detection

Evil Twin (बहुरूपिया)

- False WAP automatically clone / twin using evasdropping when client reconnect to real WAP.
- It's a MITM Attack: session hij., data theft, credential theft
- Defense: Regularly purge old wireless profiles

Secure Network Components

Types of networks

- Intranet → Private
- Extranet → DMZ
- Internet → Public

Networks are segmented because ...

Boost Performance

E.g routers divide broadcast domains

Reduce communication problems

- Reduce congestion such as broadcast storms

Providing security

- isolate traffic + user access for authorised purpose

Do segment using

- VLANs
- Routers
- switches
- Firewalls

CRITICAL

- Multihomed FW
- FW Deployment Architectures

p.t.o.

End