WIRELESS

+ TYPES OF WIRELESS N/W:

- WPAN: • Bluetooth.
  • short distances (30 feet MAX).
- PAN is unlicensed.

- WLAN: • Data Rate upto 2 Mbps (200-300 feet)
  • 802.11 standard.
- also unlicensed frequency.

- WMAN • low budget bridging network.
- fiber connections are ideal to build an ultra-solid backbone network.

- WWAN • latest cellular network.
  • very large geographical area.

+ WIRELESS DEVICES:

- WAP • central junction point for wireless stations.

AP functions as a bridge between wired & wireless network.

SOHO APs come in 2 flavors - Stand Alone
- Wireless Router

* Autonomous AP: configured, managed & maintained in isolation.
* Lightweight AP: gets its config from central device like Wireless Controller.

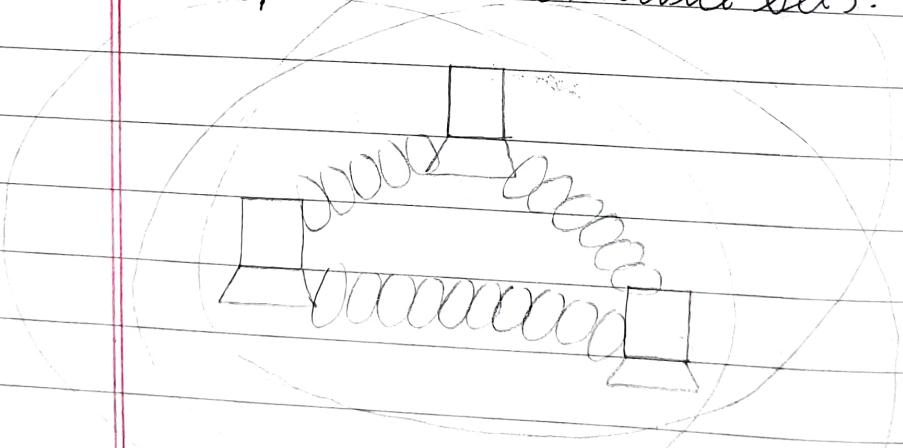
- WNIC
  - Nowadays WNIC comes built in with PC (Network Interface Card).
- W. Antennas
  - omnidirectional (Point to Multipoint)
  - directional (point to point) / Yagi

YAGI > OMNI

→ WIRELESS PRINCIPLES

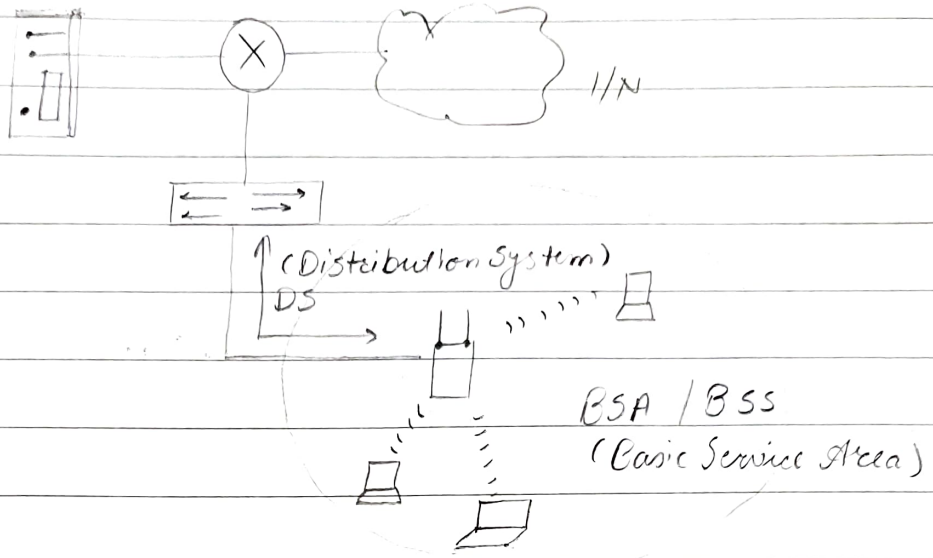
- Wireless Topologies / Architecture

Ad-hoc (Independent Basic Service Set):



- No AP is needed.
- 20-40 metres.
- does not scale well.
- very insecure.

Infrastructure (Basic Service Set)



- Use AP to communicate
- SSID needed.

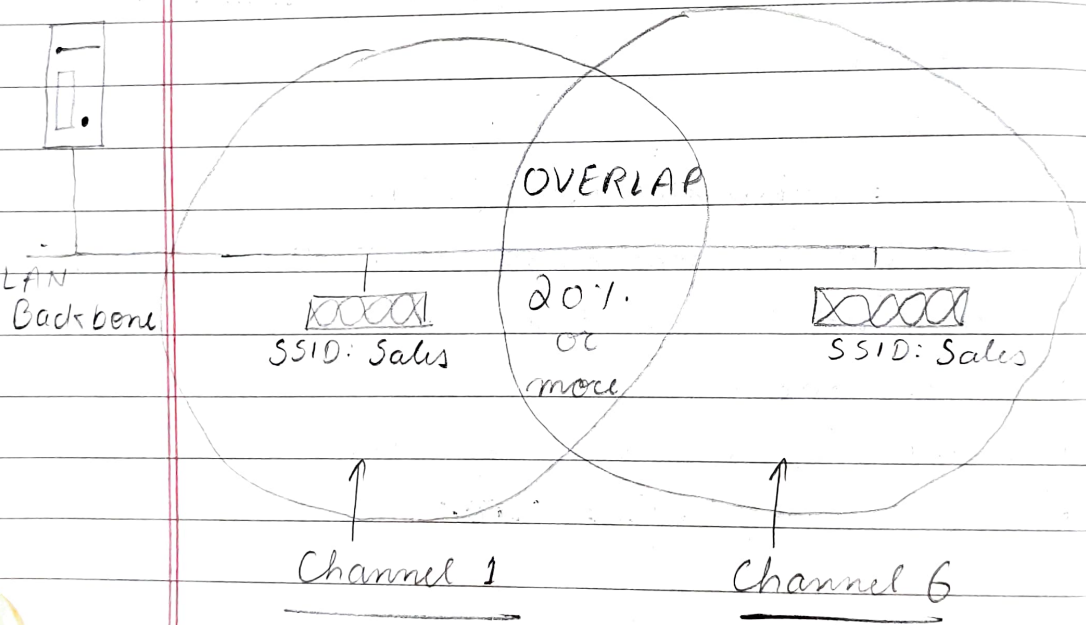
SSID (Service Set Identifier):

- SSID is a Basic name that defines BSA, transmitted from AP.
- 32 characters long
- ASCII (human readable character)
- Sequence of 1-32 OCTET.

- The network is identified by SSID.
- AP associates a MAC (virtual) to the SSID. or it can be BSSID or MBSSID
  - BSSID → Base
  - MBSSID → Multiple

ESS (Extended Service Set):

- ESS allows users to roam from one AP to another without disconnecting the network.
- AP must overlap by 20% of their signal or more to their neighbor's cell. channels (frequency) of each AP should be different.

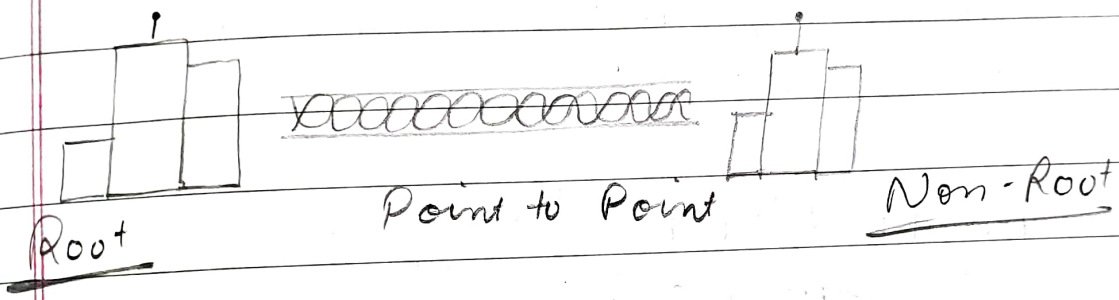


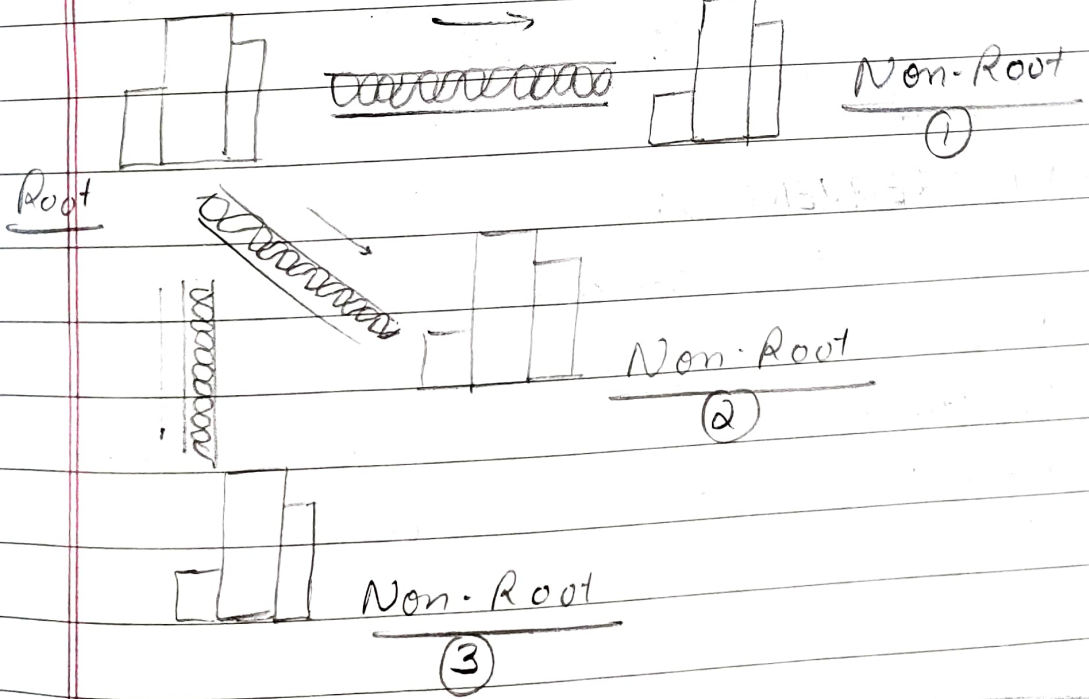
Repeater:

- gain of directional antenna. overlap needed.
- for every repeater installed, you loose half throughput
- So it is only useful for low bandwidth

Bridging :
- connect 2 or more wired LANs.
- usually located within seprate buildings.
- No routing capabilities.

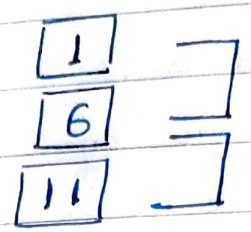
→ Point To Point
→ Point To MultiPoint





→ NON OVERLAPPING CHANNELS →

2.4 GHz Band :



When you have 2 AP in same area on over-lapping channel, it effect network performance.

5 GHz Band : UNII 1 | lower 36, 40, 44, 48
UNII 2 | middle 52, 56, 60, 64
UNII 3 | upper 149, 153, 157, 161

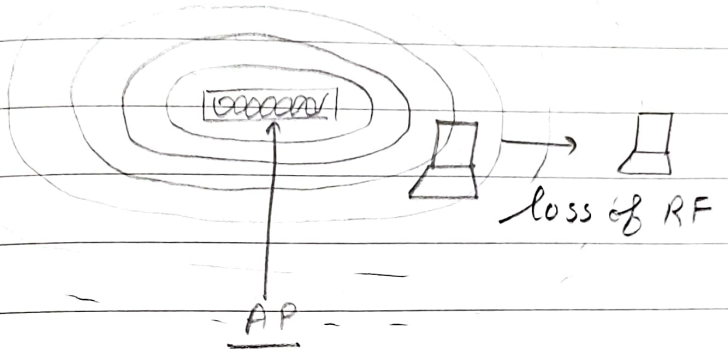
→ RF (RADIO FREQUENCY) :

signal transmission via radio waves.
1 Hz : RF cycle occurs once a second.
1 MHz : RF — — one million times / sec.
1 GHz : RF — — one billion — —

- lower frequency travel farther but provide less bandwidth.
- higher frequencies can't travel long distances. they carry higher bandwi.

RF problems:

Free space path lost:



Absorption: ✓

Reflection: ✓

Multipath: multiple reflecting surfaces.

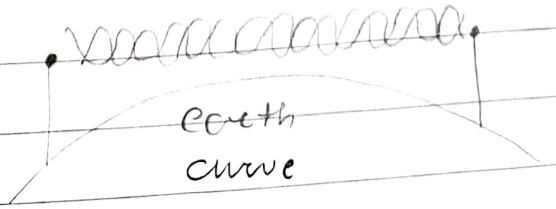
Refraction: ✓

Diffraction: Signal bend around an object.

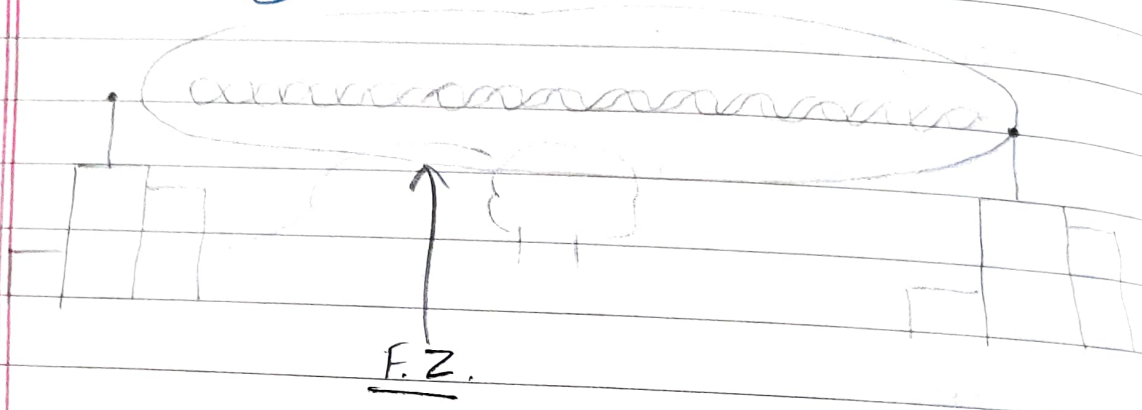
Scattering: ✓

RF operational Requirments:

- Line of Sight



- Fresnal Zone



→ FZ should be at least 60% clear for signal transmission.

RSSI (Received signal Indicator)
−30 db to −60 db is ✓

SNR (Signal to Noise Ratio)

WIRELESS SECURITY:

Open Access: Any device can join the network if it is in range of AP.

- Authentication is done at L2.
- not secure.

WEP (Wired Equivalent Privacy):

→ WEP prevents client from sending & receiving data from an access point until client enters correct WEP keys.

→ WEP key is compost of 40 or 128 bits & statically defined by network admin on the AP.

WPA (Wifi protected access)

- PSK
- RADIUS / TACACS

	WPA	WPA 2	WPA3
AUTHENTICATION			
A. ENTERPRISE			
	802.1X / EAP	802.1X / EAP	802.1X / EAP
	TKIP / MIC	AES - CCMP	GCMP 256
B. PERSONAL			
	PSK	PSK	PSK
	128 Bit RC4 W/ TKIP	128 - AES	128 - AES

ROUTING:

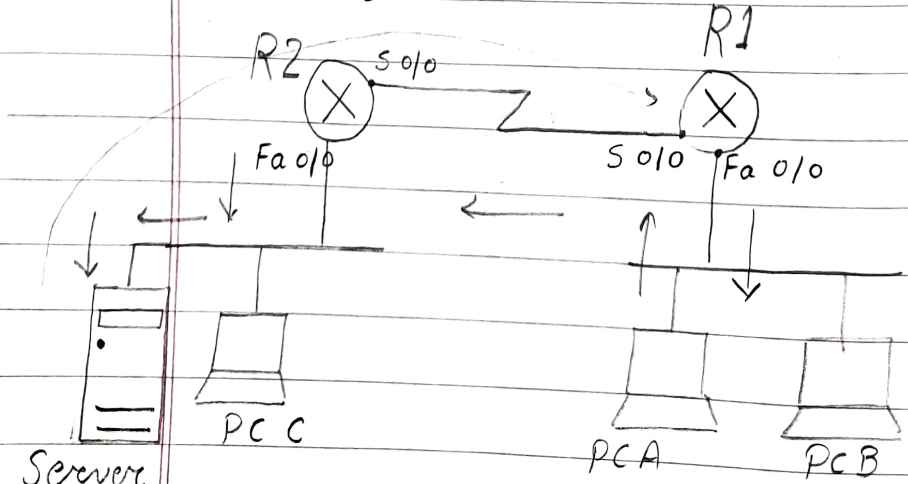
factors, a router must know to be effectively route packets:

1. Destination address.
2. Neighbor routers.
3. Possible routes to all remote network.
4. Best route to each remote network.

ROUTING PROTOCOL CODES:

C	(Connected (Directly)
S	(Static Route)
I	(IGRP)
R	(RIP)
B	(BGP)
D	(EIGRP)
EX	(EIGRP external)
O	(OSPF)
L	(Local host route)

ROUTING PROCESS:



Scenario:

PC A wants to communicate Server.

PC A will place server's IP in the destination of IP header & his IP as source.

To send it out, it must go through the L2. So PC will place its MAC in source of L2 header & MAC of Fa 0/0 (R1) in the destination.

Packet will reach R1, R1 will open the IP packet and will realize that the destination IP is on another network.

R1 will check its IP Routing table & after that identifies that the exit interface should be S0/0 (R1).

Again it will have to go through ARP & MAC addresses.
Finally packet will reach F 0/0 of R2 and R2 will see its distination as Server on his own network.
And the packet will be delivered.

ROUTING TYPES:

1. STATIC 2: DYNAMIC 3. DEFAULT

- STATIC ROUTING:

→ No overhead on Router's CPU as router has to be configured statically.
→ No Bandwidth usage between routers, saving money on WAN links.
→ Not fesible for larger networks.

ip route 192.168.10.0 255.255.255.0 172.16.10.2 150 furmanent.

[if this applied, after shutting an int, routes will wiped out automatically.]

- DEFAULT ROUTING:

(Gateway of last resort)

→ Default route is used by IP to forwa-rd any packets with a distination not found in the routing table.

ip route 0.0.0.0 0.0.0.0 172.16.10.5
(default)

- DYNAMIC ROUTING:

Adminstrative Distance: It is used to rate the trustworthiness of routing information received.

AD = 0 — 255

most trusted — No traffic

Default AD	Route Source
0	Directly Connected
1	Static Route
20	External BGP
90	EIGRP
110	OSPF
120	RIP
170	External EIGRP
200	Internal BGP
255	Unknown

115 → 1515

Distance Vector: hop count. (Ex: RIP)

Link State: Bandwidth (Ex: OSPF)

Advance Distance Vector: distance + Bandwidth (Ex: EIGRP)

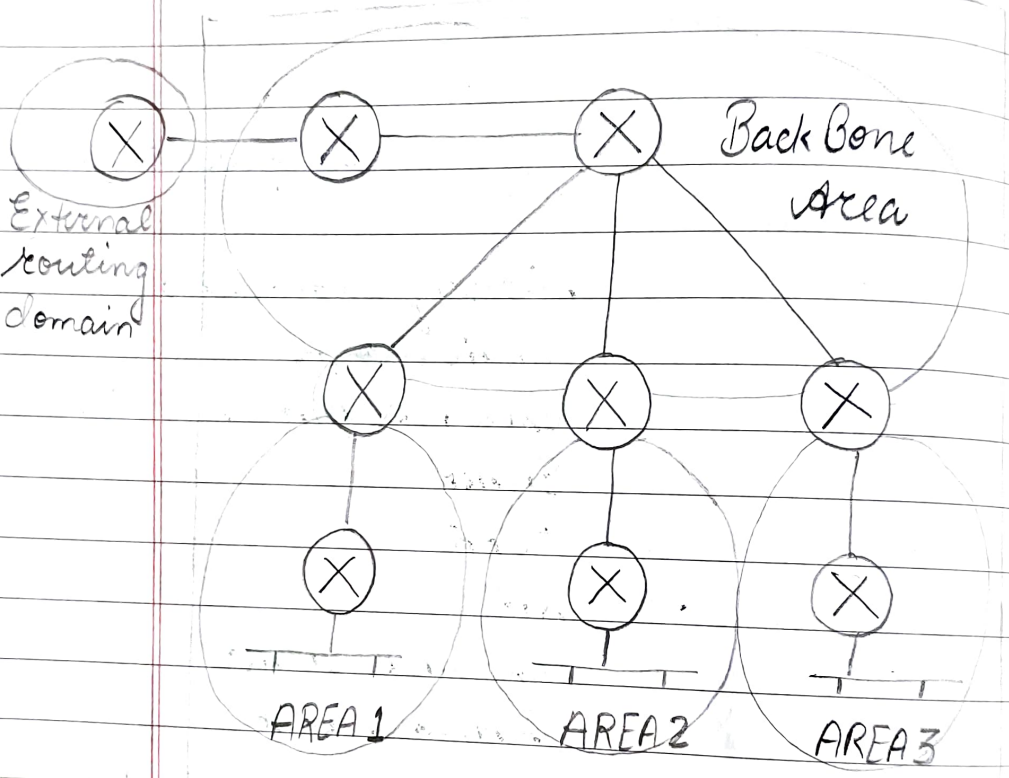
↑

METRICS

LSA updates Multicast address

- POINT TO POINT → 224.0.0.5
- BROADCAST → 224.0.0.6
- POINT TO MULTIPOINT → NA

OSPF:
- Allows for creation of areas & AS.
- minimize routing update traffic.
- highly flexible, versatile and scalable.
- supports VLSM / CIDR.
- unlimited hop count.



» AUTONOMOUS SYSTEM 1

* OSPF Design

Link: network or router interface

Router ID: IP address used to identify the router.

↓ highest IP of all loopback interf.
highest IP of all active physica interfaces.

Date
Page

Neighbor: Following should be same between the neighbors:

AREA ID

STUB AREA FLAG

AUTH. PASSWORD (if using one)

HELLO & DEAD INTERVALS

Adjacency: Relationship between 2 OSPF routers.

DR (Designated Router): DR is elected whenever OSPF routers are connected to same broadcast network to minimize number of adjacency.

- Elections are won based on router's priority level.
- If tie, RID breaks it.

BDR: Hot standby for the DR on broadcast. BDR receives all routing updates from OSPF adjacent routers.

- It does not disperse LSA updates.

Hello protocol: 224.0.0.5

LSA: OSPF router will only exchange LSA with routers it has established adjacency for.

OSPF Area: Grouping of contiguous network & routers.

- All router share a common Area
- All routers in the same topology area shares same routing table.

OSPF Operation →

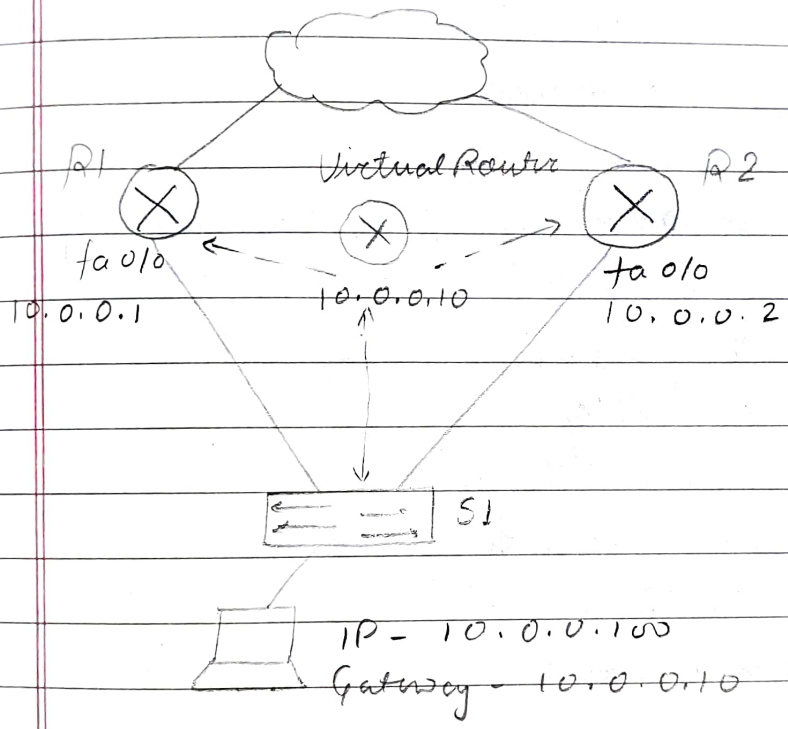
1. Neighbor & Adjacency initialization
2. LSA Flooding
3. SPF Tree Calculation

router ospf 1 (PID)
network 10.0.0.0 0.255.255.255 area 0
(WILDCARD)
passive-interface fa 0/1
default-info originate
int loopback 0
ip add ___ ___

sh ip ospf
" " " database
sh ip protocols

FHRP: To prevent single point of failure, FHRP gives us way to configure more than one physical router to appear as a single logical one.

The virtual router has its own IP & MAC.



HSRP (HOT STANDBY)
- Cisco's proprietary
- Standby group will share IP & MAC.
- don't load balance

VRRP (VIRTUAL ROUTER REDUNDANCY)
- IEEE (open standard)
- same as HSRP.

GLBP (GATEWAY LOAD BALANCING)
- LOAD Balancing
- Cisco's pro.

Date
Page

SECURITY FUN:

Vulnerability: weaknesses present in a system.

WHY DO THEY EXIST?

- Bugs or flaws in H/W or S/W
- Bad configuration
- Legacy systems
- Unpatched systems
- HUMANS!!

Exploit: Takes advantage of a vulnerability.

Threat: Anything that can exploit a vulnerability

- Unstructured Threats
- Structured Threats
- External Threats
- Internal Threats

Mitigation:

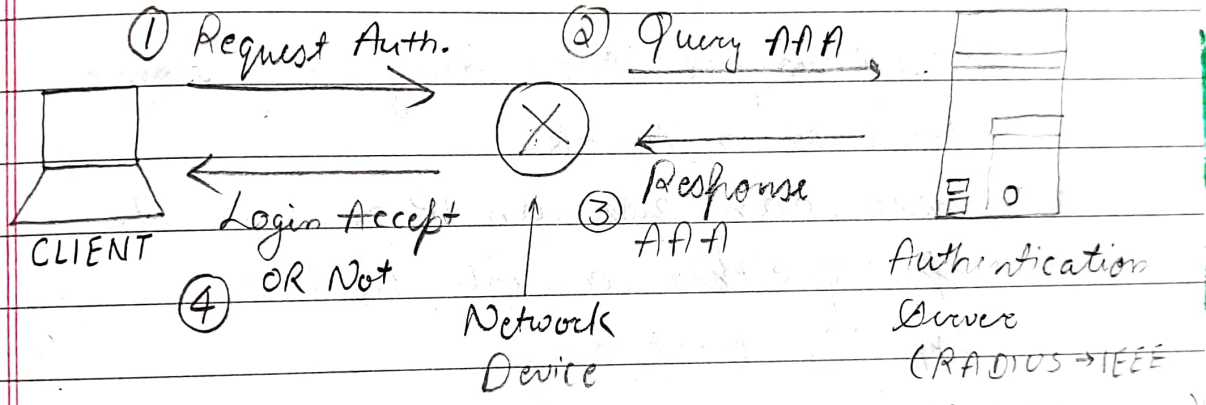
- Awareness
- Apps OWASP
- Net Infrastructure
- HUMANS: Training & Testing
- AUPs., etc.
- Password elements.

Multi Factor Authentication:

- By something they know (Password / Pin)
- ——— are (eyes, Biometric)
- ——— posses (key, card, OTP)
- ——— do (behavior)

AAA concepts:

1. Centralized Server
2. AAA Clients
3. Protocols (RADIUS, TACACS+)



(AAA Working)

aaa new-model
username ——— password ———
radius/tacacs+ server Secure Login
address ipv4 ———
key ———

aaa group server radius/tacacs+ ———
server name ———
aaa authentication login default gr. ———
local

ACLS : • Comparison in sequential order.
(line 1 -> 2 -> 3 --)

- Every packet is compared with lines of access-list until a match is made.
- Implicit - deny.

TYPES:

STANDARD ACCESS LIST:

Range : 1 - 99
1300 - 1999

→ used to permit or deny any source host or network.
→ user can use an IP address to specify either a sigle host or a range.
→ specify host only

- access-list __ deny N/W WILDCARD
- permit ___ ___

EXTENDED ACCESS LIST:

Range: 100 - 199
2000 - 2699

- can filter application layer.
- can select port no

access-list 110 permit tcp any host 172.16.0.1 eq 23 log
access-list permit ip any any

NAMED ACL:

- A way to create ACLs by 'name'.
- easier to maintain.

MAINTANANCE:

show access lists —
show —— name / no

* Standard ACL should be placed near to the destination of the packets.

eq ftp-data	20
ftp	21
telnet	23
smtp	25
domain	53
bootps	67
bootpc	68
tftp	69
www	80
pop3	110
snmp	161

Interchangable

NAT: Private IP ⟷ Public IP

TYPES: Static: one to one
Dynamic: many to many
Overloading PAT: one to many

TYPES OF N/W:
Inside local: Inside Internal network private, owned by you
Outside local: Address of an outside host as it appears to the inside network.
Inside Global: The NAT-IP (actual public IP of the host on Internet)
Outside Global: External network, global IP address.

STATIC Conf.:
ip nat inside source static 10.1.1.1 170.46.2.2

DYNAMIC Conf:
ip nat pool abc 170.162.1.2 170.16 2.1.30 netmask 255.255.255.0
ip nat inside source list 1 pool abc

PAT: ip not inside source list 1 pool abc overload

VPN: creation of private network across the internet.

- tunneling of IP & non-TCP/IP protocols.

Security
Cost Saver
Scalable
compatibility

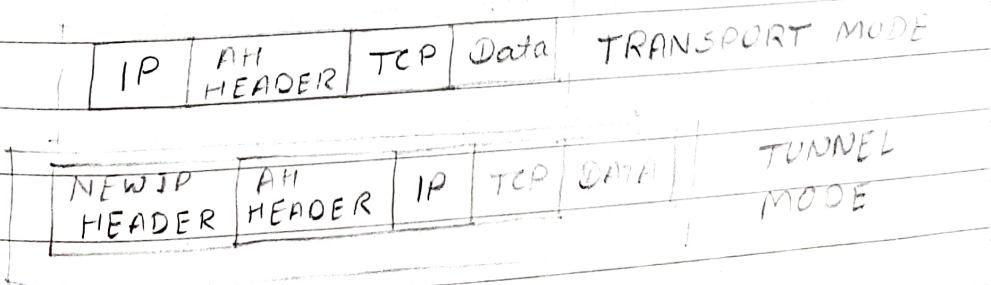
Remote Access VPN: Remote users to securely access corporate network.

Site to Site: A company to connect its remote sites without expensive Frame Relays.

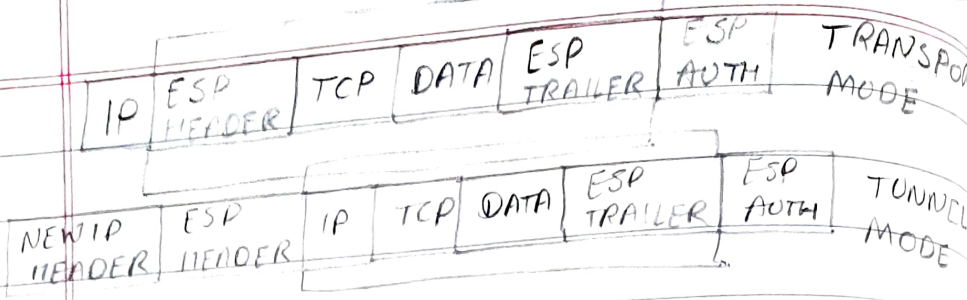
IPSEC: Umbrella of many security protocols.

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)

AH: One way hash for packet Authentication
ESP: Confidentiality, Data Integrity, Authentic-ation, Anti-Replay service, Traffic Flow.



AH



ESP

GRE Tunnels + IPSEC

Configuration of tunnels:

```
int tunnel 0
tunnel mode GRE ip
tunnel source ____
tunnel destination ____

sh int tun 0
```

— — —

L2 MPLS VPN:

VPWS (Virtual Private Wire Service) = EoMPLS

VPLS (V. P. LAN Switching Service)

L3 MPLS VPN:

L2 forwarding

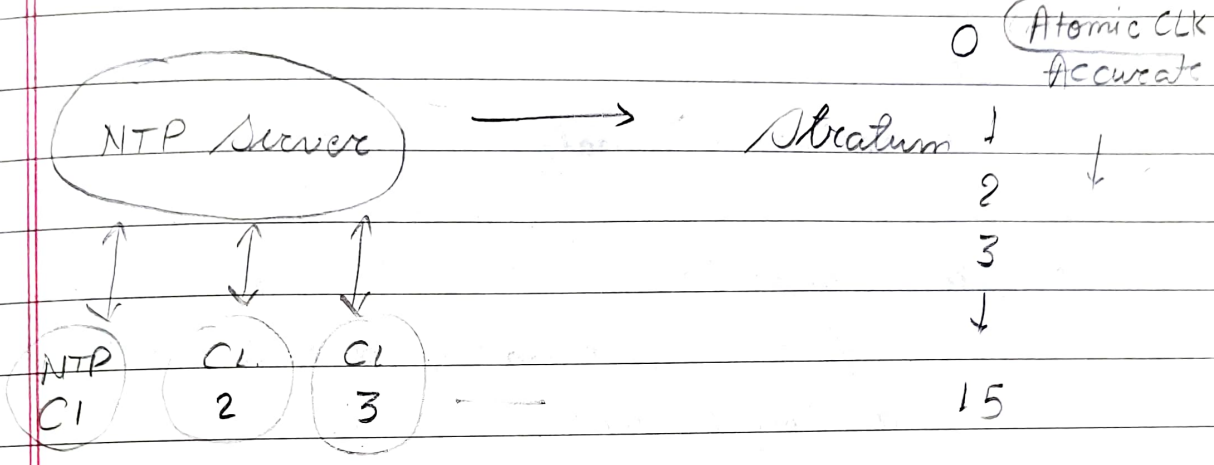
PPTP

L2TP

GRE

NTP: describe time for all your network devices.

- clock synchronization is very critical for logs & traking of events in the network.



ntp server ___ IP ___ master / server

sh ntp (Associations)

sh ntp (status)

~+

clock set 10:00:01 15th May 2020

sh clock

— — —