CCNA

Book 2
(Routing and Switching)

Prepared by:
Eng. Ahmed Nabil
(DoN)

Session 13 outlines :

- Static Routing.
- Dynamic Routing :
  - RIP v2.

Ahmed Mahmoud

Ahmed Mahmoud

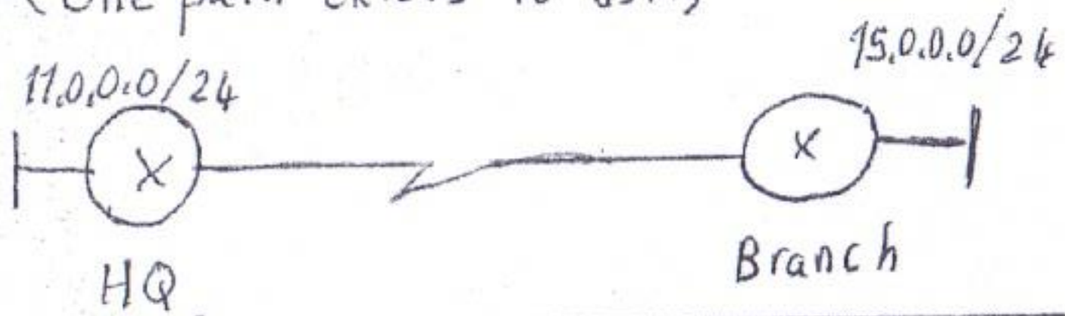
Session 1:/1

Routing Classification

Static Routing

- Building routing table **manually**
- Used if network is **simple**

(One path exists to dst.)

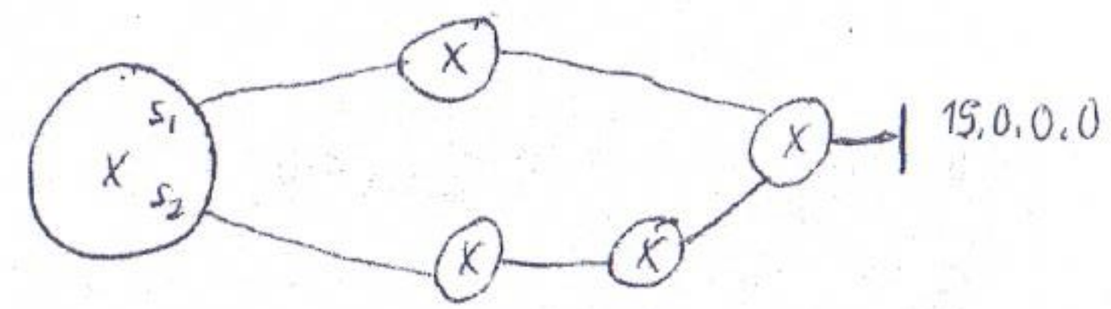


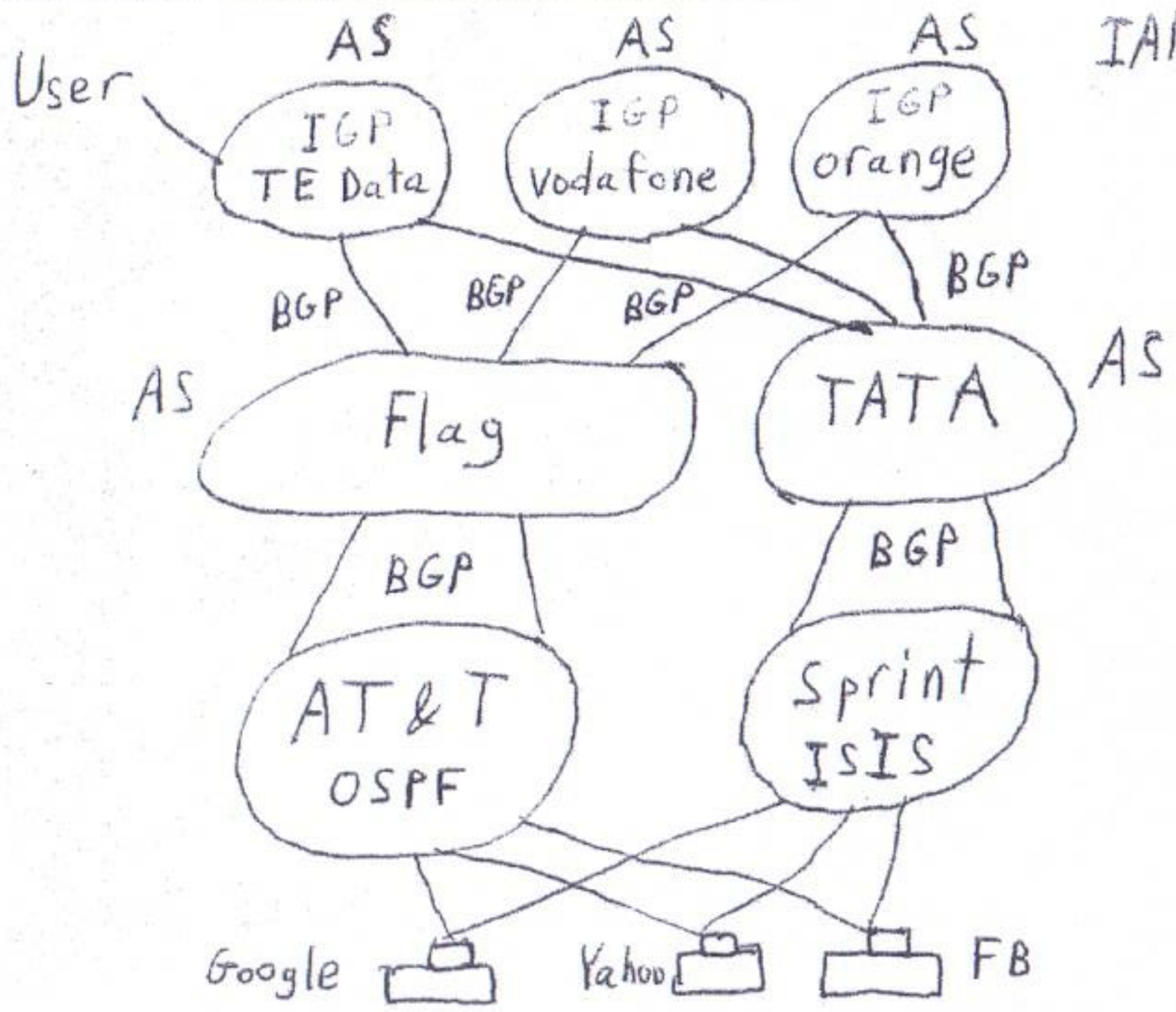
Dynamic Routing

S/W

- Building routing table **automatically** using protocols
- Used if network is **complex**

(many paths exist to dst.)





IANA
- IP
- AS no. (unique number) (1-65,535)

Dynamic Routing

IGP — Interior Gateway Protocol

- Distance Vector: RIP$_{v1}$, IGRP
- Advanced Distance Vector: RIP$_{v2}$, EIGRP
- Link state: ISIS, OSPF

Protocols that run inside Autonomous System (AS)

EGP — Exterior Gateway Protocol

EGP

BGP: Border Gateway Protocol

Protocols that run between ASs.

Static Routing: The router has 2 Tables: Routing & Arp Tables

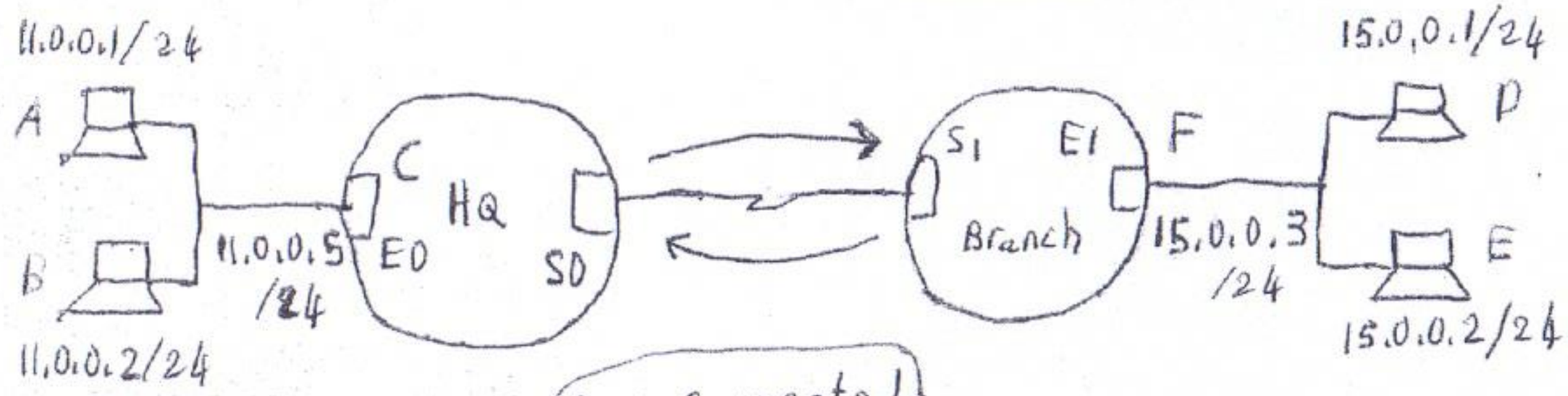
Session 1 /2

Arp Cache

MAC	IP
A	11.0.0.1
B	11.0.0.2
C	11.0.0.5

Arp Cache

MAC	IP
D	15.0.0.1
E	15.0.0.2
F	15.0.0.3



C → Connected
S → Static

Routing Table

	Network	Mask	Vector
C	11.0.0.0	/24	E0
S	15.0.0.0	/24	S0

Routing Table

	Network	Mask	Vector
C	15.0.0.0	/24	E1
S	11.0.0.0	/24	S1

Vector = Exit Interface

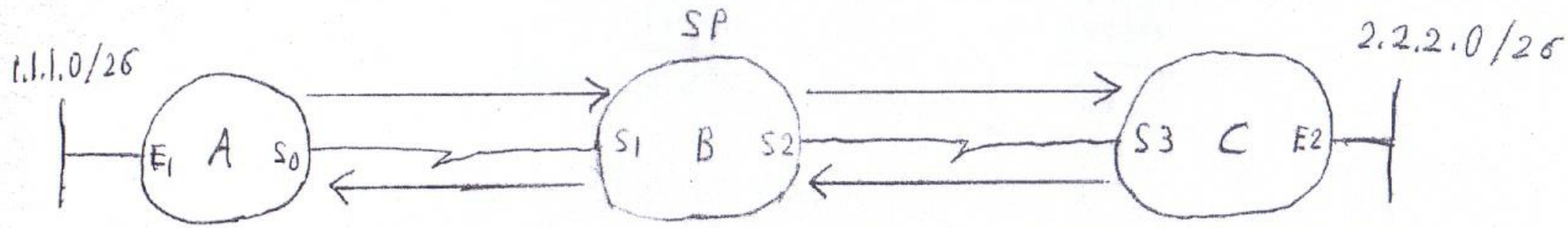
* If dst. IP (static) doesn't exist in the routing table, the router will drop the data (UnKnown IP).

Command: HQ(config#) IP route 15.0.0.0 255.255.255.0 S0
(network, mask, vector)

Branch(config#) IP route 11.0.0.0 255.255.255.0 S1

Session 1 /2

* We need network 1.1.1.0/26 to reach 2.2.2.0/26 & vice versa.



C	1.1.1.0	/26	E1
S	2.2.2.0	/26	S0

S	2.2.2.0	/26	S2
S	1.1.1.0	/26	S1

C	2.2.2.0	/26	E2
S	1.1.1.0	/26	S3

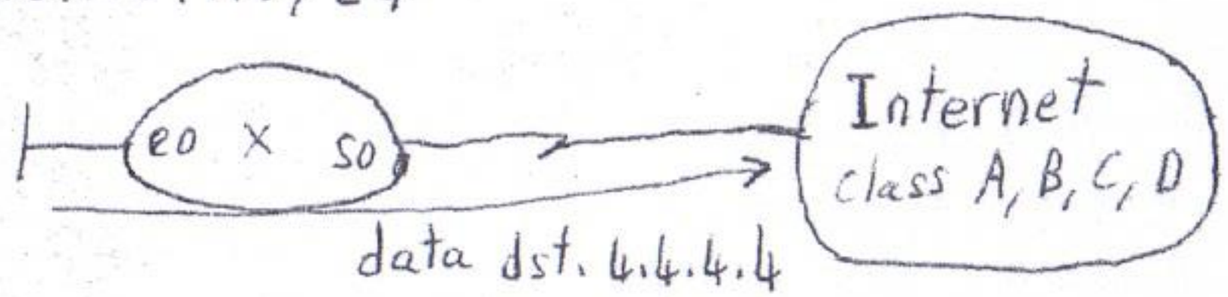
A(config)# IP route
2.2.2.0 255.255.255.192 S0

B(config)# IP route
2.2.2.0 255.255.255.192 S2
1.1.1.0 255.255.255.192 S1

C(config)# IP route
1.1.1.0 255.255.255.192 S3

Home Router (Stubrouter) ⇒ Default Static

192.168.1.0/24



Homerouter(config)# IP route 0.0.0.0 0.0.0.0 S0
all networks mask vector

C	192.168.1.0	/24	E0
S*	0.0.0.0	/0	S0

→ Last resort & Static to all

Session 1 /4

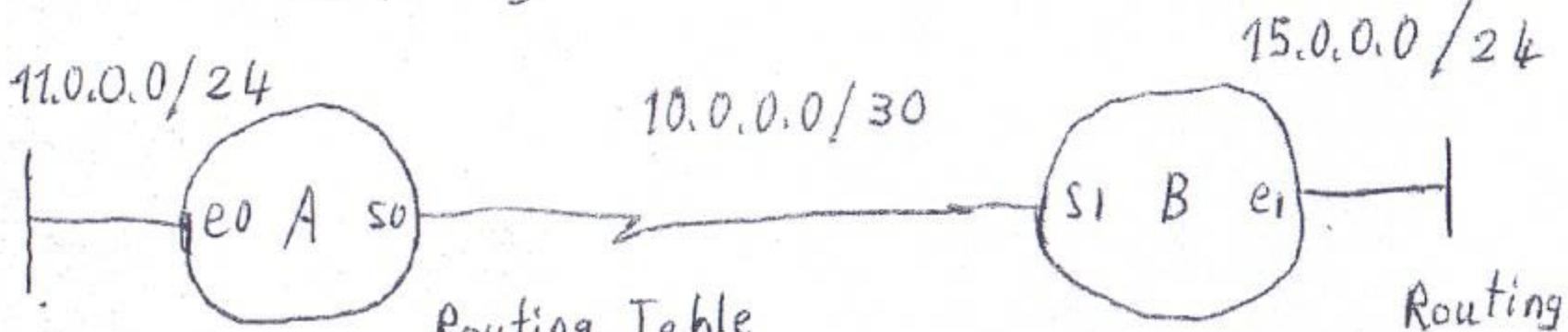
Dynamic Routing:

Advanced Distance Vector (RIP_{v2})

Routing Information Protocol → Routers signaling

* RIP: Exchange information between Routers.
* Metric = Distance = Hop #

@Startup: 1 (Config) # router rip
2 (config-router) # version 2



Routing Table

	Network	Mask	Vector	Distance
C	11.0.0.0	/24	e0	0
C	10.0.0.0	/30	s0	0

Routing Table

	Network	Mask	Vector	Distance
C	15.0.0.0	/24	e1	0
C	10.0.0.0	/30	s1	0

Advertisment/Update →

	metric
11.0.0.0/24	1
10.0.0.0/30	1

← Advertisement/Update

	metric
15.0.0.0/24	1
10.0.0.0/30	1

After Last Update (A)

C	11.0.0.0	/24	e0	0
C	10.0.0.0	/30	s0	0
R	15.0.0.0	/24	s0	1
~~R~~	~~10.0.0.0~~	~~/30~~	~~s0~~	~~1~~

RIP ← (R)

← short distance

long distance

After Last Update (B)

C	15.0.0.0	/24	e1	0
C	10.0.0.0	/30	s1	0
R	11.0.0.0	/24	s1	1
~~R~~	~~10.0.0.0~~	~~/30~~	~~s1~~	~~1~~

← short distance

long distance

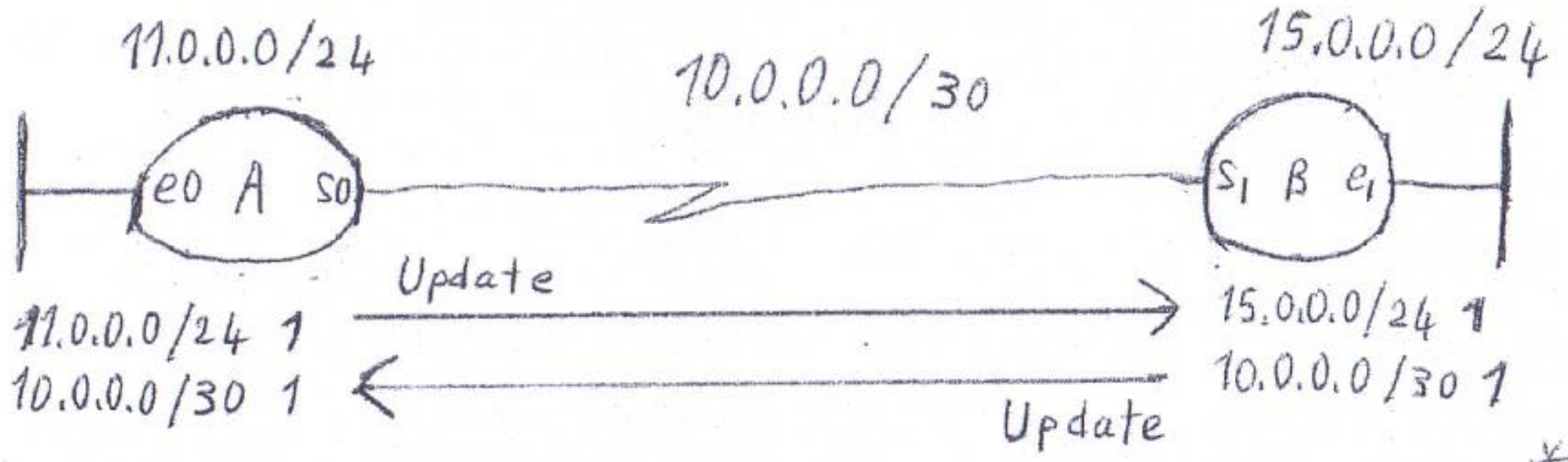
Maged Abd El-Wareth

@Convergence: Steady State

still send periodic update every 30 seconds to act as "Keep alive".

* Router will flush after 180 sec (3 min) = Hold down time = Invalid time

C	11.0.0.0	/24	e0	0
C	10.0.0.0	/30	S0	0
R	15.0.0.0	/24	S0	1

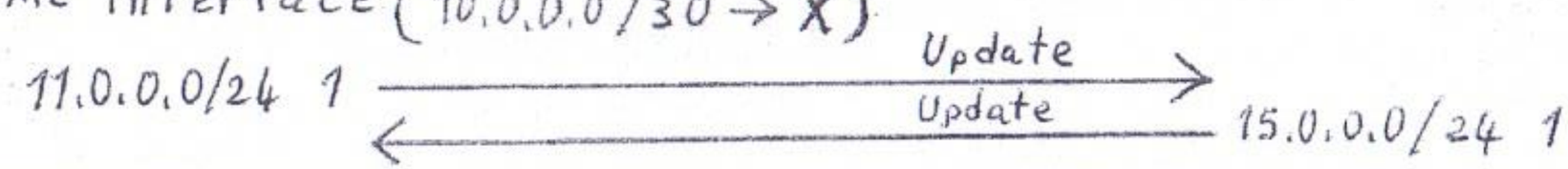


C	15.0.0.0	/24	e1	0
C	10.0.0.0	/30	S1	0
R	11.0.0.0	/24	S1	1

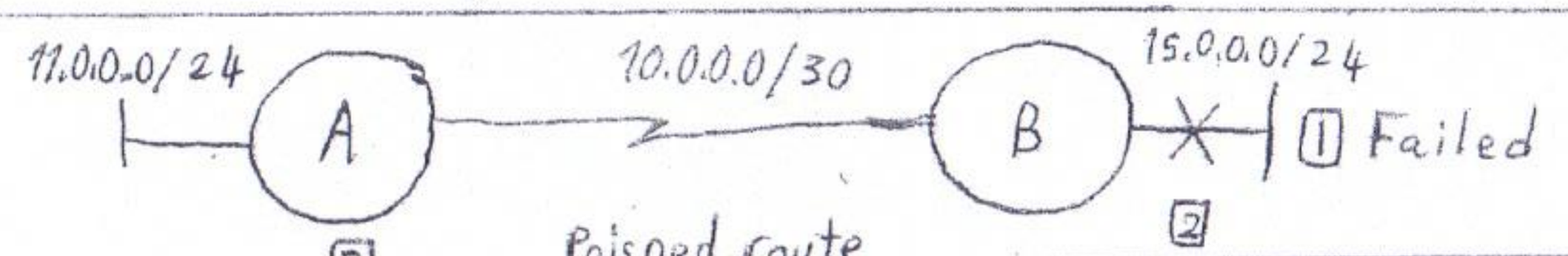
* Disadv.: Waste Resources
  - Bandwidth
  - Memory
  - CPU

Split Horizon: Route learnt from Interface should never by advertised back on same interface (10.0.0.0/30 → X)

Save Resources



@Change:



* sending update immediately @change

C	11.0.0.0	/24	e0	0
C	10.0.0.0	/30	S0	0
~~R~~	~~15.0.0.0~~	~~/24~~	~~S0~~	~~1~~

3 Poisned route

Triggered 15.0.0.0/24 - metric ∞

4 Poison reverse - as Ack

~~C~~	~~15.0.0.0~~	~~/24~~	~~e1~~	~~0~~
C	10.0.0.0	/30	S1	0
R	11.0.0.0	/24	S1	1

* In RIP ∞ = 16 routers
16 > 15

Routed Protocals :

It is the protocal that Carry user data traffic from end-to-end by supporting end-to-end header (encapsolation header) & logical address.

Routing Protocals :

It is the exchange of information between routers so as each router tell others about networks it can reach to building routing table.

Routing Classification :

Static Routing :

Build routing table manually, used if network is simple (If only single Path exists to destination).

Routing table

	Network	Mask	vector
C	11.0.0.0	/24	e_0
S	15.0.0.0	/24	S_0

Connected
Static

	Network	Mast	vector
C	15.0.0.0	/24	e_1
S	11.0.0.0	/24	S_1

→ (Config) ✱ ip route Network Mask vector or ip of the next hop.

ex: (Config) ✱ ip route 15.0.0.0 255.255.255.0 S_0

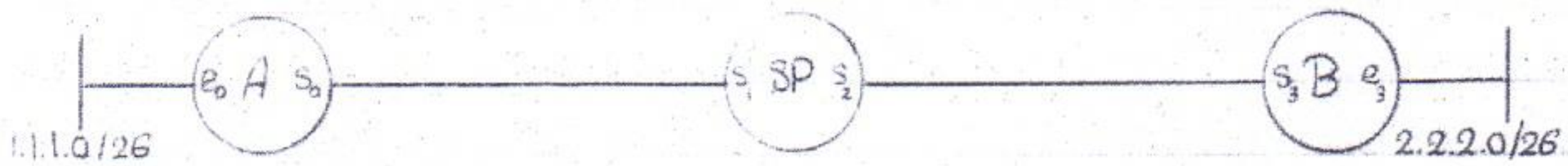
Dynamic Routing :

Build routing table automatic by software, used if network is Complex (many paths exist to destination).

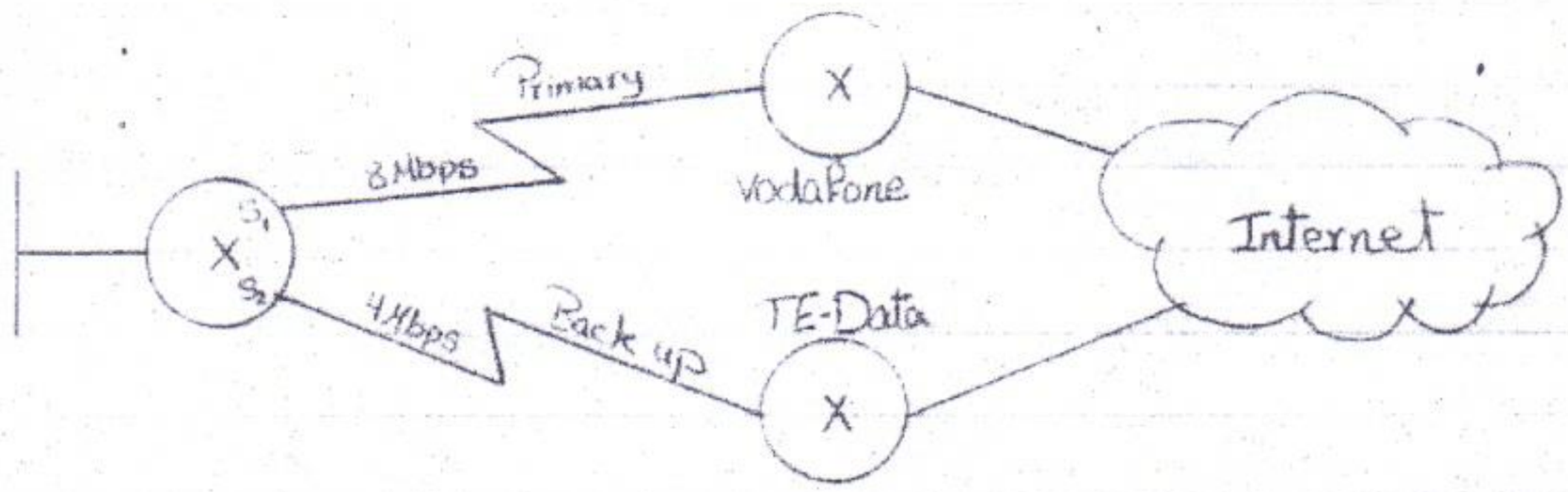
ex: IGP & EGP.

Static Routing:

we need network 1.1.1.0/26 to reach network 2.2.2.0/26 & vice versa ...



C	1.1.1.0	/26	e0	S	1.1.1.0	/26	S1	C	2.2.2.0	/26	e1
S	2.2.2.0	/26	S0	S	2.2.2.0	/26	S2	S	1.1.1.0	/26	S0



Network IP	Mask	vector	Distance (1-255)
0.0.0.0	0.0.0.0	S_2	10
0.0.0.0	0.0.0.0	S_1	

least distance is best ...

- If you didn't write distance, so two distances are the same, so it'll make load sharing (load balancing) ...

Default static Route:

... IP = Mask = 0.0.0.0 like home router ...

- For point-to-point network used mask "/30".

Dynamic Routing :

IGP

Interior Gateway Protocal

Used within Autonomous System

- Routing Information Protocal
  Version 1 & Version 2 ...
  RIPv1 RIPv2
- Interior Gateway Routing Protocal ...
  IGRP
- Enhanced Interior Gateway Routing Protocal ... EIGRP
- Intermediate system to Intermediate System ... ISIS
- Open Shortest Path First ... OSPF

EGP

Exterior Gateway Protocal

Used between Autonomous System

- Exterior Gateway Protocal ...
  EGP
- Border Gateway Protocal ...
  BGP

Link state

ISIS , OSPF

Advanced distance vector

RIPv2 , EIGRP

Distance vector

RIPv1 , IGRP

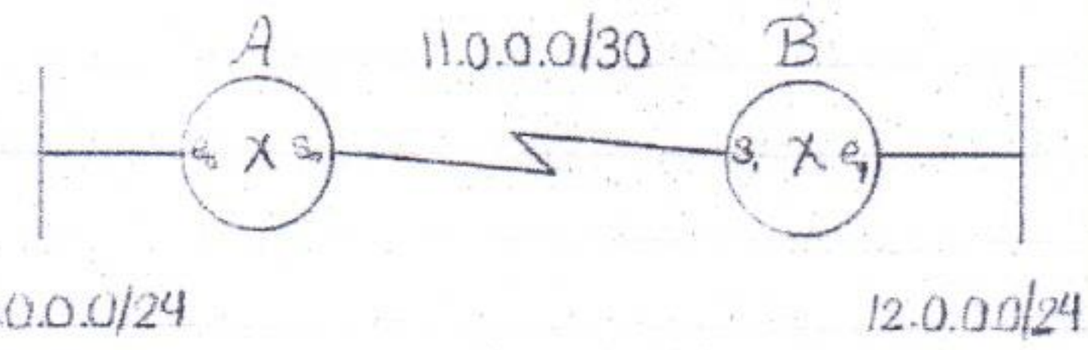
Routing Information Protocol version 2 RIPv2 :

@ **Start up :**

Just after Configuration, send periodic update every 30 second ...

@ **Convergence :**

Steady state after table is full. still send periodic update every 30 sec. Invalid time (hold time) is 3 min (6 update) ...



Disadvantage :

- used a lot of resources (Memory, bandwidth, Processing).

C 10.0.0.0 /24 e_0	C 12.0.0.0 /24 e_1
C 11.0.0.0 /30 S_0	C 11.0.0.0 /30 S_1

Advertisement (update) After 30 sec

C 10.0.0.0 /24 0 e_0	C 12.0.0.0 /24 0 e_1
C 11.0.0.0 /30 0 S_0	C 11.0.0.0 /30 0 S_1
R 12.0.0.0 /24 1 ,	R 10.0.0.0 /24 1 S_1
~~R 11.0.0.0 /30 1 S_0~~	~~R 11.0.0.0 /30 1 S_1~~

(Keep alive) After 30 sec

C 10.0.0.0 /24 0 e_0	C 12.0.0.0 /24 0 e_1
C 11.0.0.0 /30 0 S_0	C 11.0.0.0 /30 0 S_1
R 12.0.0.0 /24 1 S_0	R 10.0.0.0 /24 1 S_1
~~R 12.0.0.0 /24 1 S_0~~	~~R 10.0.0.0 /24 1 S_1~~
~~R 11.0.0.0 /30 1 S_0~~	~~R 11.0.0.0 /30 1 S_1~~
~~R 10.0.0.0 /24 2 S_0~~	~~R 12.0.0.0 /24 2 S_1~~

→ **Split horizon :**

Routes learnt from interface can't be advertised back on same interface. To save resources ...

→ **Triggered update :**

Sending update immediately @ Change ...

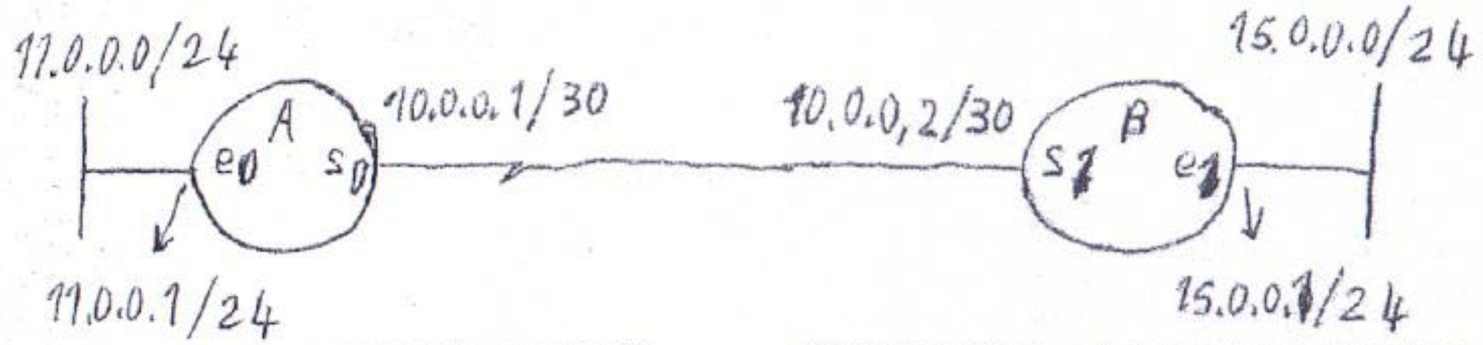
@ **Change :**

If route failed, send update that network has metric ∞ ($\infty = 16$) ...

⇒ we can use the distance option to make best & backup static route path

Static Routing:

Session 2 /1



	Network	Mask	Vector
C	11.0.0.0	/24	e0
S	15.0.0.0	/24	s0

	Network	Mask	Vector
C	15.0.0.0	/24	e1
S	11.0.0.0	/24	s1

A(config)# ip route 15.0.0.0 255.255.255.0 s0

vector (exit interface)

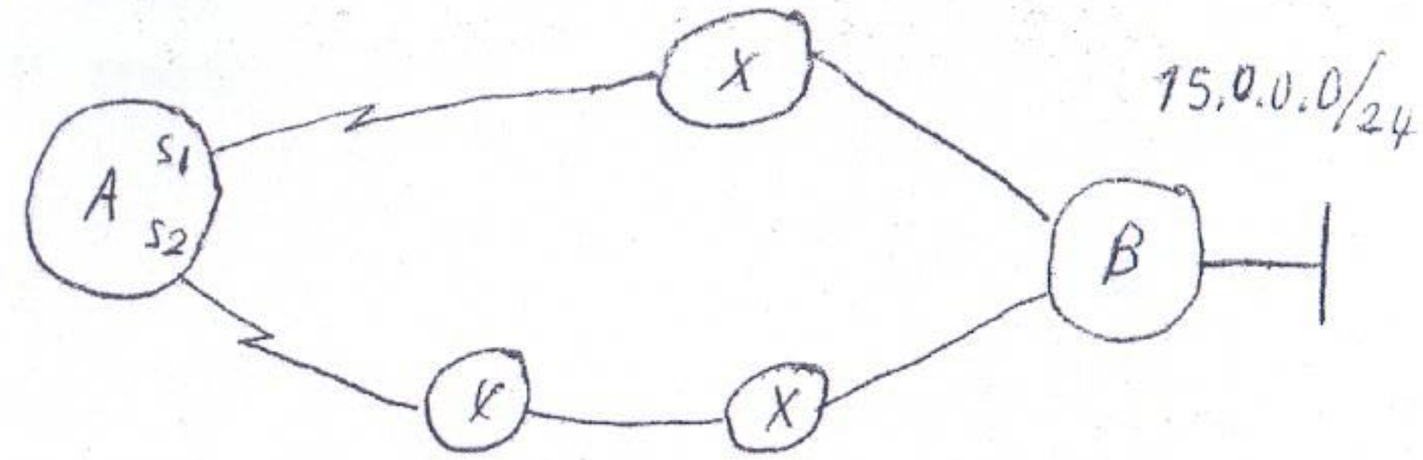
(OR)

A(config)# ip route 15.0.0.0 255.255.255.0 (10.0.0.2)

vector (IP of next hop - next router)

[Distance 1-255]

Ex: Redundancy (Primary / BacKup) = Active / Standby
= Floating Static (Backup Static)



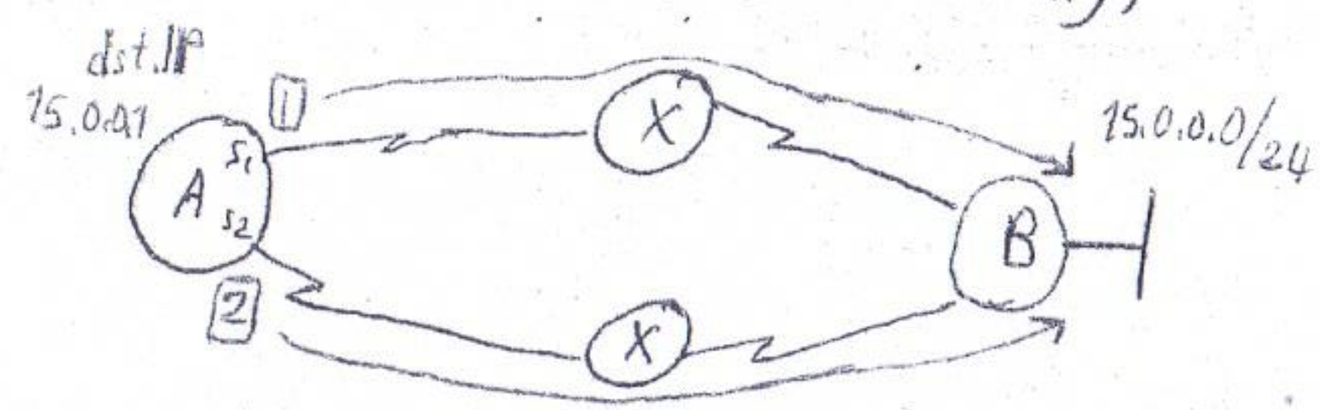
Best Path ← S 15.0.0.0 /24 s1 2

BacKup Path ← S 15.0.0.0 /24 s2 3

A(config)# ip route 15.0.0.0 255.255.255.0 s1 2

A(config)# ip route 15.0.0.0 255.255.255.0 s2 3

Load Balancy (Load Sharing)



S	15.0.0.0	/24	s1	2
S	15.0.0.0	/24	s2	2

A(config)# ip route 15.0.0.0 255.255.255.0 s1 2

A(config)# ip route 15.0.0.0 255.255.255.0 s2 2

Dynamic Routing: Advanced Distance Vector

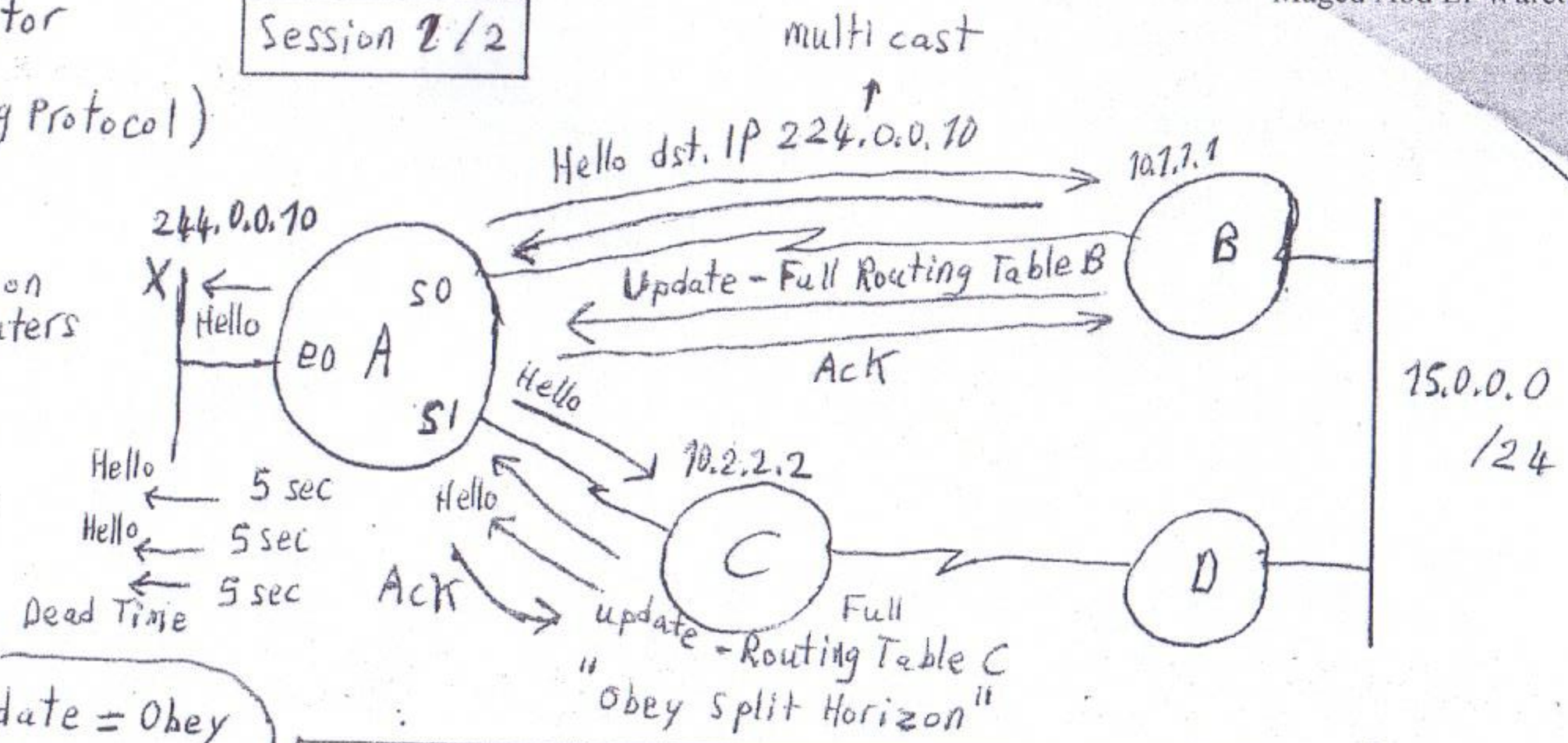
Session 2/2

* EIGRP (Enhanced Interior Gateway Routing Protocol)

@ startup: Just after configuration

(config) # router eigrp ____ → same on all routers

AS # 1-65,535



1 Neighbor Discovery: Exchange of "Hello" Handshaking

EIGRP Neighbor Table

IP of Neighbor	Interface
IP of B 10.1.1.1	S0
IP of C 10.2.2.2	S1

Update = Obey Split Horizon

show IP EIGRP neighbor (adjacent neighbor)

- Router A sends Hello to nearby routers.

@ Convergence: Steady State (no periodic update)

Periodic Hello
- every 5 sec, If link is fast, speed > T_1
- every 60 sec, If link is slow, speed ≤ T_1 (1.54 Mbps)

2 Routes Discovery: Exchange of updates "Routing Table"

Routing Table A

C	e0	
C	S0	
C	S1	
D 15.0.0.0/24	S0	1

DUAL Algorithm

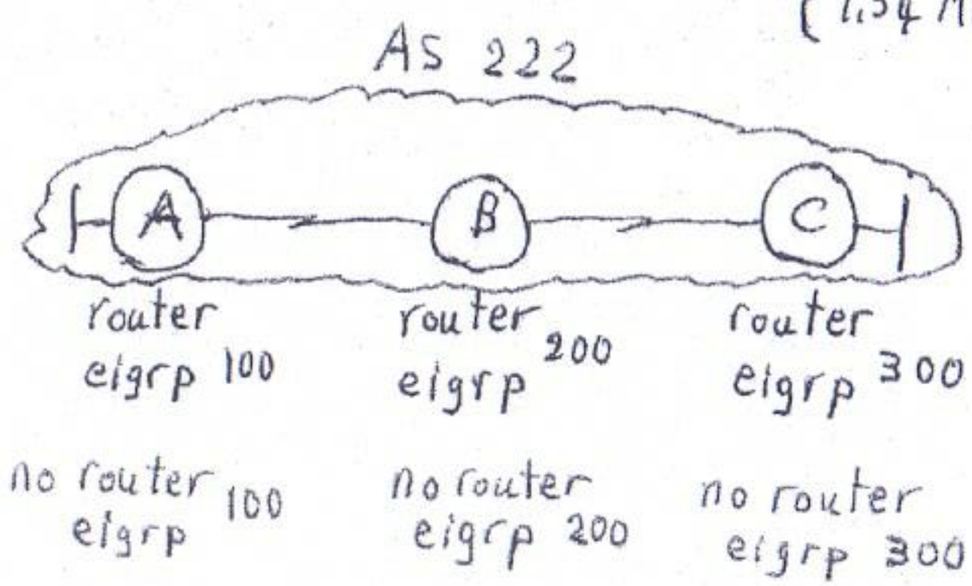
Copy of Successor

EIGRP Topology Table (All learnt routes)

Routing Table A
Routing Table B 15.0.0.0/24 metric 1
Routing Table C 15.0.0.0/24 metric 2

Routing Table B → Successor (Best Path)

Routing Table C → Feasible Successor (Backup Path)

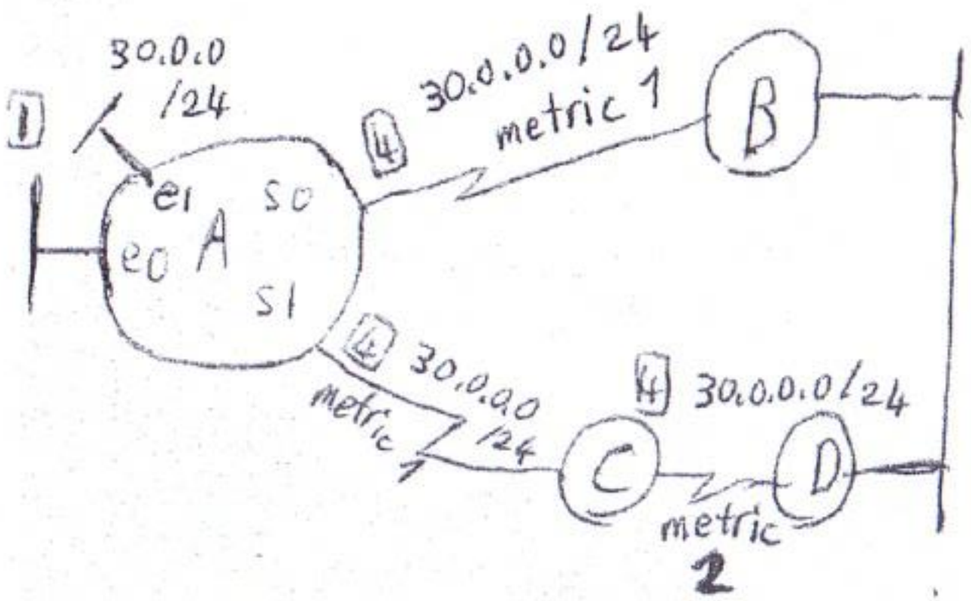


Session 2 /3

@ change: → New network appears
→ Old network disappears

FS: Feasible Successor

1 If new network appears:



Topology Table (A)

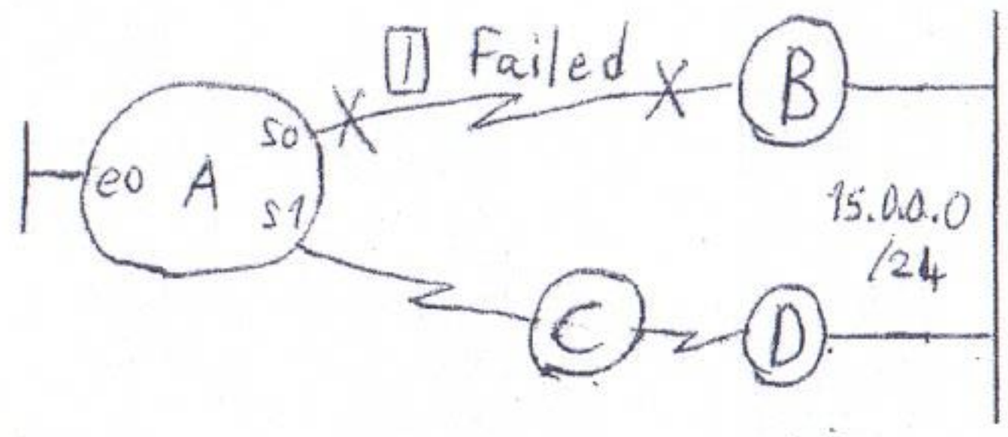
2	30.0.0.0 /24	e1	0

Routing Table (A)

3	30.0.0.0 /24	e1	0

4 Send partial (affected part) triggered update to neighbors.

2 If Successor fails & there is FS:



Topology Table (A)

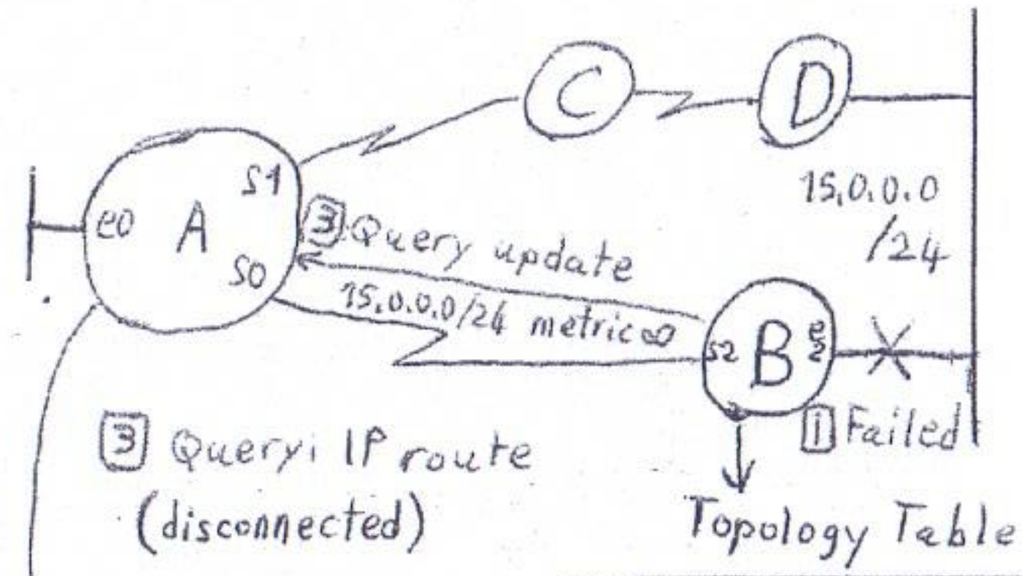
2	~~15.0.0.0/24~~	~~S0~~	~~1~~ → Successor
3	15.0.0.0/24	S1	2 → Feasible Successor

Routing Table (A) Copy

2	~~D 15.0.0.0/24~~	~~S0~~	~~1~~
3	D 15.0.0.0/24	S1	2

To be new Successor

3 If Successor fails & there is no FS:



3 Query: IP route (disconnected)

Topology Table

2	~~15.0.0.0/24~~	~~e2~~	~~0~~
7	15.0.0.0/24	S2	3

3 → A, C, D

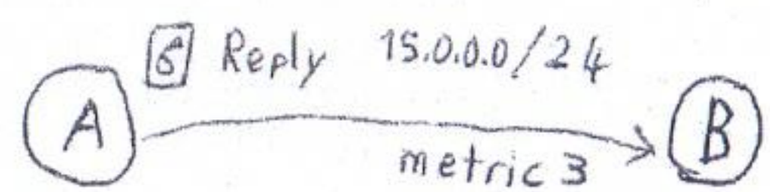
Topology Table

4	~~15.0.0.0/24~~	~~S0~~	~~1~~	Successor
	15.0.0.0/24	S1	2	FS

5 To be new successor

Routing Table

4	~~D 15.0.0.0/24~~	~~S0~~	~~1~~
5	D 15.0.0.0/24	S1	2



Enhanced Interior Gateway Routing Protocal EIGRP :

@ **start up :**

Just after Configuration .

1. **Neighbor discovery :**

exchange of hello " handshaking with directly Connected & understand same protocal" ...

Send hello to network 224.0.0.10 ⇒ Multicast class D ...

dead Time = 3 hello = 15 sec ...

Complete EIGRP neighbor table ...

2. **Routes discovery :**

exchange of updates "use DUAL Algorithm [Diffusion Update Algorithm]" to determine ~ Successor - Best Path ~ and ~ Feasible Successor - Backup Path ~ ...

Save all learnt routes in EIGRP Topology table then

Copy successor - Best Path to EIGRP Routing table ...

@ **Convergance :**

no periodic update, periodic hello to act as keep alive

~ High speed interface when speed > T_1 (1.54 Mbps) Send hello every 5 sec .. ~ .. low speed interface when speed ≤ T_1 Send hello every 60 sec ...

Dead Time (hold time) = 3 Hello ...

@ **Change :**

1. **If new network appears :** to every 20 router take 2 sec ...

- New network appears .
- Add to Topology table .
- DUAL check Best Path & Backup Path .
- Copy the best Path to routing table .
- Send partial (effected part or new part only) triggered update to neighbors.

2. <u>If network failed and there is feasible successor :</u> 10 μsec ≈ 0 sec
no packet loss.

- Network failed.
- Remove it from Topology & Routing table.
- Copy Backup path from topology table to Routing table.
- Send triggered partial update to neighbors.

3. <u>If network failed and there is no feasible successor:</u> 100msec
every 1 minute

- Network failed.
- Remove it from Topology & Routing table.
- Send Query update on 224.0.0.10 with metric ∞.
- Another routers will remove it from routing table.
- If another router has backup path to this network on Topology table, will Copy it to its routing table.
- Reply to the 1st router by new path (as a triggered update).

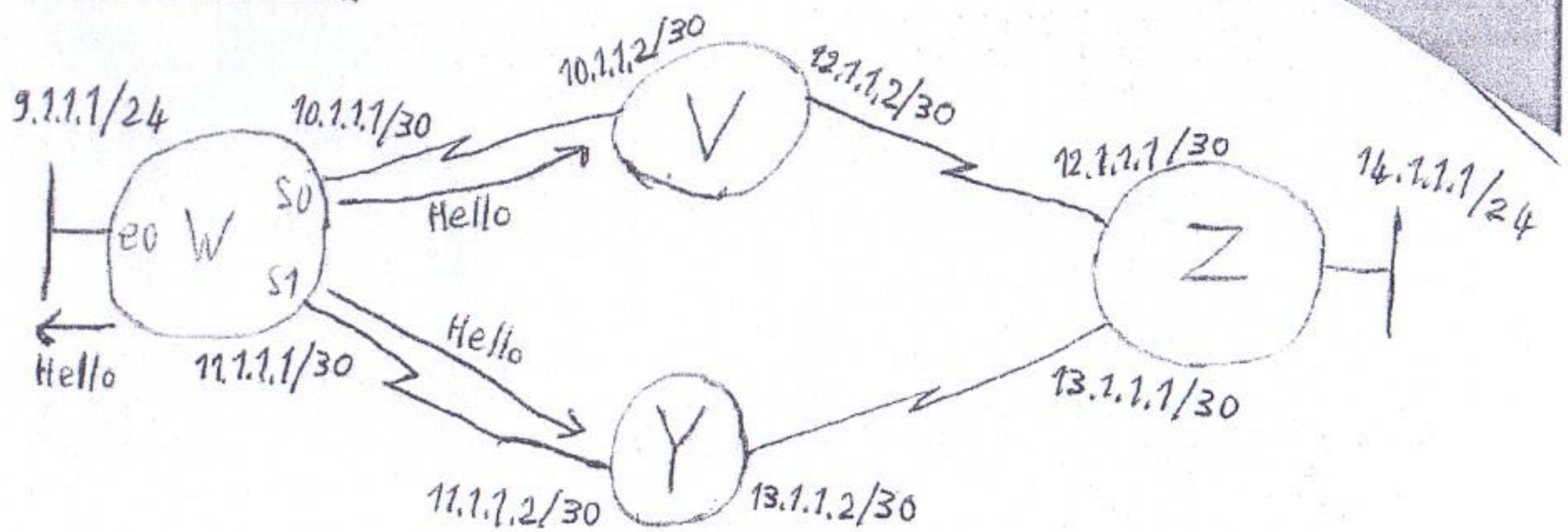
Session 3/1

Link State: < ISIS / OSPF

@Startup: Just after configuration

(config) # router OSPF 1-65,535
Process ID

Process ID < should never be zero / may not match between routers.



[1] Neighbor Discovery: Exchange of "Hello" Handshaking

OSPF Neighbor Table

IP of Neighbor	Interface
IP of V 10.1.1.2	S0
IP of Y 11.1.1.2	S1

show IP OSPF neighbor
Adjacent Neighbors

[2] Routes Discovery: Exchange of "Updates"
LSA: Link State Advertisement

Link	State	Advertisement
9.1.1.1/24	10 Mb	Router ID W
10.1.1.1/30	64 Kb	
11.1.1.1/30	64 Kb	

* Each router will form a packet describing itself and send it to neighbors.

LSDB: Link State Data Base (all LSAs) - W

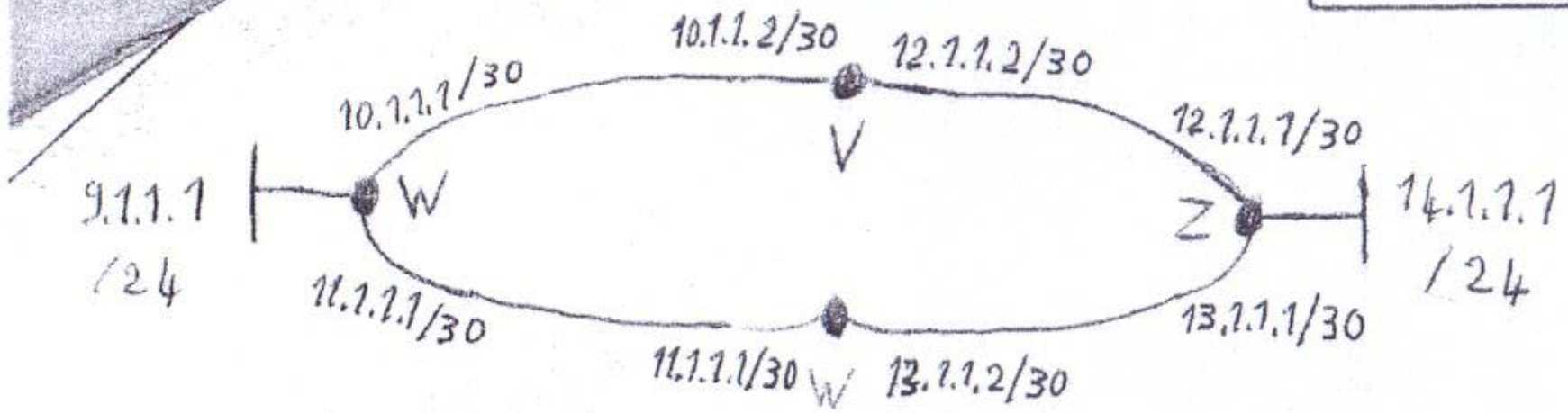
W	9.1.1.1/24	10 Mb
	10.1.1.1/30	64 Kb
	11.1.1.1/30	64 Kb
V	10.1.1.2/30	64 Kb
	12.1.1.2/30	64 Kb
Y	11.1.1.2/30	64 Kb
	13.1.1.2/30	64 Kb
Z	12.1.1.1/30	64 Kb
	13.1.1.1/30	64 Kb
	14.1.1.1/24	10 Mb

show IP OSPF data base

* Each router that receives LSA will take a copy of it in its LSDB and sends LSA as it is to all other neighbors.

Session 3/2

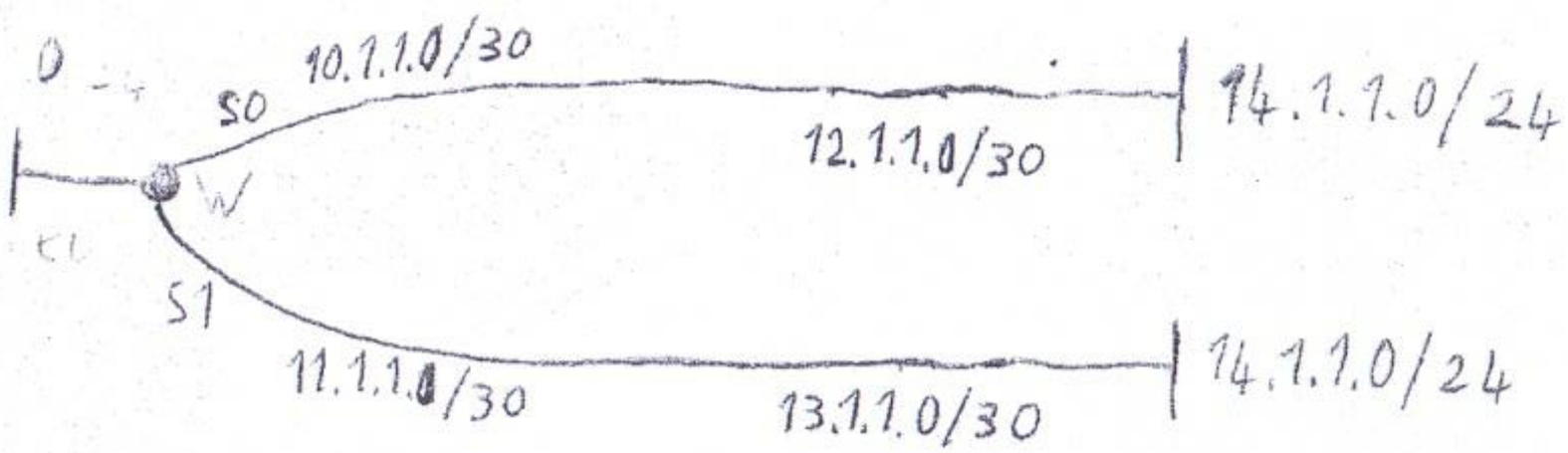
LSDB Tree



⇓

SPF

Dijkstra Algorithm (Shortest Path First)



⇒ SPF Tree

Routing Table: W

9.1.1.0/24	e0	0
10.1.1.0/30	S0	0
11.1.1.0/30	S1	0
12.1.1.0/30	S0	1
13.1.1.0/30	S1	1
14.1.1.0/24	S0, S1	2

Open Shortest Path First OSPF :

@ **Start up :**

Just after Configuration.

1. **Neighbor discovery :**

exchange of hello "handshaking with directly connected" ...

dead time is 4 hello ...

Send hello to Network 224.0.0.5 ⇒ MultiCast class D

Complete OSPF neighbor table ...

2. **Routing discovery :**

exchange of updates "link state Advertisement - LSA" ...

each router will form a packet describing itself called LSA ...

Send LSA to neighbors ...

each neighbor that receives LSA will take a copy of it in its LSDB (link State Data Base) & send another copy as it is to all other neighbors ...

Use Dijkstra Algorithm to determine Shortest Path First (SPF) by drow LSDB ...

Dynamic Routing Protocols

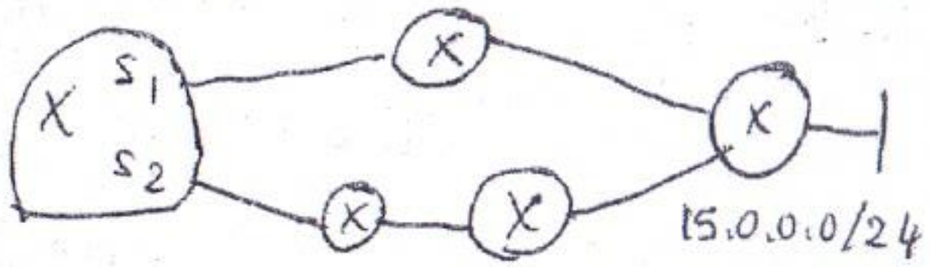
	Routing Information Protocol version 2 - RIPv2	Enhanced Interior Gateway Routing Protocol - EIGRP	Open Shortest Path First - OSPF	Boarder Gateway Protocol - BGP
1	Advanced Distance Vector Protocol	Advanced Distance Vector Protocol - CISCO	Link State Standard Protocol	Boarder Gateway Protocol
2	It sends periodic updates every 30 second from all interfaces	It sends full routing table @ startup	It sends LSA @ startup	It sends full routing table @ startup
	Uses Multicast Address 244.0.0.9	Uses Multicast Address 244.0.0.10	Uses Multicast Address 244.0.0.5 - 244.0.0.6	Using Unicast Address
3	Use Split Horizon & Triggered update @ change	Use Split Horizon & Triggered partial update @ change	Use Split Horizon & Triggered LSA update @ change	Use Split Horizon & Batched Updates every 30 second
4	It's classless routing protocol	It's classless routing protocol (Send mask in updates)	It's classless routing protocol	It's classless routing protocol
5	Support Authentication Password - Optional	Support Authentication Password - Optional	Support Authentication Password - Optional	Support Authentication Password - Optional
6	Uses Bellman Ford Algorithm to calculate best path	Uses DUAL Algorithm to calculate best & backup paths	Uses Dijkstra Algorithm to calculate best path	Uses BGP Algorithm to calculate best path
7	Symbol in routing table "R"	Symbol in routing table "D"	Symbol in routing table "O"	Symbol in routing table "B"
8	Administrative Distance: 120	Administrative Distance: 90	Administrative Distance: 110	Administrative Distance: 20 (WAN) -200 (LAN)
9	Metric is measured by hops - max. 15 - infinity 16	Metric is composite $M = 256 * [(10^7 / BW) + (10*Delay)]$	Metric is cost $M = 10^8 / BW$	Metric is composite of 10 attributes
10	Support equal load sharing - 4 by default - 16 by configuration	Support equal & unequal load sharing - 4 by default - 16 by configuration	Support equal load sharing only - 4 by default - 16 by configuration	No load sharing by default
11	Support Auto-Summary (by default)	Support Auto-Summary (by default)	Support Hierarchical design	Support Auto-Summary (by default) .

Session 1/2

RIP v2	EIGRP	OSPF	BGP
Advanced Distance Vector	Adv. Distance Vector - Cisco Protocol	Link State open < standard / source	Eterior Gateway protocol
Send periodic updates every 30 sec from all interfaces using Multicast → 224.0.0.9	@Startup: send full routing table on Multicast → 224.0.0.10 (no periodic update)	@Startup: send LSA using Multicast [224.0.0.5 / 224.0.0.6	@Startup: send full routing table using Unicast
Classless Protocol	Classless Protocol (send mask in updates)	Classless Protocol	Classless Protocol
@change: triggered update - use split horizon	@change: triggered partial update - use split horizon	@change: triggered LSA partial update - No split horizon	Triggered batched updates every 30 sec - use split horizon
Support Authentication Password option	Authentication Password - optional	Authentication Password - option	Authentication Password - optional
Bellman-Ford Algorithm calculate best path	DUAL Algorithm calculate best & backup paths	Dijkstra Algorithm calculate best path (SPF)	BGP Algorithm calculate best path
Symbol in Routing Table: R	Symbol in RT: D	Symbol in RT: O	Symbol in RT: B
Support Auto-Summary by default	Auto-Summary by default	Support Hierarchial Design	Auto-Summary by default
Support Equal Load Sharing 4 by default - 16 by Configure.	Equal & Unequal Load Sharing 4 by default - 16 by Configure.	Support Equal Load Sharing 4 by default - 16 by Configure.	NO Load Sharing

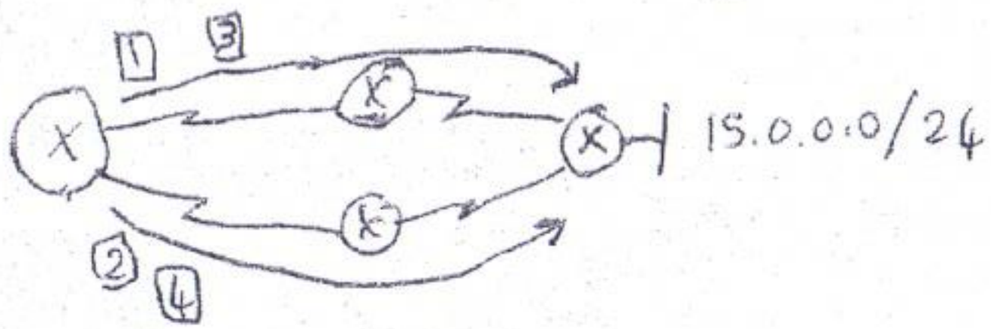
Session 4/2

* RIPv2 : Metric is Hop



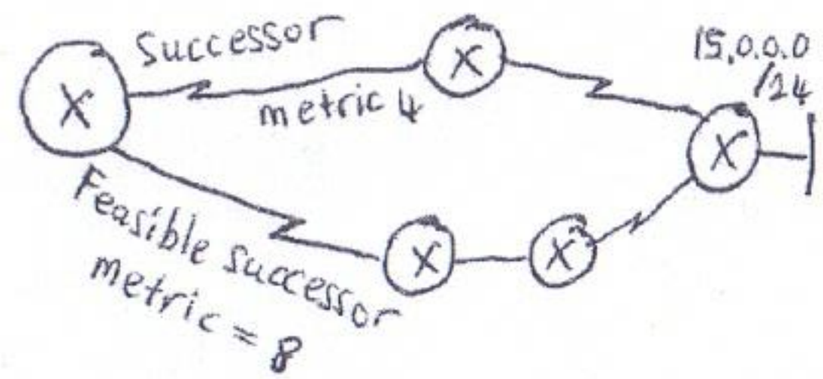
R	15.0.0.0/24	S1	2
R	15.0.0.0/24	S2	3

* RIPv2 : Support Equal Load Sharing = Load Balancing



(config)# maximum paths 1-16 (default: 4)

* EIGRP : Equal & Unequal Load Sharing



(config)# router eigrp 222

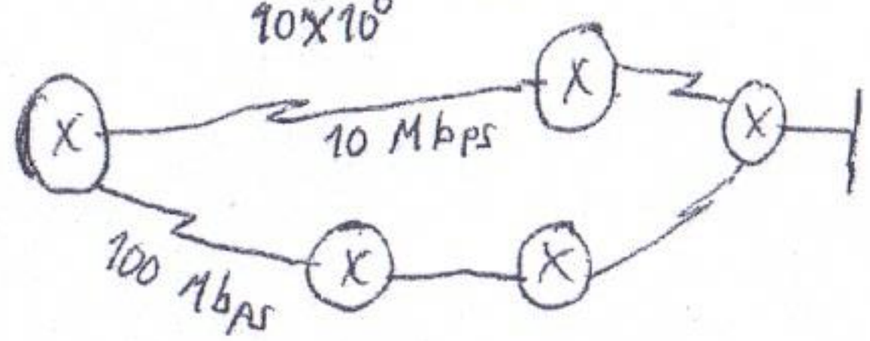
(config-router)# variance

↓

Unequal Load sharing

* OSPF : Metric is Cost

$$Cost = \frac{10^8}{10 \times 10^6} = 10$$

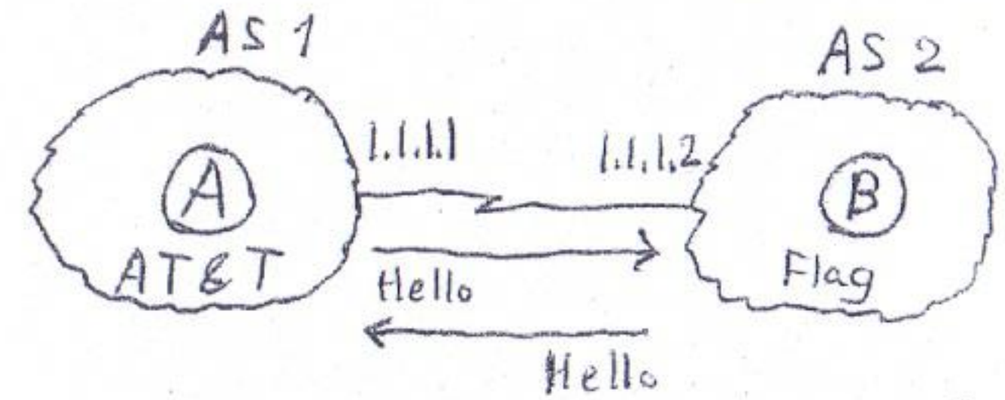


$$Cost = \frac{10^8}{100 \times 10^6} = 1$$

Cost 1 → ✓

Cost 10 → X

* BGP : send full routing table @startup to configure neighbors



A(config)# router BGP 1

A(config-router)# neighbor 1.1.1.2 remote-AS 2 ← AS of B

A(config-router)# neighbor 1.1.1.2 password Cisco

B(config)# router BGP 2

B(config-router)# neighbor 1.1.1.1 remote-AS 1

B(config-router)# neighbor 1.1.1.1 password Cisco

Maged Abd El-Wareth

ISIS : 115

Protocol	Administrative Distance
BGP	200 → Internal, 20 → External
RIP	120
OSPF	110
EIGRP	90 → Internal, 170 → External
Static	0, 1
Connected	0

Protocol	Metric	
BGP	10 Attributes	
RIP	Hop	
OSPF	Cost : $\frac{10^8}{BW}$	metric ↓ = BW ↑
EIGRP	Composite $256\left(\frac{10^7}{BW} + 10 \times delay\right)$	metric ↓ = BW ↑ + delay ↓

Best Path:

1. Least Administrative Distance

then

2. Least Metric

then

3. Load sharing (Load Balancing)

up to 4 paths by default

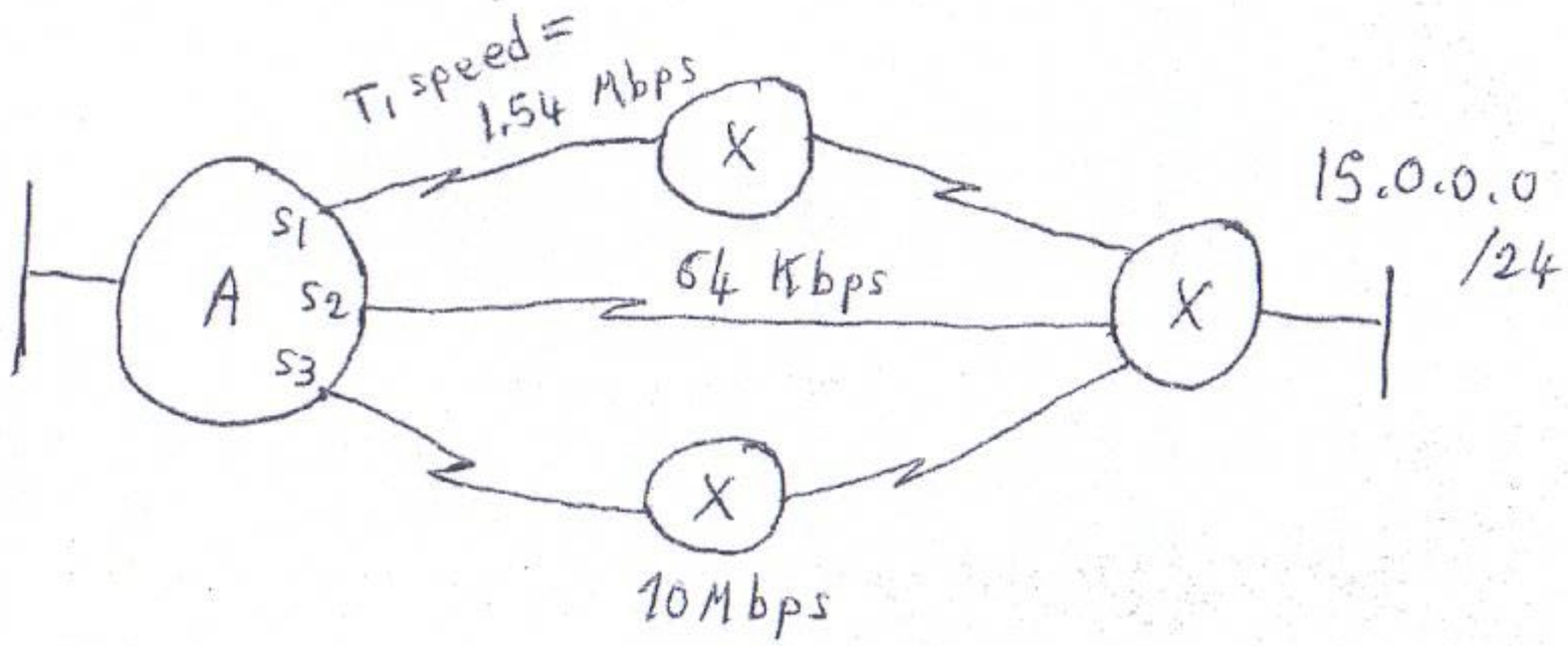
& max 16 paths by configuration

Maged Abd El-Wareth

Neglect Delay:

Scenario:

- Which path will router A choose to reach network 15.0.0.0/24?



A If RIP_{v2} is the routing protocol

$\Rightarrow S_2$ (metric is hop), admin. distance 120

B If OSPF is the routing protocol

$\Rightarrow S_3 \left(\text{metric is cost} = \frac{10^8}{BW} \right)$

C If EIGRP is the routing protocol

$\Rightarrow S_3 \left[\text{metric is composite} \quad 256 \left(\frac{10^7}{BW} + 10 \times \text{delay} \right) \right]$

D If RIP_{v2}, OSPF, EIGRP are running

$\Rightarrow S_3$ (EIGRP Path)

Scenario: Neglect Delay

- If RIPv2 is the routing protocal which interface will router A use to send data to network 20.0.0.0/24 ?

Metric = hop so S_2 with metric zero...

- If EIGRP is the routing protocal which interface will A use to go to 20.0.0.0/24 ?

$$\text{Metric} = 256\left[\frac{10^7}{BW} + (10 \times \text{Delay})\right]$$

$$S_1 = 256\left(\frac{10^7}{1.54 \times 10^3}\right) = 1662337.6623$$

$$S_2 = 256\left(\frac{10^7}{64}\right) = 4 \times 10^7$$

$$S_3 = 256\left(\frac{10^7}{10 \times 10^3}\right) = 256 \times 10^3 \quad \ldots \quad \text{Good}$$

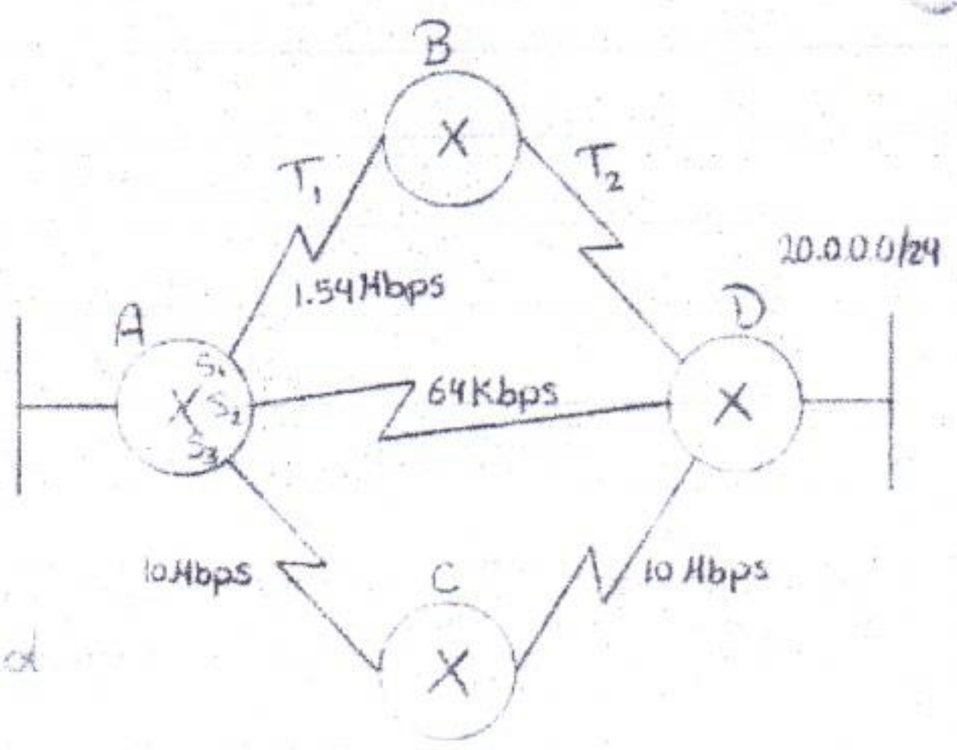
- If OSPF is the routing protocal which interface will router A use to send data to network 20.0.0.0/24 ?

$$\text{Metric} = \frac{10^8}{BW}$$

$$S_1 = \frac{10^8}{1.54 \times 10^3} = 64935.064935$$

$$S_2 = \frac{10^8}{64} = 1562500$$

$$S_3 = \frac{10^8}{10 \times 10^3} = 10^4 \quad \ldots \quad \text{good}$$

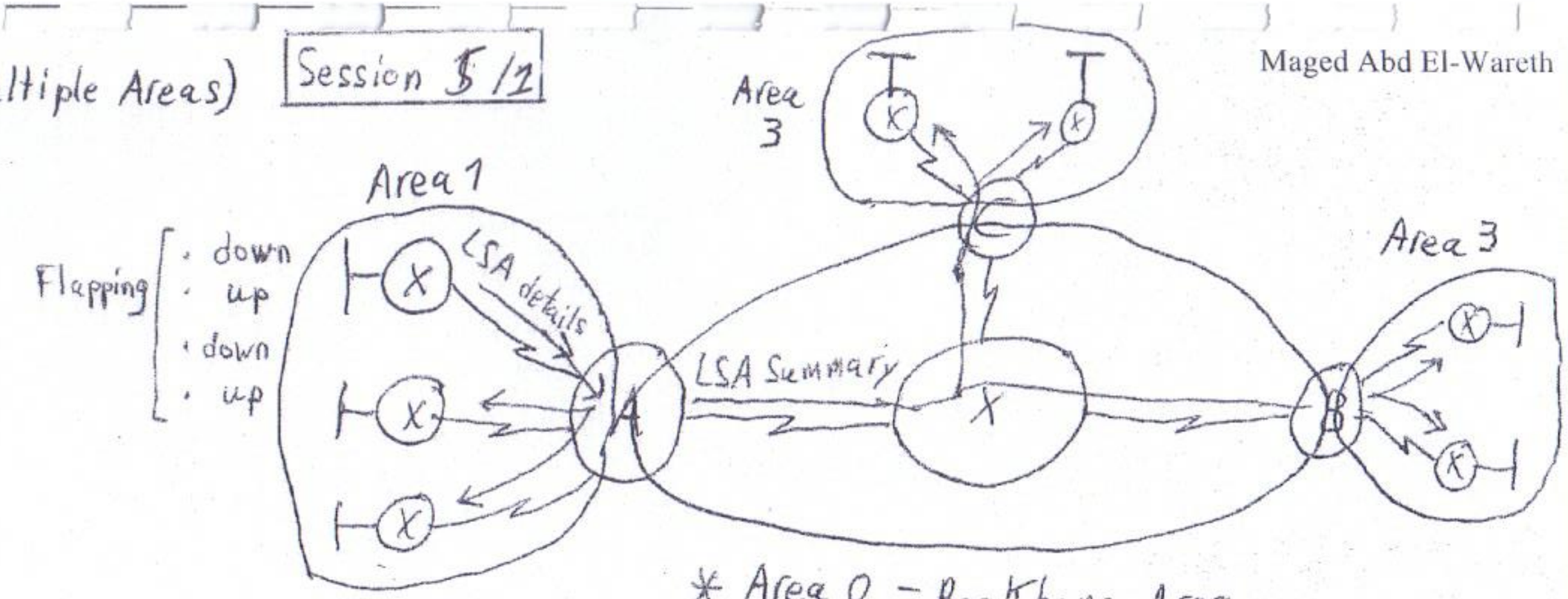


OSPF Hierarchial Design: (Multiple Areas) Session 5/2

OSPF Problem:

1. Need high CPU
2. Need big memory
3. Instability affect entire AS

* # routers >50, flapping will be higher (more ups & downs).

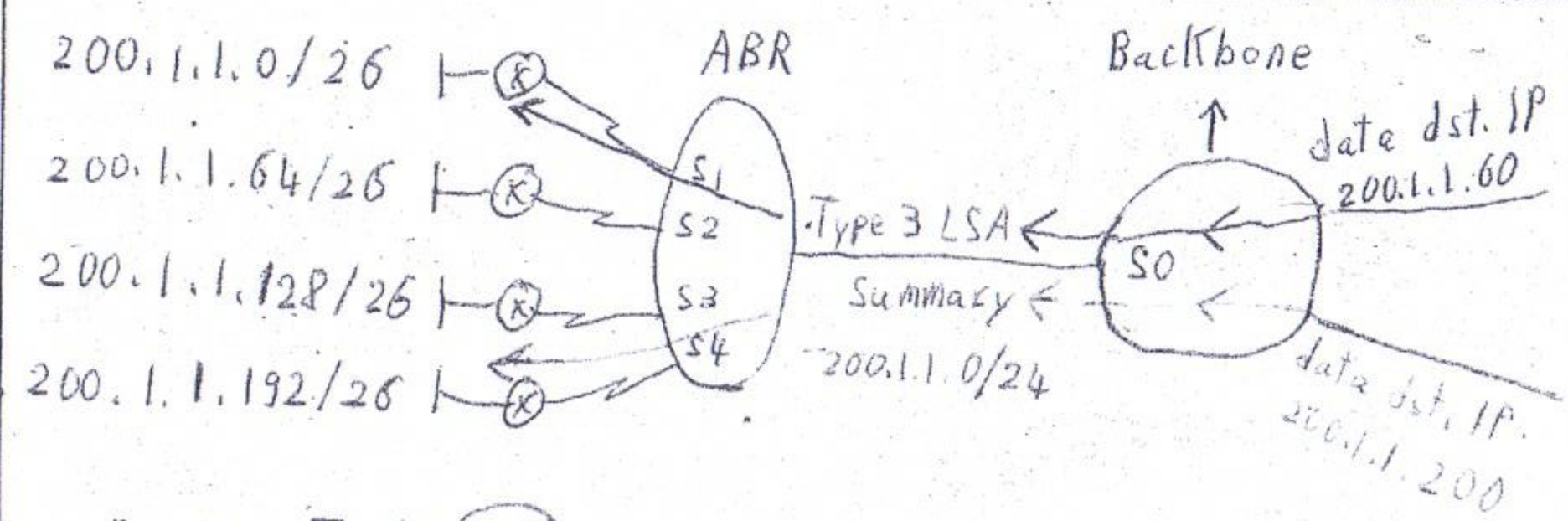


* Area 0 = Backbone Area
(ABR) * Routers A, B, C are Area Border Router

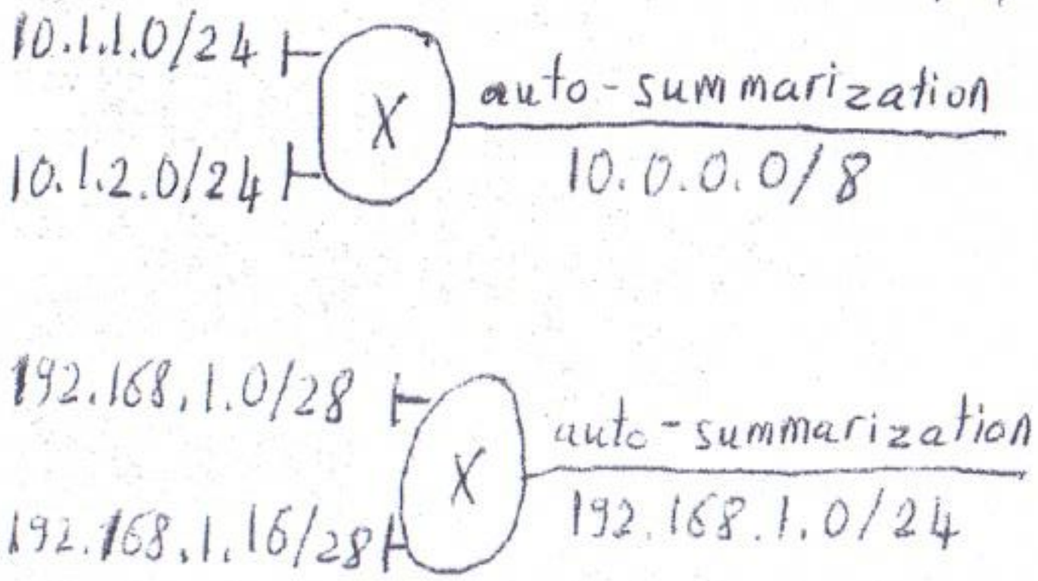
OSPF Solution: Auto Summarization

- Divide AS into sub AS called areas.

* Routers know details about their area (Type 1 LSA), summarize only about other areas (Type 3 LSA)



RIP$_{v2}$ / EIGRP / BGP: Auto Summarization Class A/8, B/16, C/24



Routing Table (ABR)

O 200.1.1.0/26	S1	0, 60, 63
O 200.1.1.64/26	S2	
O 200.1.1.128/26	S3	
O 200.1.1.192/26	S4	192, 200, 255

Backbone Routing Table

O 200.1.1.0/24	S0

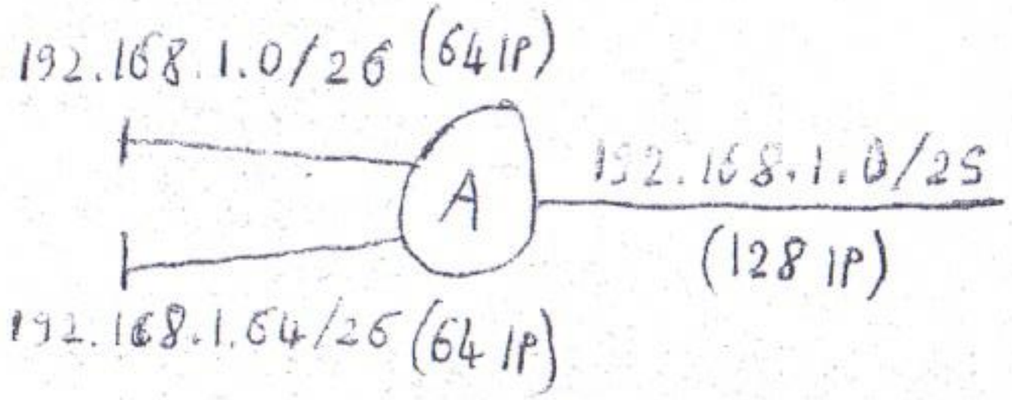
S0: 200.1.1.0, 200.1.1.60, 200.1.1.200, 200.1.1.255

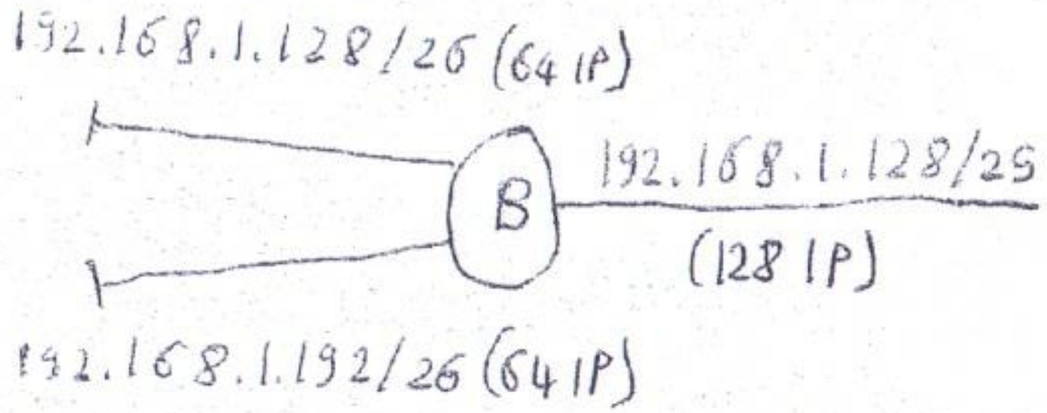
Session 8 : 2

Route Aggregation

Summarization

- It is grouping many subnets & advertise them as a bigger subnets (or) max as a major network.





192.168.1.128 = 192.168.1.1000 0000

192.168.1.192 = 192.168.1.1100 0000

192.168.1.1000 0000 / 25

192.168.1.128/25

Supernetting (CIDR)

[Classless Inter Domain Routing]

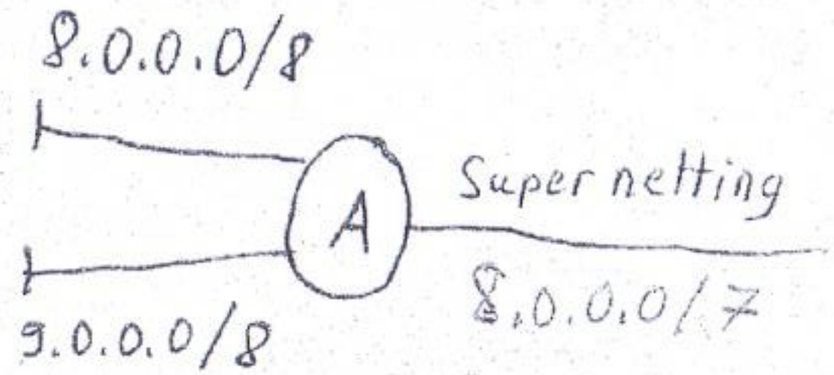
- It is grouping major networks & advertise them as one big super network.

8.0.0.0 = 0000 1000.0.0.0

9.0.0.0 = 0000 1001.0.0.0

0000 1000.0.0.0/7

8.0.0.0/7



4.0.0.0 = 0000 0100.0.0.0

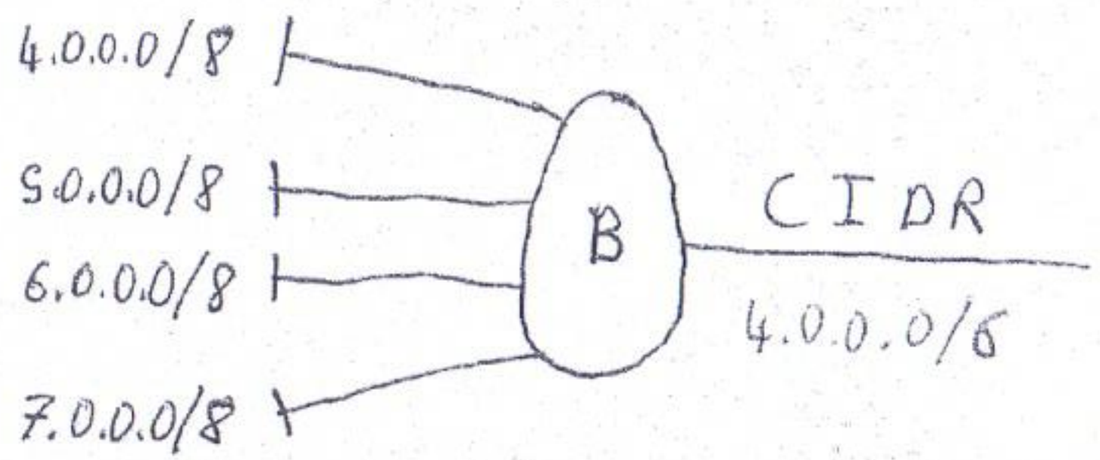
5.0.0.0

6.0.0.0

7.0.0.0 = 0000 0111.0.0.0

0000 0100.0.0.0/6

4.0.0.0/6



Maged Abd El-Wareth

OSPF Operation:

@Startup: Just after configuration

(config)# router OSPF Process ID
1 - 65,535

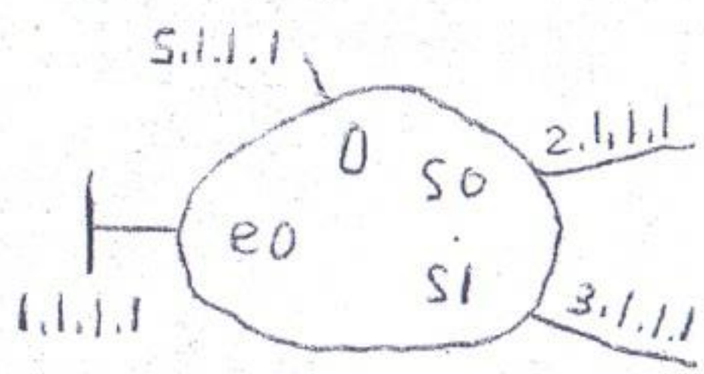
0 Create Router ID:

Manually

A It is the highest IP Address configured on loopback Interface

Internal, S/w virtual/logical, always up

(config)# router loopback 0
(config-If)# IP address 5.1.1.0 255.255.255.255
subnet mask



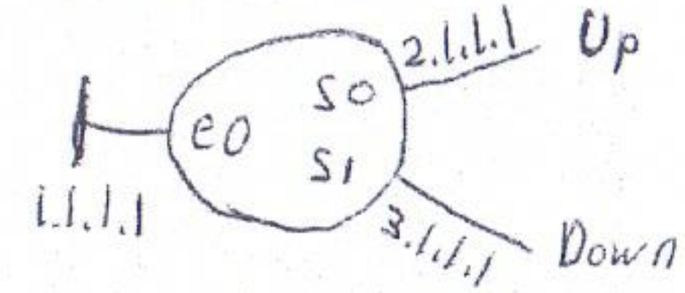
RID = 5.1.1.1

Automatically

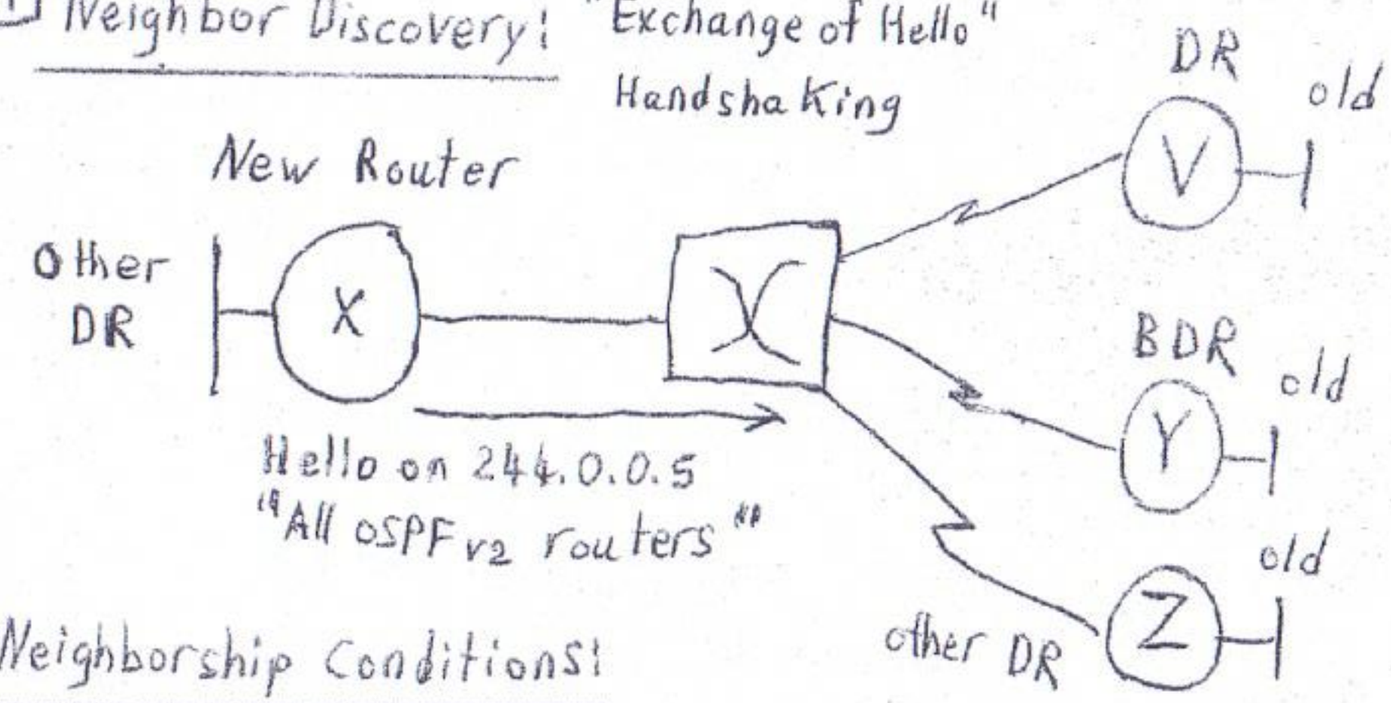
B It is the highest IP Address configured on physical active interface.

Ethernet, Serial, Up

(Router ID)
RID = 2.1.1.2



1 Neighbor Discovery: "Exchange of Hello" Handshaking



*Neighborship Conditions:

1. Same Authentication Password (option)
2. Same Area ID
3. Same hello interval (10 sec)
4. Same dead interval (40 sec)

← Hello

2 way state,
two way handshaking

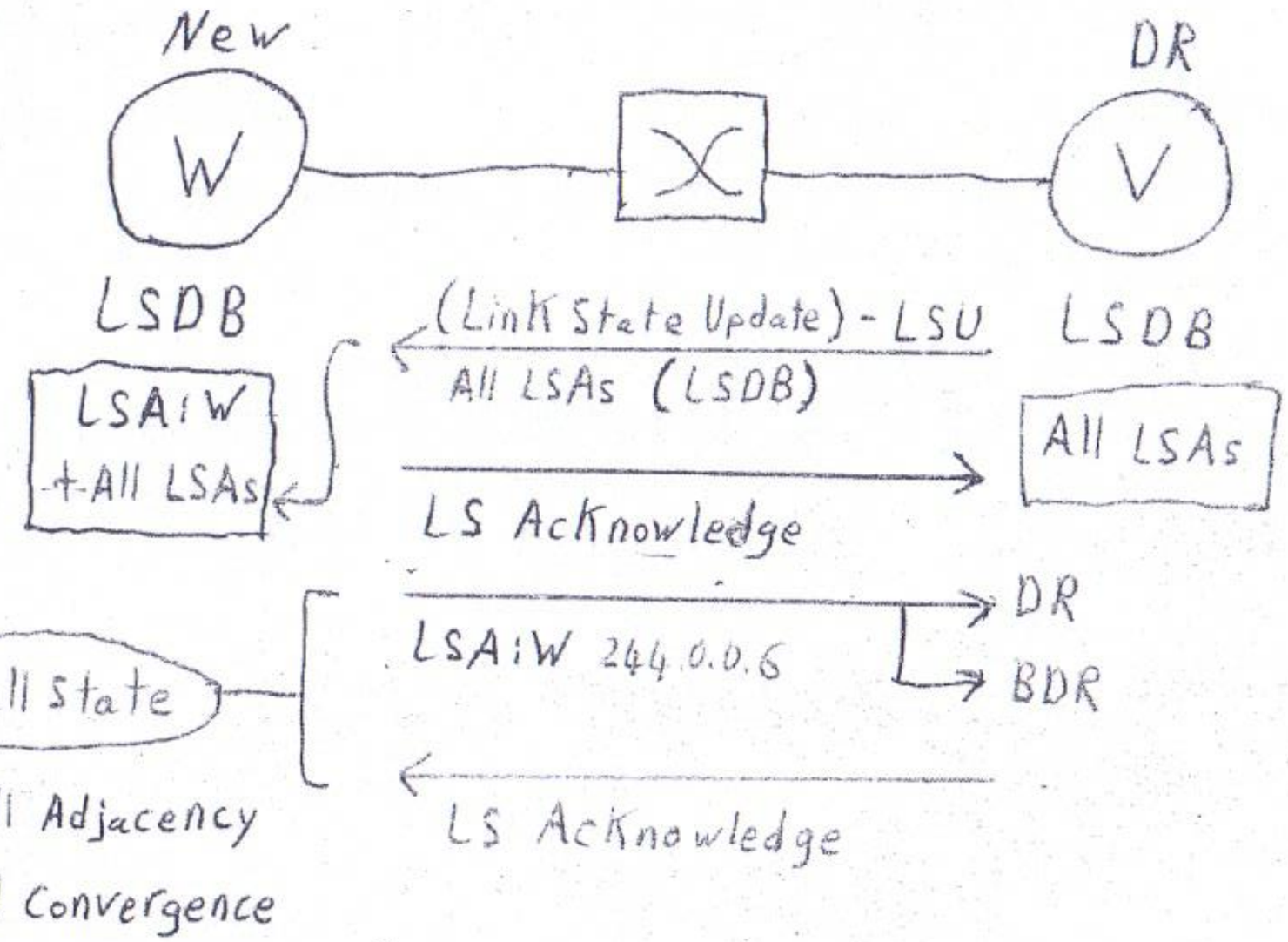
Session 5/4

2 Routes Discovery: "Exchange of Updates" ⇒ LSAs (LSDB)

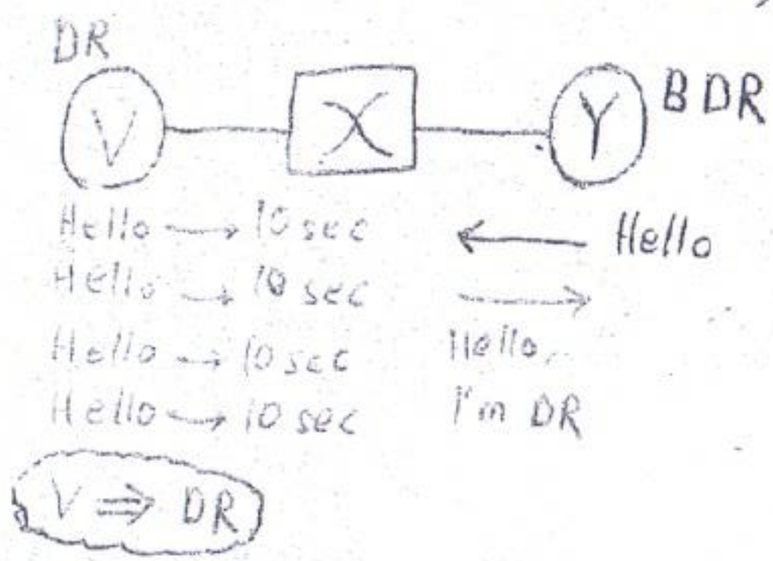
* Electing DR & BDR

Designated Router & Backup DR

DR → wellcome new comers



A First router to boost OSPF with enough time (40 sec) (DR)



B Router having highest priority (DR)

(config)# ip ospf priority 0–255

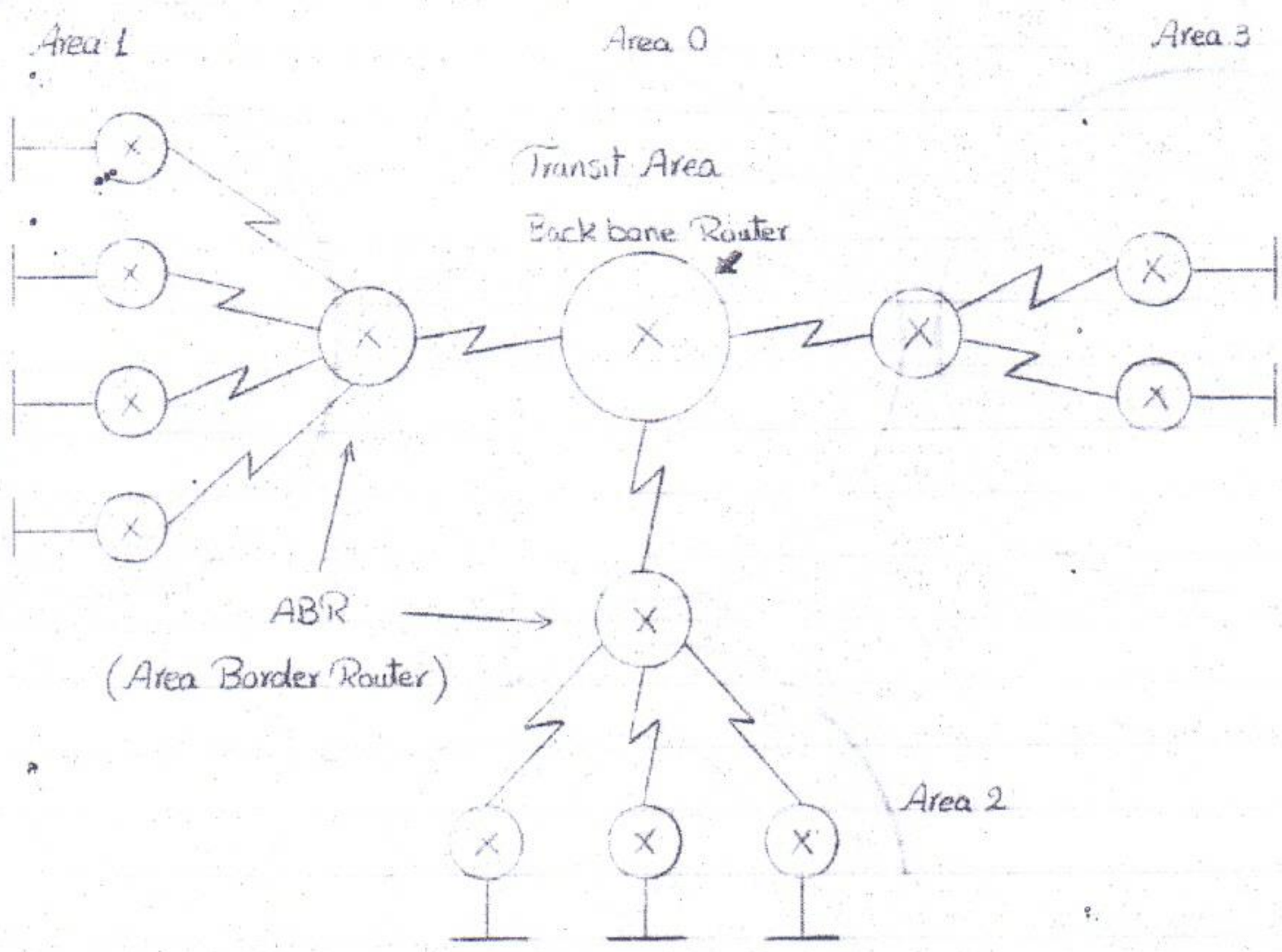
default = 1

C Router having highest RID (DR)

* 244.0.0.5 → Hello
* 244.0.0.6 → LSA < DR / BDR

Hierarchical design :

Multiple area OSPF, Dividing Autonomous System into Sub-autonomous System called Areas ... each area contain maximum 50 routers ...

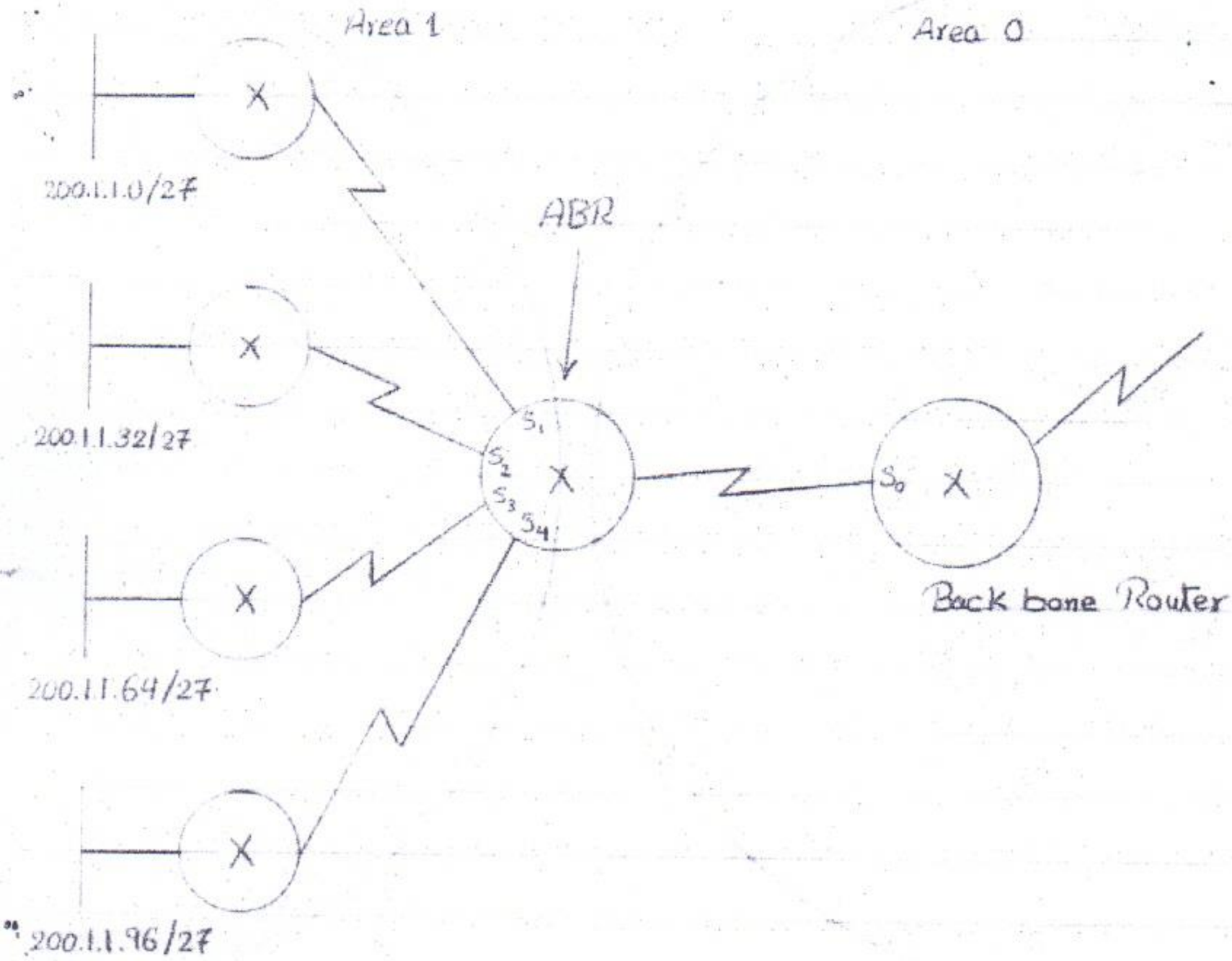


Disadvantages before Areas :

- Need big memory.
- Need big CPU.
- Instability affect the Autonomous System.

Advantage After Areas :

- Each router will know details about its area & summary only about other areas ... Type 1 LSA "O" Type 3 LSA "OIA"



O	200.1.1.0 /27	S_1
O	200.1.1.32 /27	S_2
O	200.1.1.64 /27	S_3
O	200.1.1.96 /27	S_4

ABR 'Routing table'

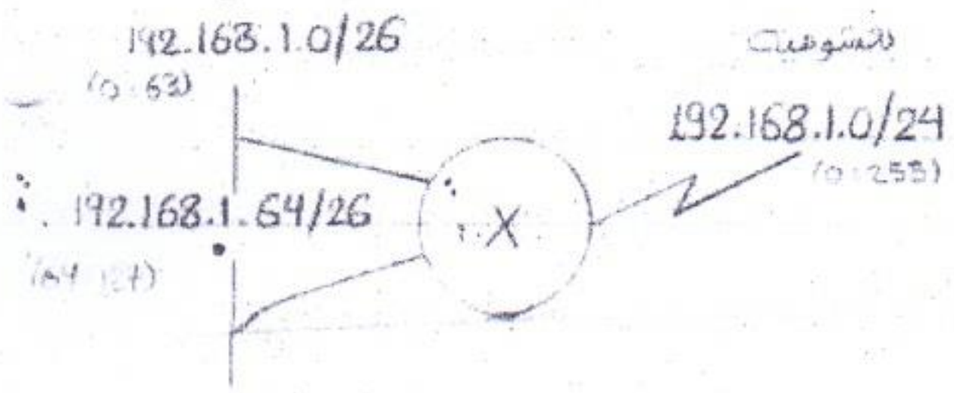
OIA	200.1.1.0/25	S_0
OSPF Inter Area		

Back bone Router 'Routing table'

Route Aggergation :

Summarization

Grouping many subnets & advertise them as a bigger subnet or max. a major network ...

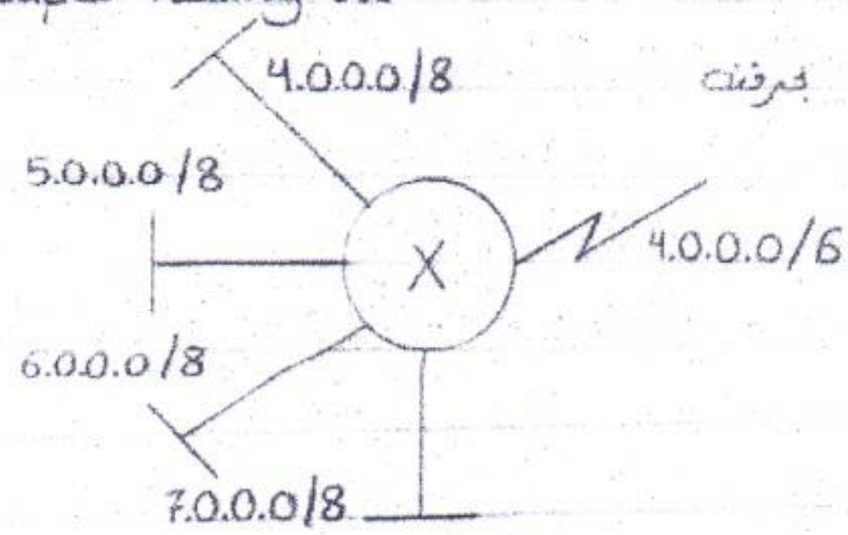


eigrp & ripv2 support auto-summary by default ...

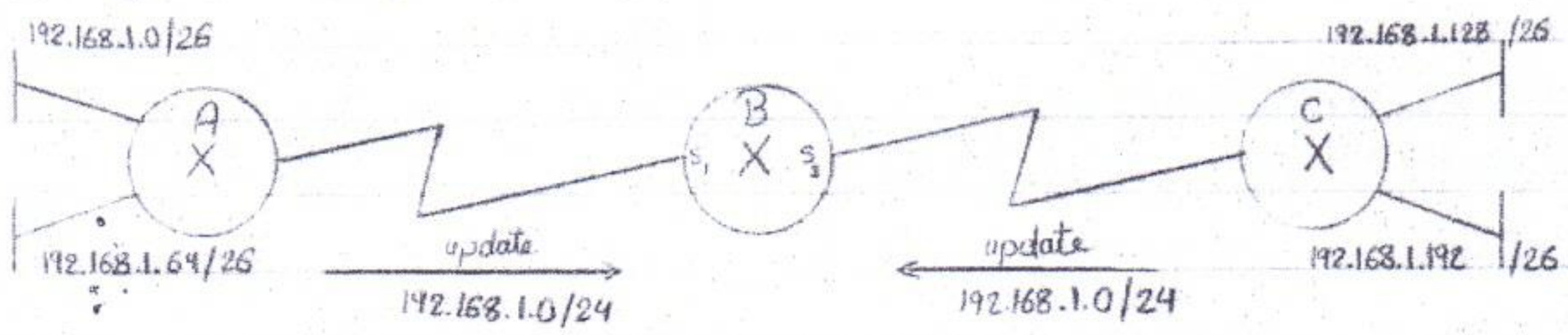
Classless Inter Domain Routing (CIDR)

Grouping many networks & advertise them as one big super network

Super netting ...



Disadvantage: Discontiguous network.



B Routing Table

D	192.168.1.0	/24	S_1
D	192.168.1.0	/24	S_2

To disable auto-summary in configuration "no auto-summary" ...

OSPF Operation:

@ start up:

Just after Configuration.

0. Create Router ID: 32-bit
   a. It is the highest IP address Configured on loopback interface.
   b. It is the highest IP address Configured on physical active interface.
      NIC WIC

1. Neighbor Discovery:

   Exchange of Hello = Handshaking.

   Neighborship Conditions:
   - Same authentication password.
   - Same area ID.
   - Hello interval = 10 sec.
   - Dead interval = 4 Hello = 40 sec.

2. For multiple access

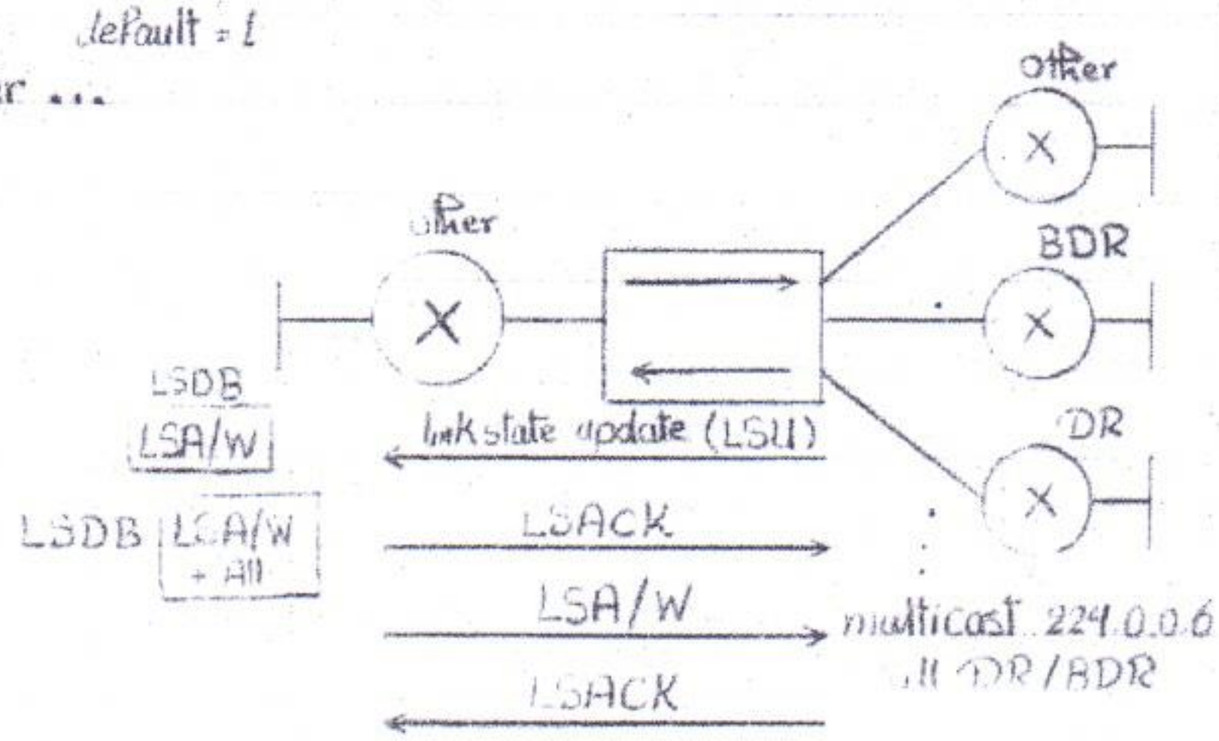
   Elect DR & BDR:

   Designated Router: welcome new comer
   a. Router that first boots OSPF with enough time 40 sec ...
   b. Router having highest priority on interface..
      0-255
      default = 1
   c. Highest RID.

   Backup Designated Router ...

3. Routes Discovery:

   Exchange of LSDB.



OSPF Configuration

Session 6 /1

@ Startup! Just after Configeration

(config)# router OSPF Process ID

(config-router)# network IP interface wild card mask area 0

↓

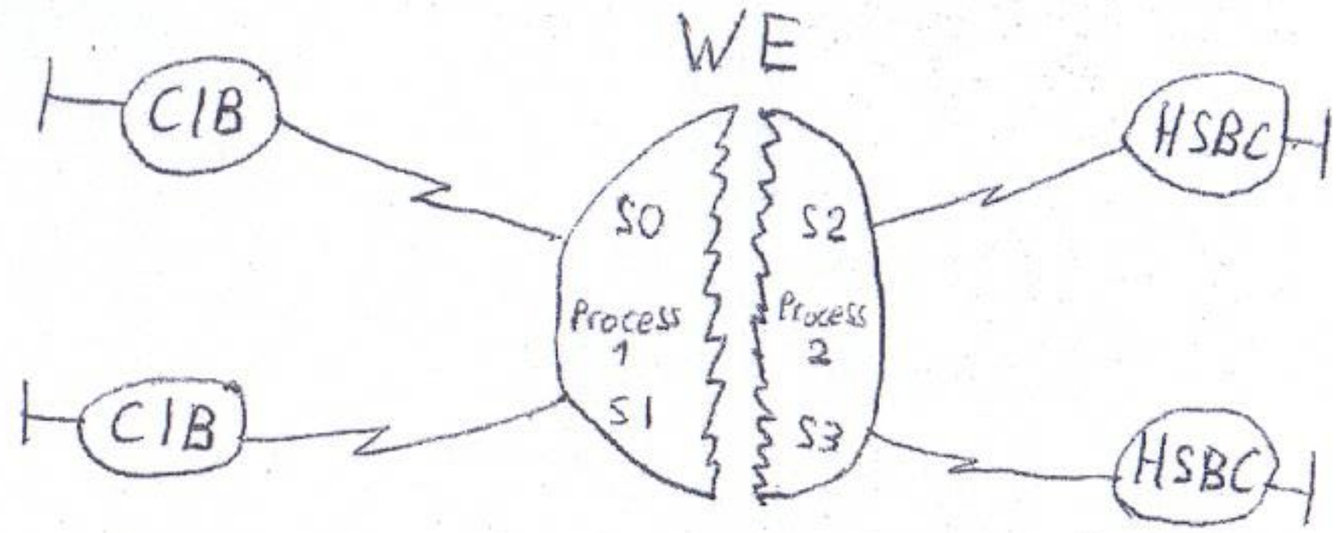
Inverted mask

0000 ------ 1111

exact match — doesn't care

Subnet mask : 00000 11111

Wild card mask : 11111 00000



Ex: Run OSPF Process 1 on S0 & S1

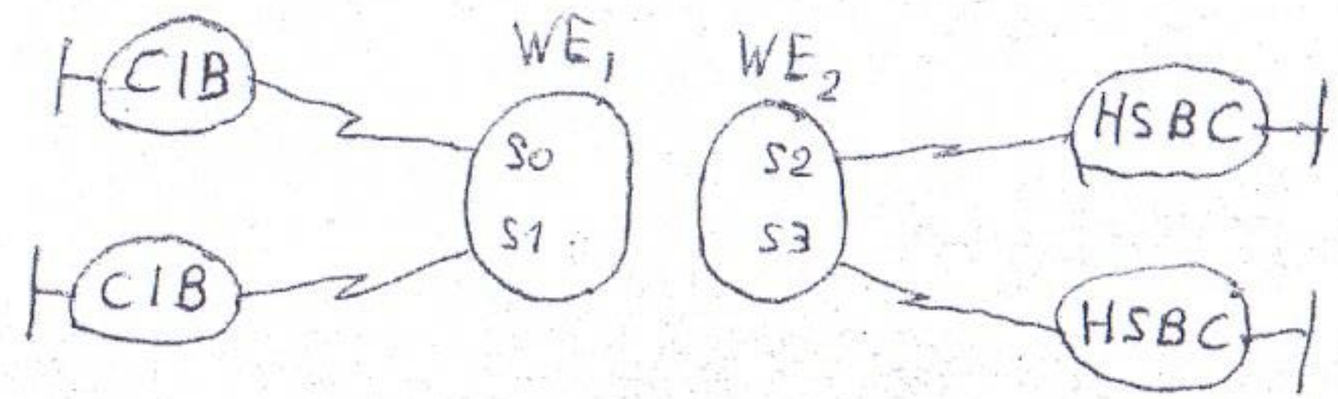
WE(config)# router OSPF 1

(config-router)# network 10.2.3.4 0.0.0.0 area 0 → S0

(config-router)# network 10.7.3.8 0.0.0.0 area 0 → S1

OR (config-router)# network 10.0.3.0 0.255.0.255 area 0

10.X.3.X



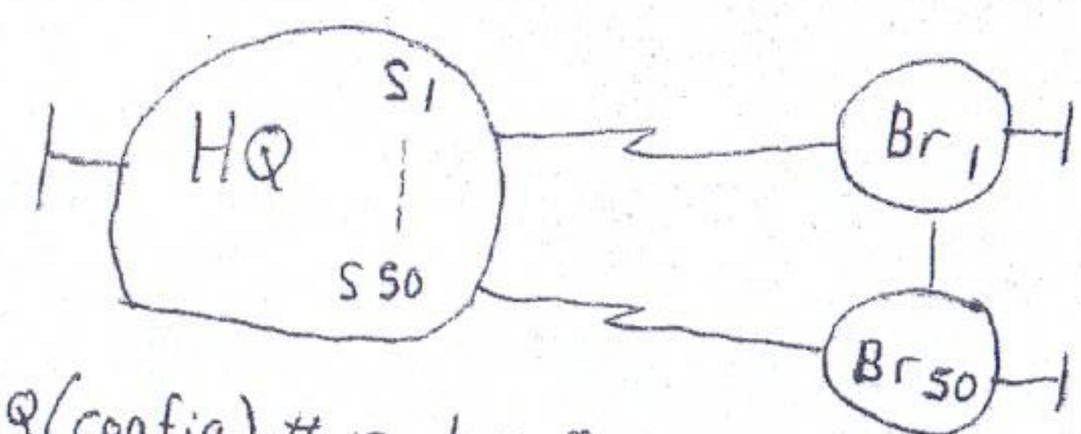
Ex: Run OSPF Process 2 on S2 & S3

(config)# router ospf 2

(config-router)# network 192.168.0.0 0.0.255.255 area 0

192.168.X.X

Ex: Run OSPF process on all interfaces



HQ(config)# router OSPF 1

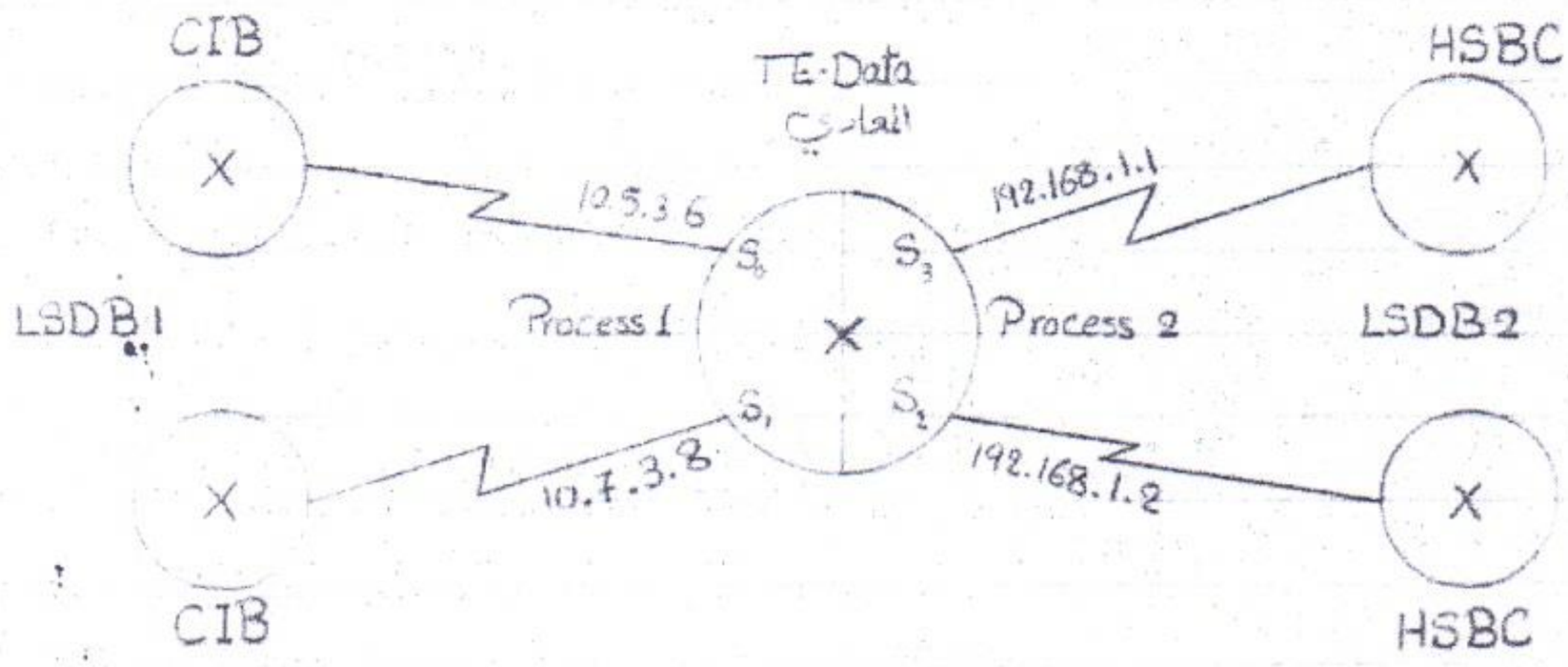
(config-router)# network 0.0.0.0 255.255.255.255 area 0 → Any Interface

OSPF Configuration:

(Config) ※ router ospf ※ 1:65535 Can never be zero, Process ID may be not match between routers

divide router in sub routers

(Config-router) ※ network IP wild card Mask Area 32-bit



(Config) ※ router ospf 1

(Config-router) ※ network 10.0.3.0 0.255.0.255 area 0.

(Config) ※ router ospf 2

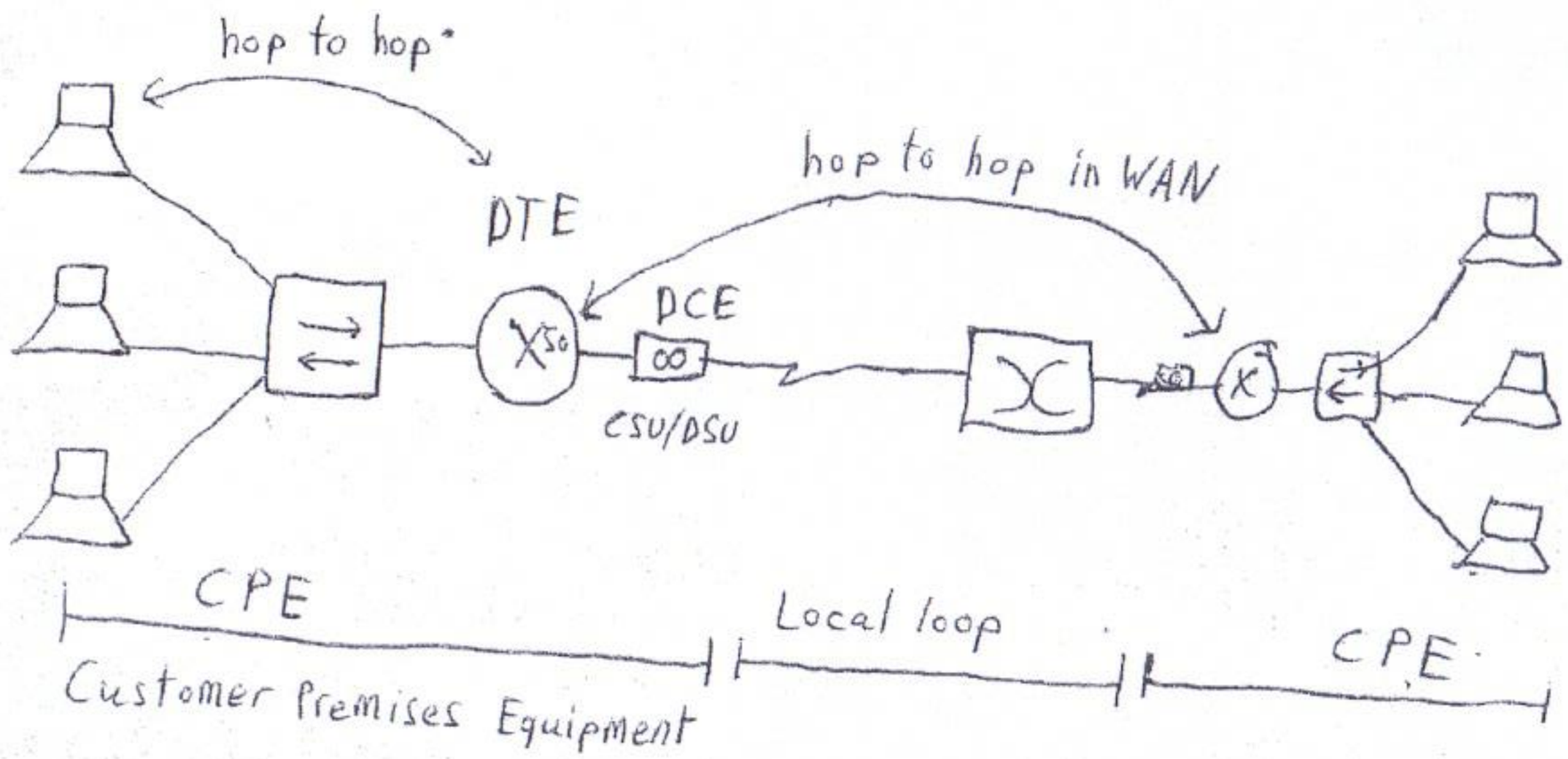
(Config-router) ※ network 192.168.1.0 0.0.0.255 area 0.

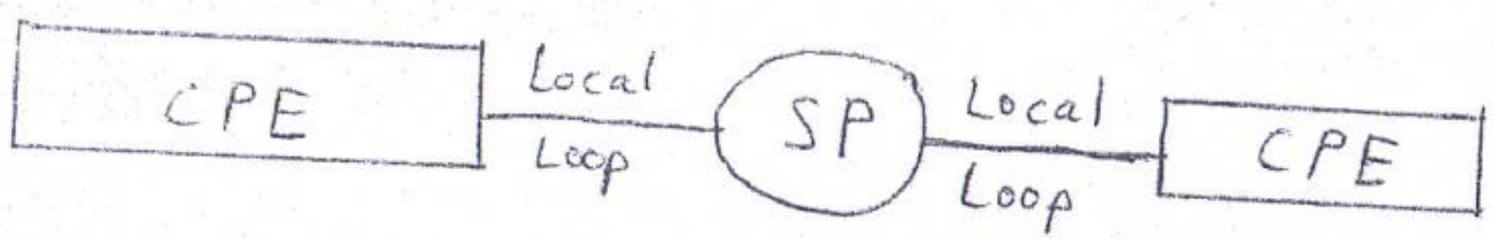
Wild Card Mask (WCM): inverted subnet mask

0 : exact match, 1 : don't care.

WAN Introduction:

Session 6 /2





WAN Speed:

DS0 = Digital Speed 0 = 64 Kb

DS1 = T_1 (1.54 Mb) / E_1 (2 Mb)

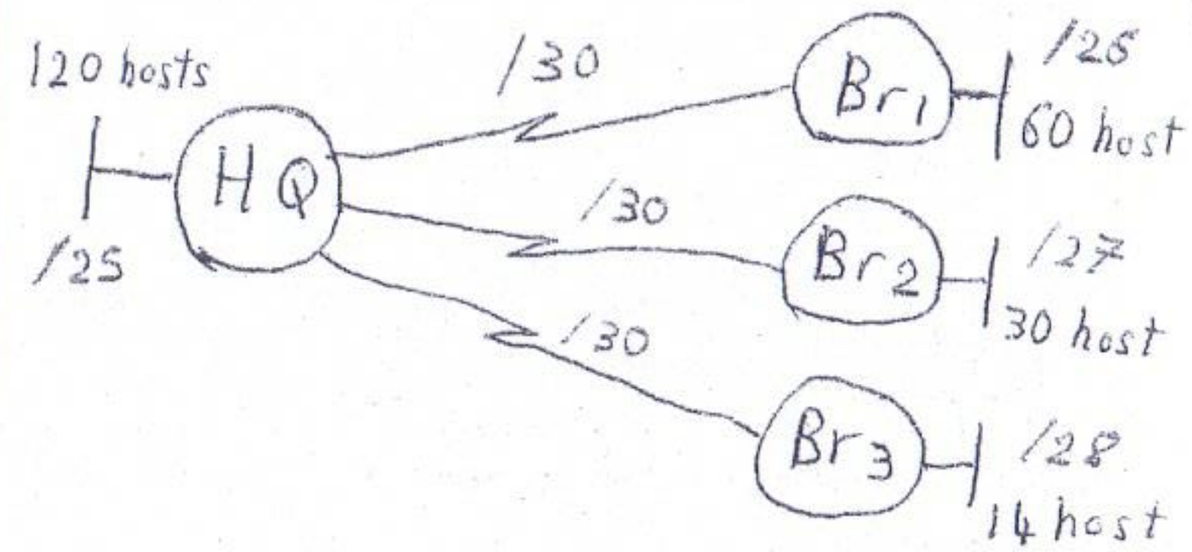
DS3 = T_3 (45 Mb) / E_3 (34 Mb)

STM 1 = 155 Mb

STM 64 = 10 Gb

STM 256 = 40 Gb

* Which routing protocols can support VLSM (Variable Length Subnet Mask)?



- Classless Protocols (RIP_{v2}, ISIS, OSPF, EIGRP, BGP)
  - support VLSM & CIDR

Classfull Protocols (RIP_{v1}, EGP, IGRP)

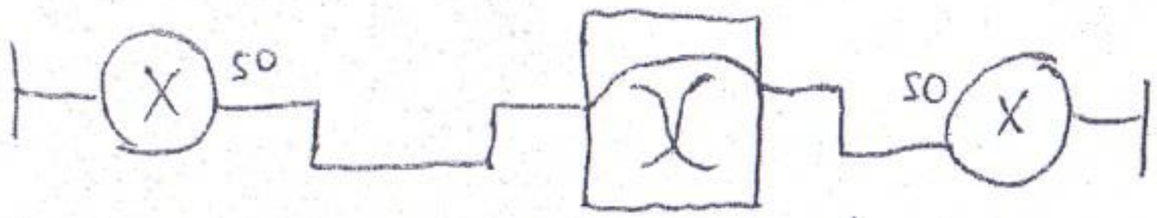
Session 6/3

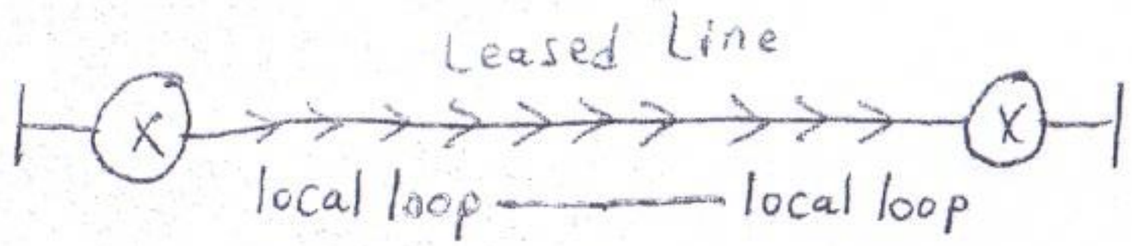
WAN Switching Classification (Private WAN)

Circuit Switching

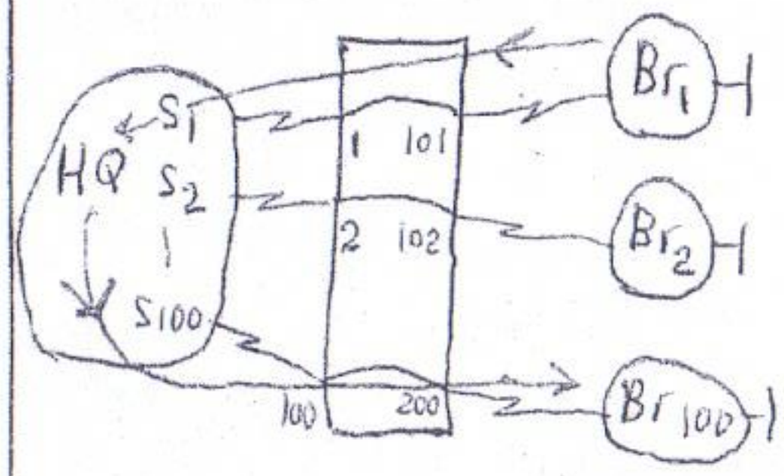
ex: HDLC : High level Data Link Control (cisco)
PPP : Point-to-Point Protocol (standard)

- It is physical cable (circuit) from hop to hop where all data move on same Path Point-to-Point.





Circuit Switching Disadv.:

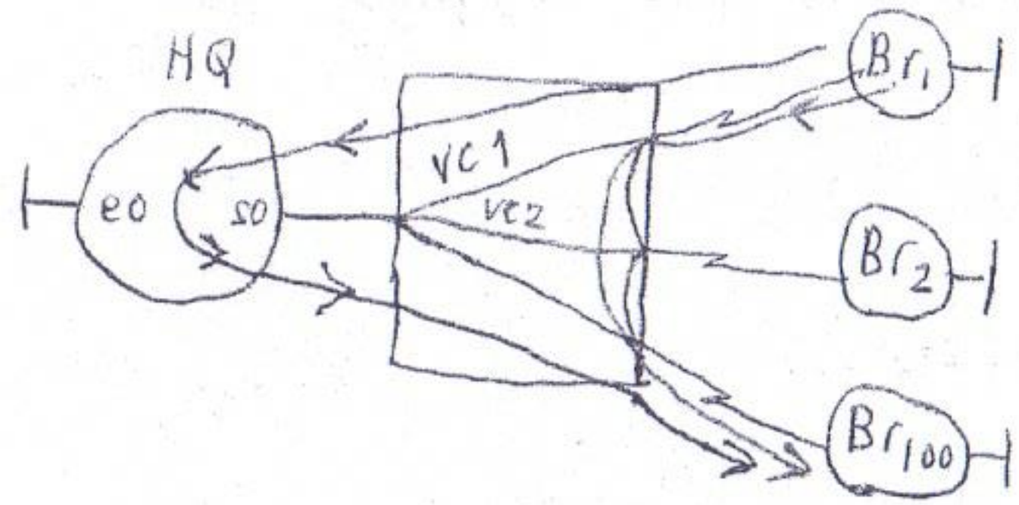


100 WIC
100 port
100 cable

Packet Switching

ex: X.25 → 45 Kb
FR → 45 Mb
ATM → 40 Gb

- It is Point to Multi Point technique based on virtual circuit & Multi Point to Multi Point



* FR is the best choice.

8 Mbps FR = L.E 100,000
8 Mbps ATM = L.E 500,000

Session 6/4

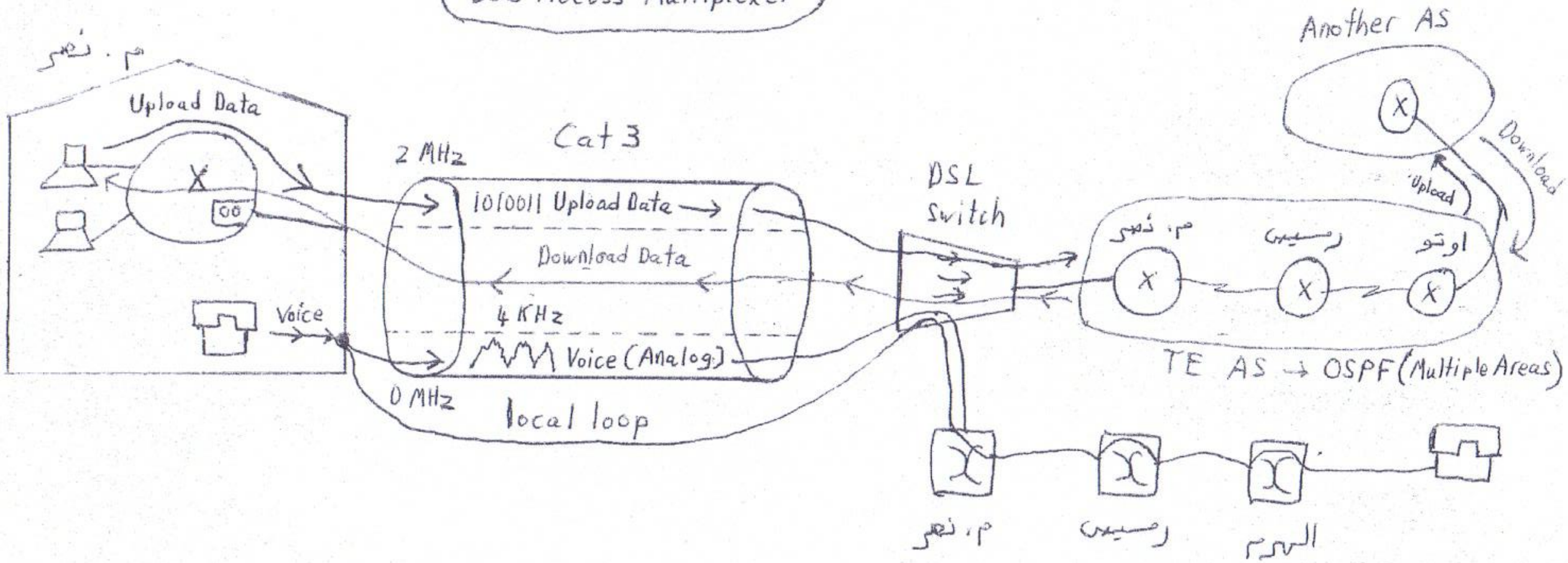
Public WAN:

BroadBand Technology:
- V Sat (Satellite)
- CATV (Cable TV)
- DSL (Digital Subscriber Line)

DSL
- ADSL: Asymetric DSL (Download > Upload) (Home users)
- SDSL: Symetric DSL (Download = Upload) (Enterprises)

- It is using all available frequences in order to gain high speeds.

DSL Switch (DSLAM)
DSL Access Multiplexer



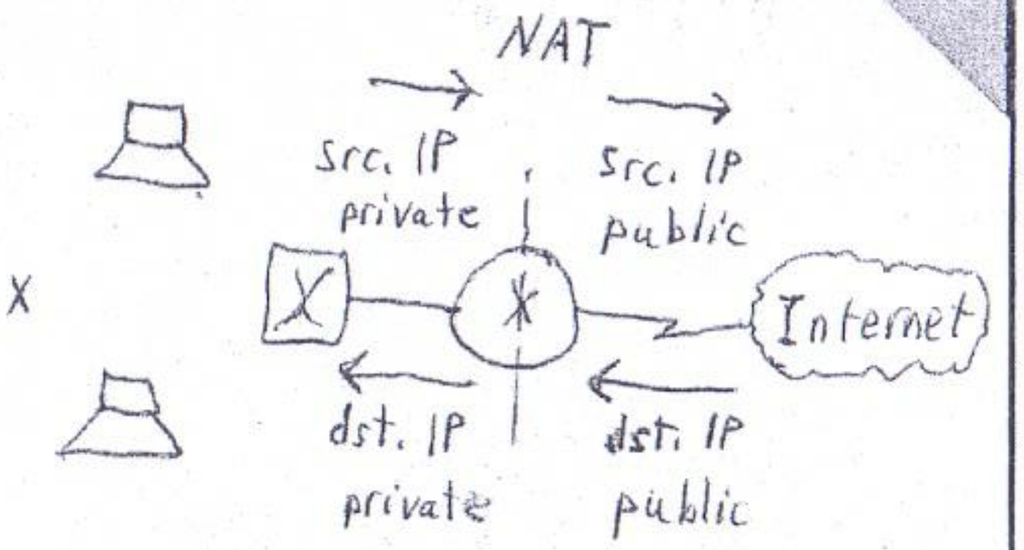
Network Address Translation (NAT)

Session 6/5

- Converts Private IP to Public IP

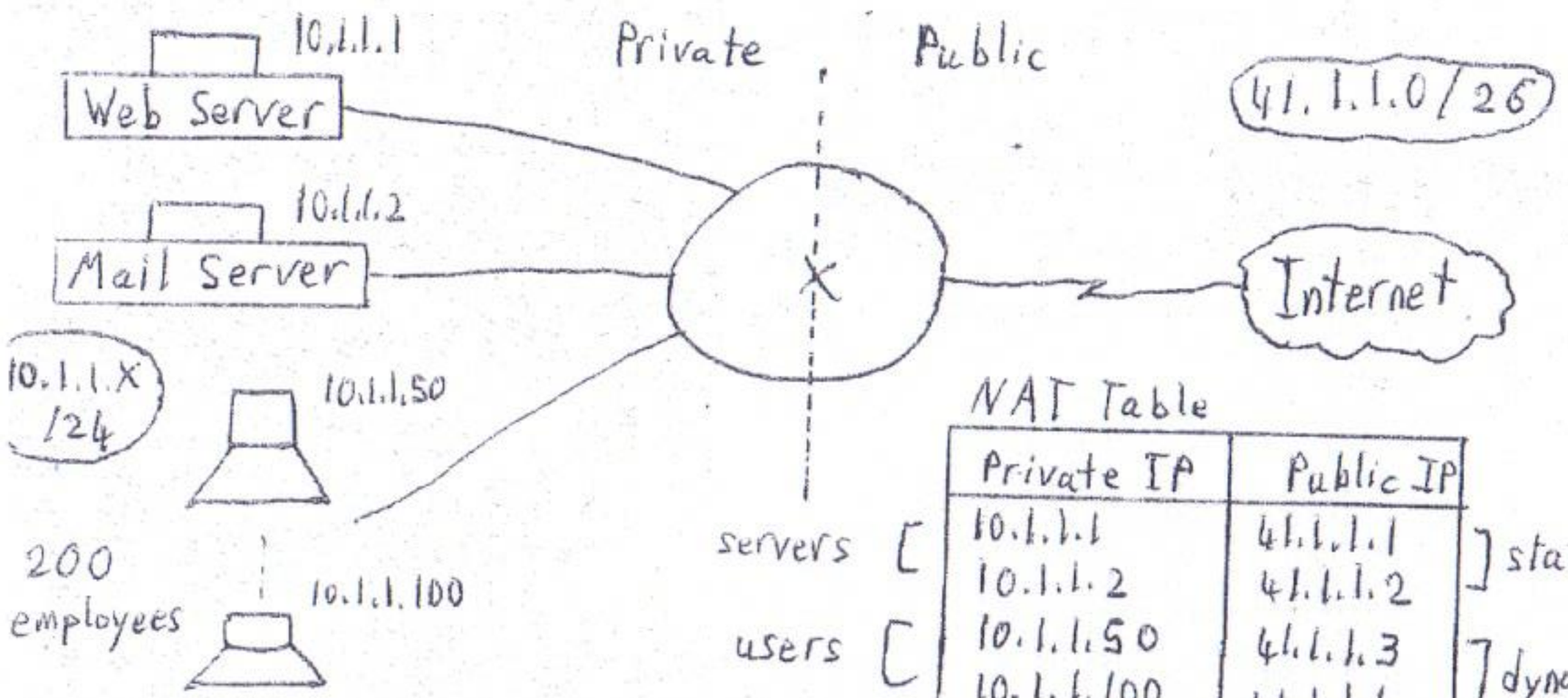
Private IPs: Class A: 10.X.X.X
Class B: 172.16.X.X – 172.31.X.X
Class C: 192.168.0.X – 192.168.255.X

APIPA
169.254.X.X
- Non routable
- private LAN only



Types of NAT:

① Static NAT: used for servers



NAT Table

	Private IP	Public IP	
servers	10.1.1.1	41.1.1.1	static
	10.1.1.2	41.1.1.2	
users	10.1.1.50	41.1.1.3	dynamic
	10.1.1.100	41.1.1.4	

(config)# ip nat inside source static 10.1.1.1 41.1.1.1 (private, public)
(config)# ip nat inside source static 10.1.1.2 41.1.1.2

show ip nat translation

② Dynamic NAT: used for users by using NAT pool

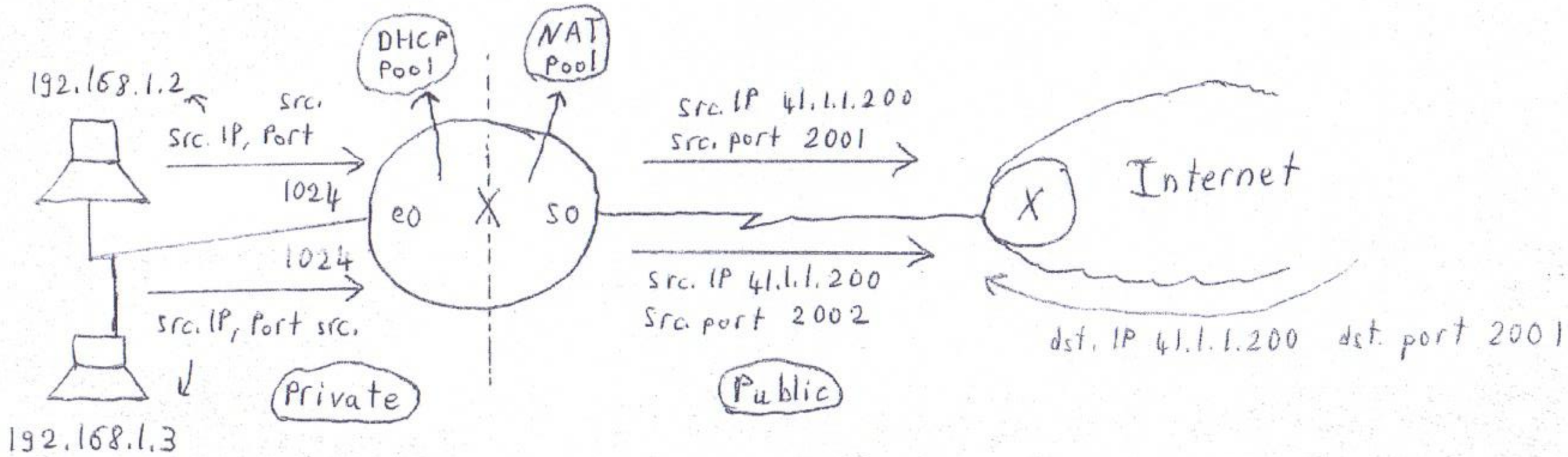
(config)# ip nat pool TE Data 41.1.1.3 41.1.1.62
(name, start ip, end ip)

netmask 255.255.255.192

Session 6/6

③ NAT with overload:

PAF: Port Address Translation



NAT Table

Local Socket	Global Socket
192.168.1.2 : 1024	41.1.1.200 : 2001
192.168.1.3 : 1024	41.1.1.200 : 2002

* Router differentiates between Devices with port numbers
* Devices can send data at the same time
* Link private ip addresses with one public ip

Which routing protocal support VLSM & CIDR ?

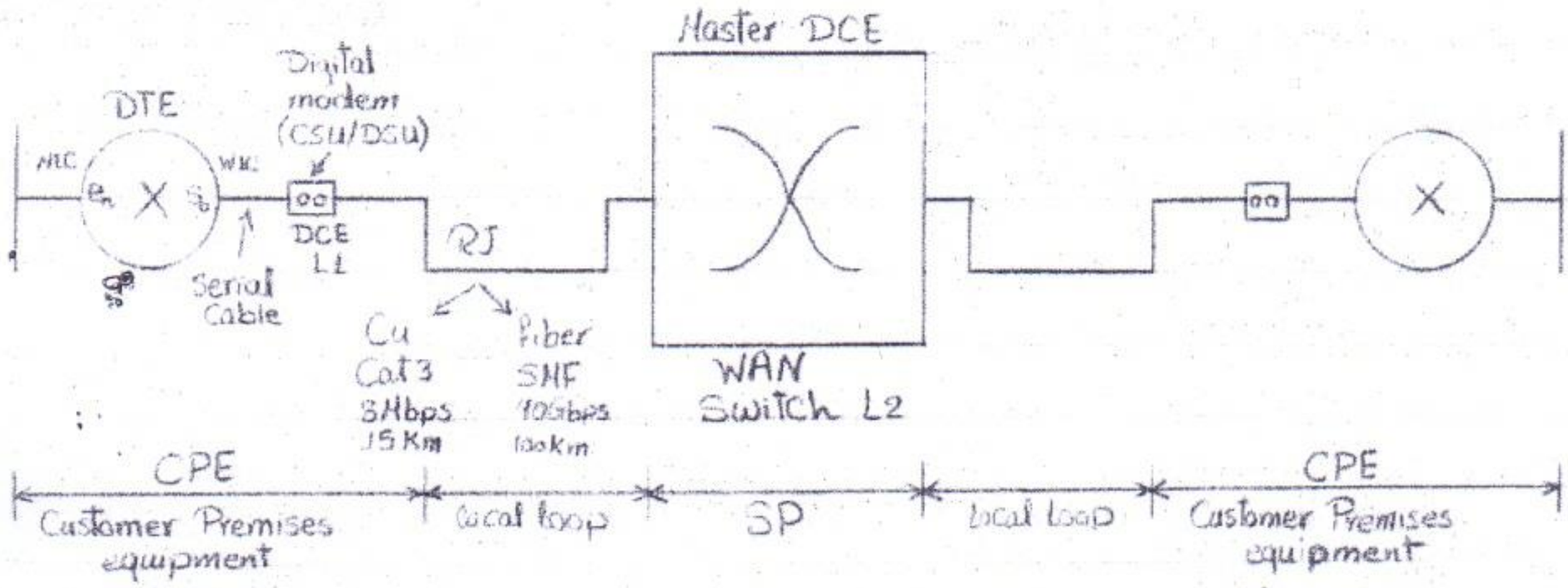
Classless protocal RIPv2, OSPF, EIGRP, BGP & ISIS

understand summarization & CIDR ...

understand FLSM & VLSM ...

Fixed length Subnet Mask	Variable length Subnet Mask

WAN Introduction :



Routing Protocals :

RIPv1, RIPv2, IGRP, EIGRP, OSPF & ISIS .

used to send and build routing tables.

Routed Protocals :

Ethernet (LAN) or X.25, ATM, FR, PPP, PPPOA, PPPOE & HDLC (WAN).

used to send data hop to hop.

WAN Speed :

DS_0 : Digital Speed Zero or Digital Service Zero = 64 Kbps.

DS_1 = T_1 : 1.54 Mbps E_1 : 2 Mbps

DS_3 = T_3 : 45 Mbps E_3 : 34 Mbps .

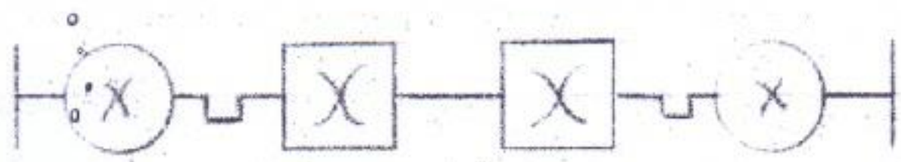
STM 1 = 155 Mbps . . . STM 64 = 10 Gbps , STM 256 = 40 Gbps.

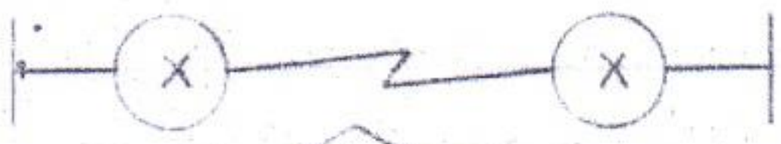
WAN Switching:

Private WAN

Circuit Switching

It is a physical Cable from hop to hop where all data moves on the Same path point to point.





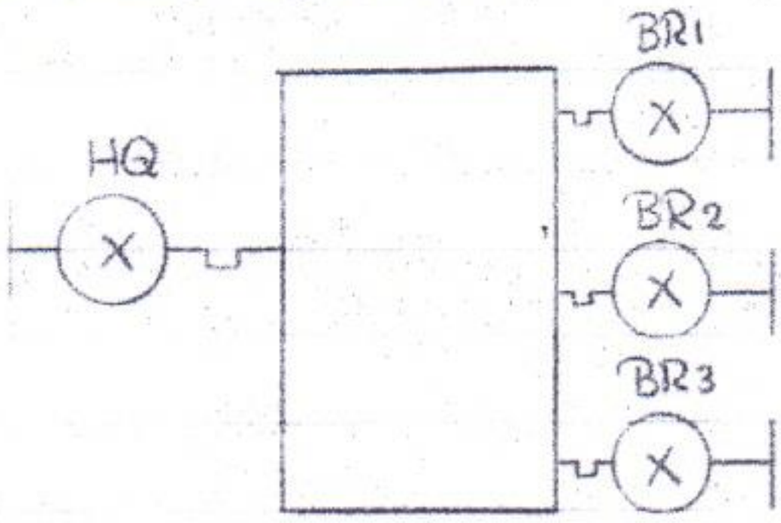
Dedicted C.S — Permenant C.S — static. C.S — leased line

Ondemand C.S — Temp. C.S — Dynamic C.S

Packet Switching

Point to multipoint.

ex. X.25, FR, ATM.



X.25 → 45 Kbps

Frame Relay → 45 Mbps

ATM → 10 : 40 Gbps

Asyncronous Transfer Mode

Public WAN : Broad Band Technologies :

Using all available Frequencies in order to gain higher speeds.

Digital Subscriber Line (DSL)

ADSL

Asymmetric DSL

Download > Upload

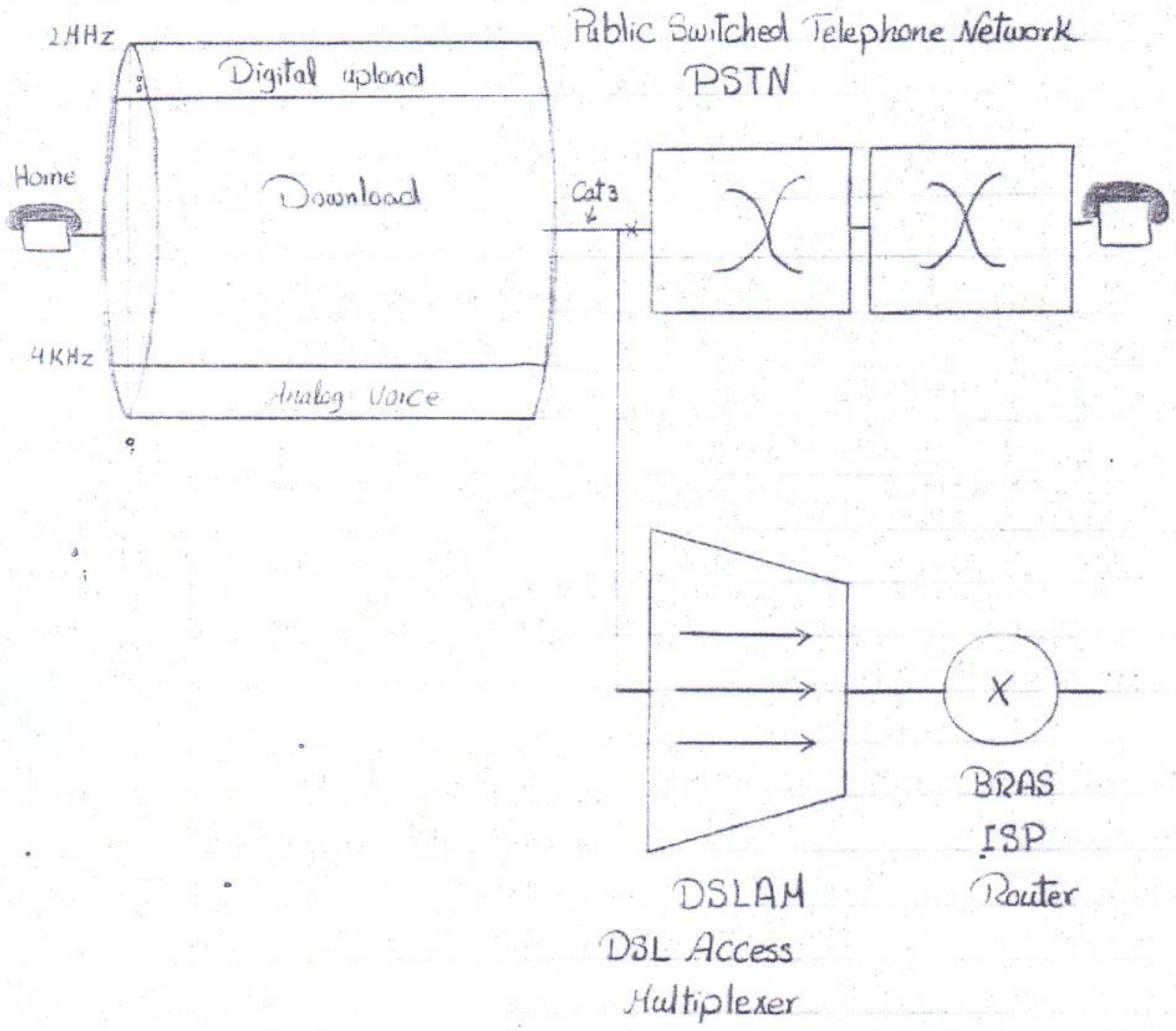
Home users

SDSL

Symmetric DSL

Download = Upload

Enterprises


Public Switched Telephone Network
PSTN
2MHz
Digital upload
Home
Download
Cat3
4KHz
Analog Voice
BRAS
ISP
Router
DSLAM
DSL Access
Multiplexer

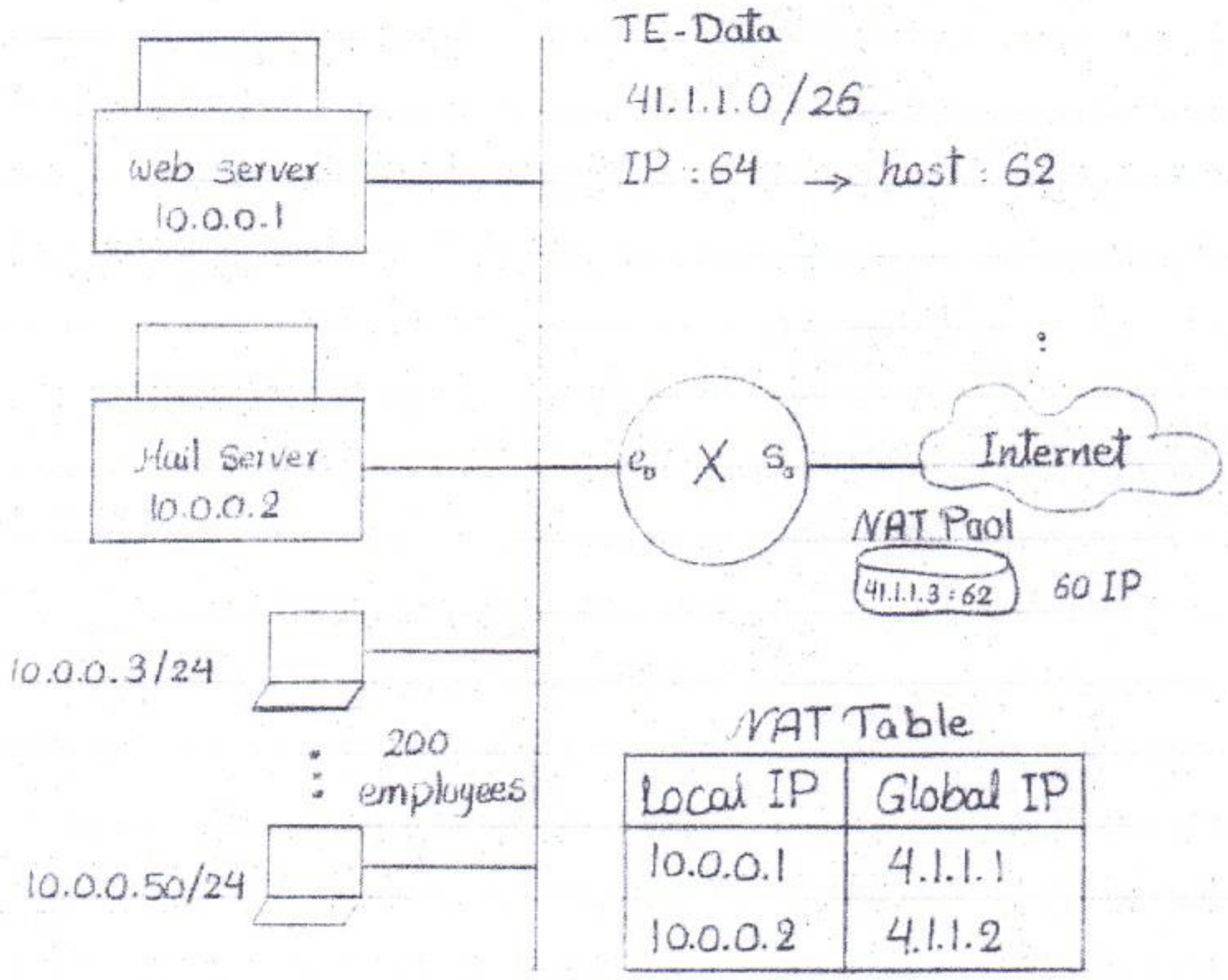
Network Address Translation (NAT):

Private IP:

- Class A: 10.0.0.0 /8
- Class B: 172.16.0.0/12
- Class C: 192.168.0.0 /16

Types of NAT:

1. Static NAT: used with servers.



NAT Table

Local IP	Global IP
10.0.0.1	4.1.1.1
10.0.0.2	4.1.1.2

(Config) ※ ip nat inside source static Private IP Public IP

2. Dynamic NAT: used with users.

(Config) ※ ip nat pool TEData Name start IP end IP

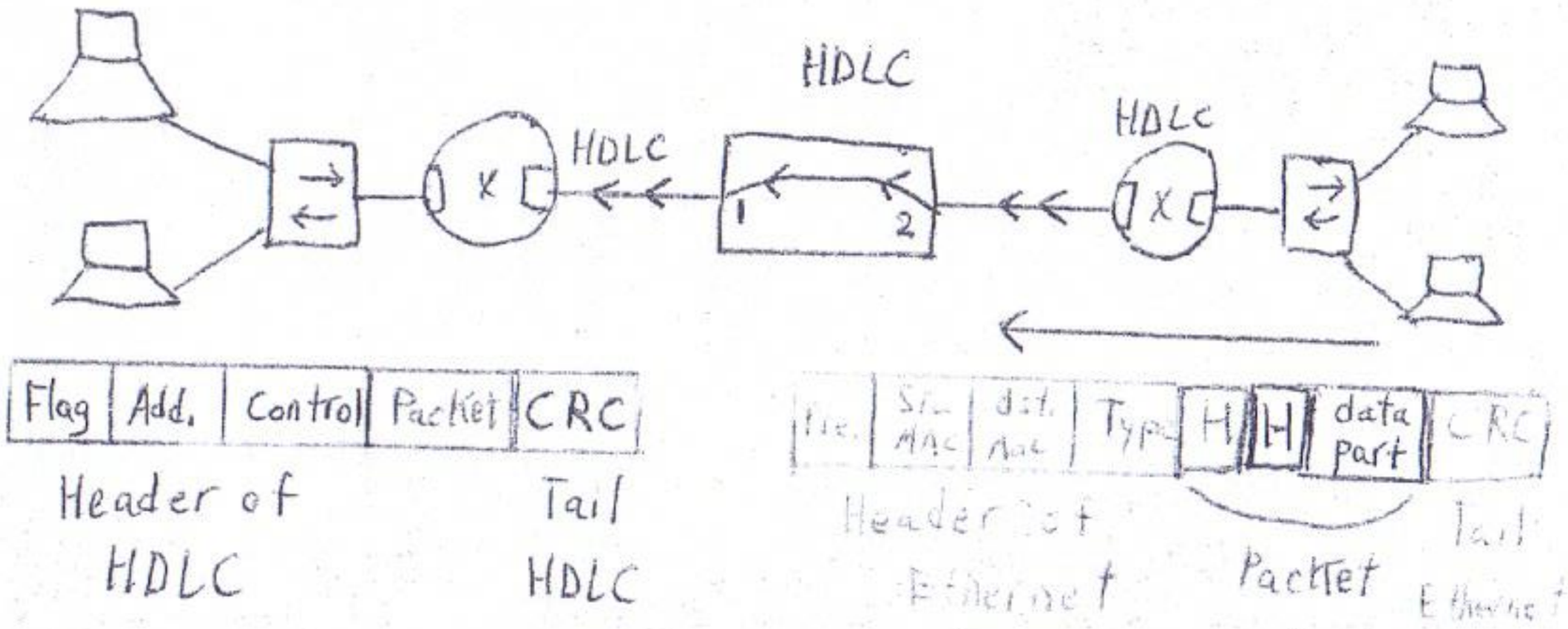
3. Dynamic NAT with overload (PAT Port Address Translation):

used with users "All devices on network used the same public IP".

Session 7/2

Circuit Switching: Point-to-Point Switching

Encapsulation:



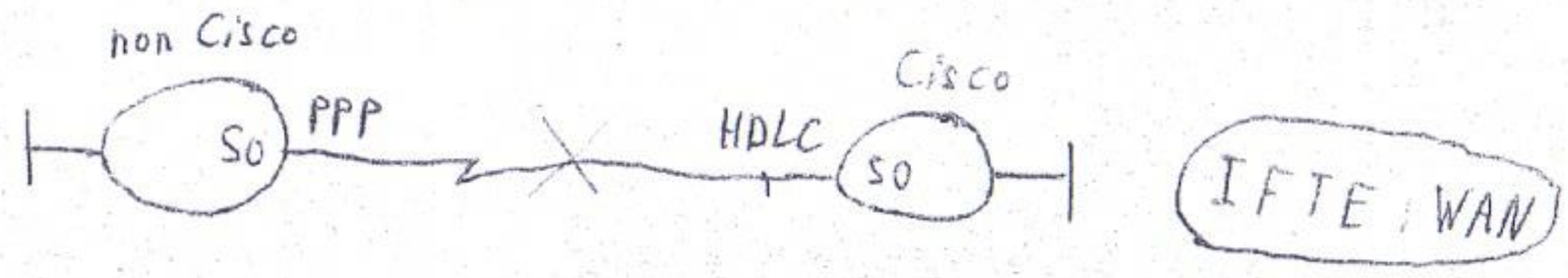
* ISO HDLC (Highlevel Data Link Control)
  - not supported by Cisco

Flag	Address	Control	Packet	CRC
0111 1110	1111 1111 (as Broadcast)	↓ used in operation		

* Cisco HDLC (default in all Cisco WIC) - Serial

Flag	Address	Control	Type	Packet	CRC

4 → IP_{v4}
6 → IP_{v6}

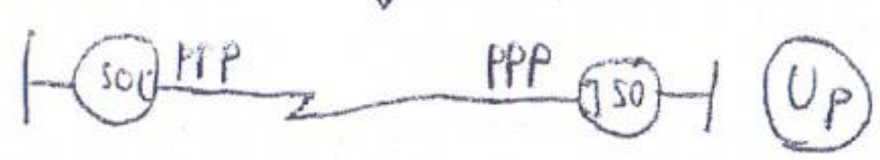


show ip interface brief

Interface	status (L1)	protocol (L2)
S0	up	down / up

mismatch in L2 protocol
missing clockrate

(config) # interface S0
(config-if) # encapsulation PPP
⇓



up → match

* PPP (Point-to-Point Protocol)

Flag	Address	Control	Type	Packet	CRC

14 → IP_{v4}
16 → IP_{v6}

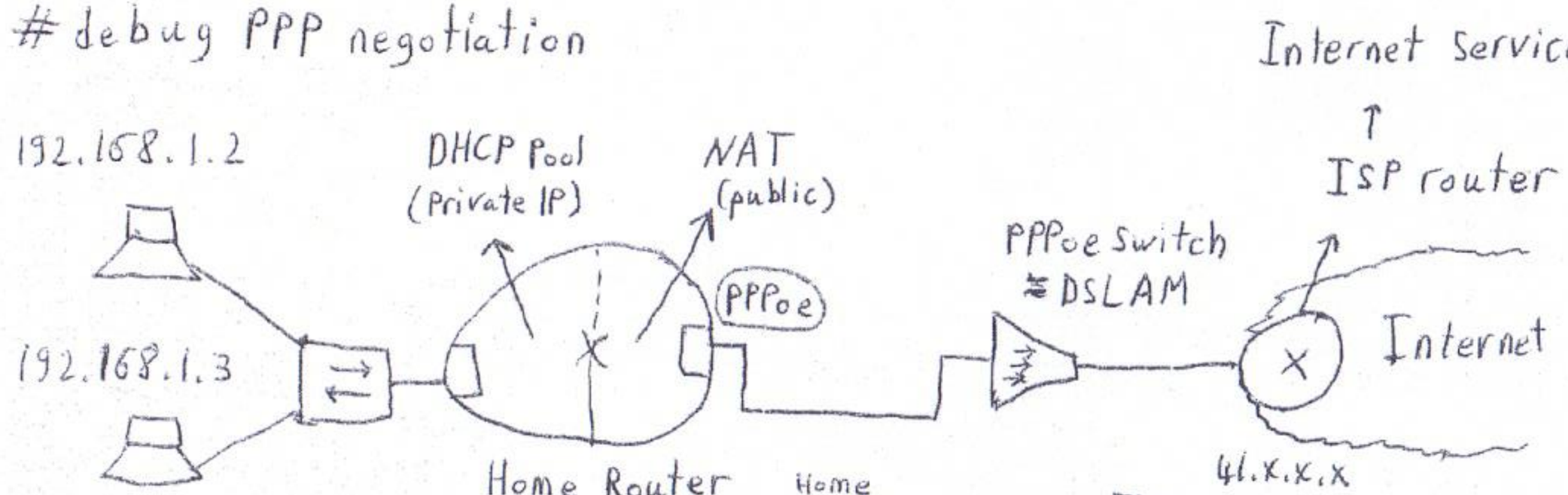
PPP Operation & PPPoe Operation:

Session 7/2

↓ Private WAN

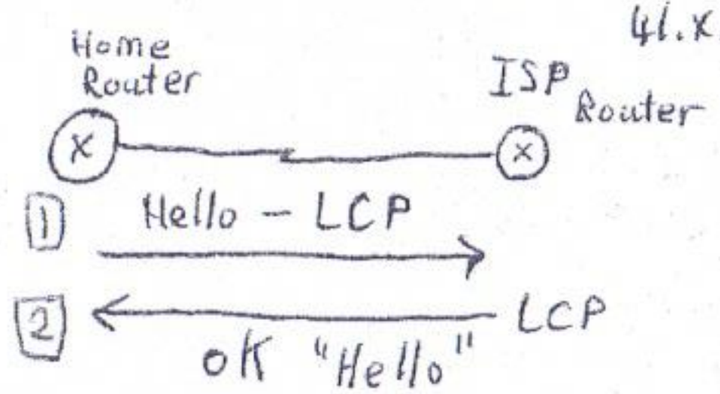
↓ Public WAN

debug PPP negotiation



Phase 1

[options negotiation
optional authentication]



Phase 1: (Neighbor Discovery)

"exchange of Hello" = LCP

Link Control Protocol,

Phase 2: (IP Discovery) 3 NCP – Please give me real IP

NCP = Network Control Protocol 4 Here is your real IP 41.1.1.200/32

Phase 3: (data from hop to hop)

PPP H	Packet	PPP T

PPPoe

1	PADI : PPPoe Active Discovery Initiation
2	PADO : PPPoe Active Discovery Offer
3	PADR : PPPoe Active Discovery Request
4	PADS : PPPoe Active Discovery Session Confirmation

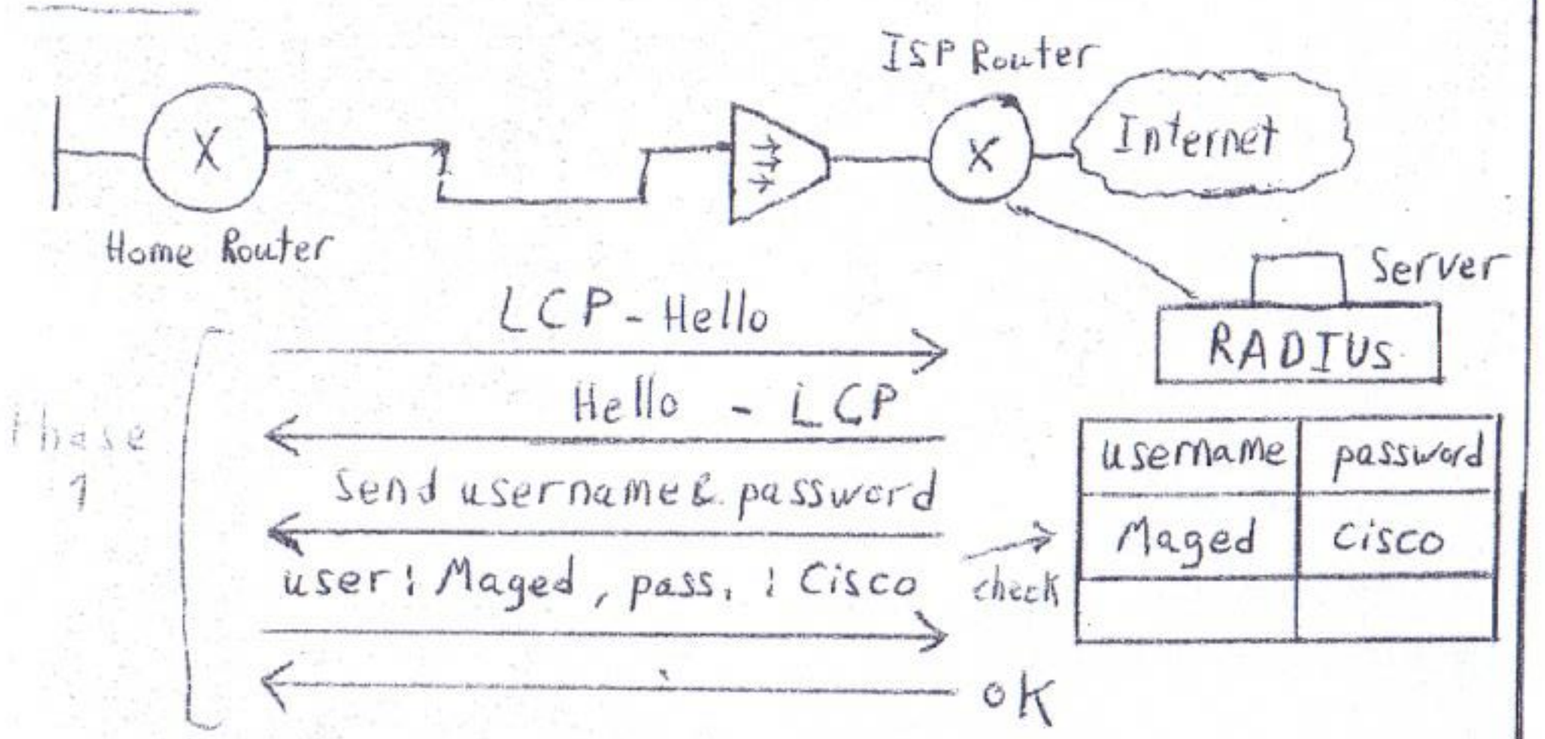
Session 1/3

PPP & PPPoe Authentication Option:

- PAP : PPPoe Authentication Protocol → Clear Text Password
- CHAP : Challenge Handshake Auth. Protocol → Hashed Password

```
(config)# interface S0
(config-if)# encapsulation PPP
(config-if)# PPP authentication {PAP/CHAP}
```

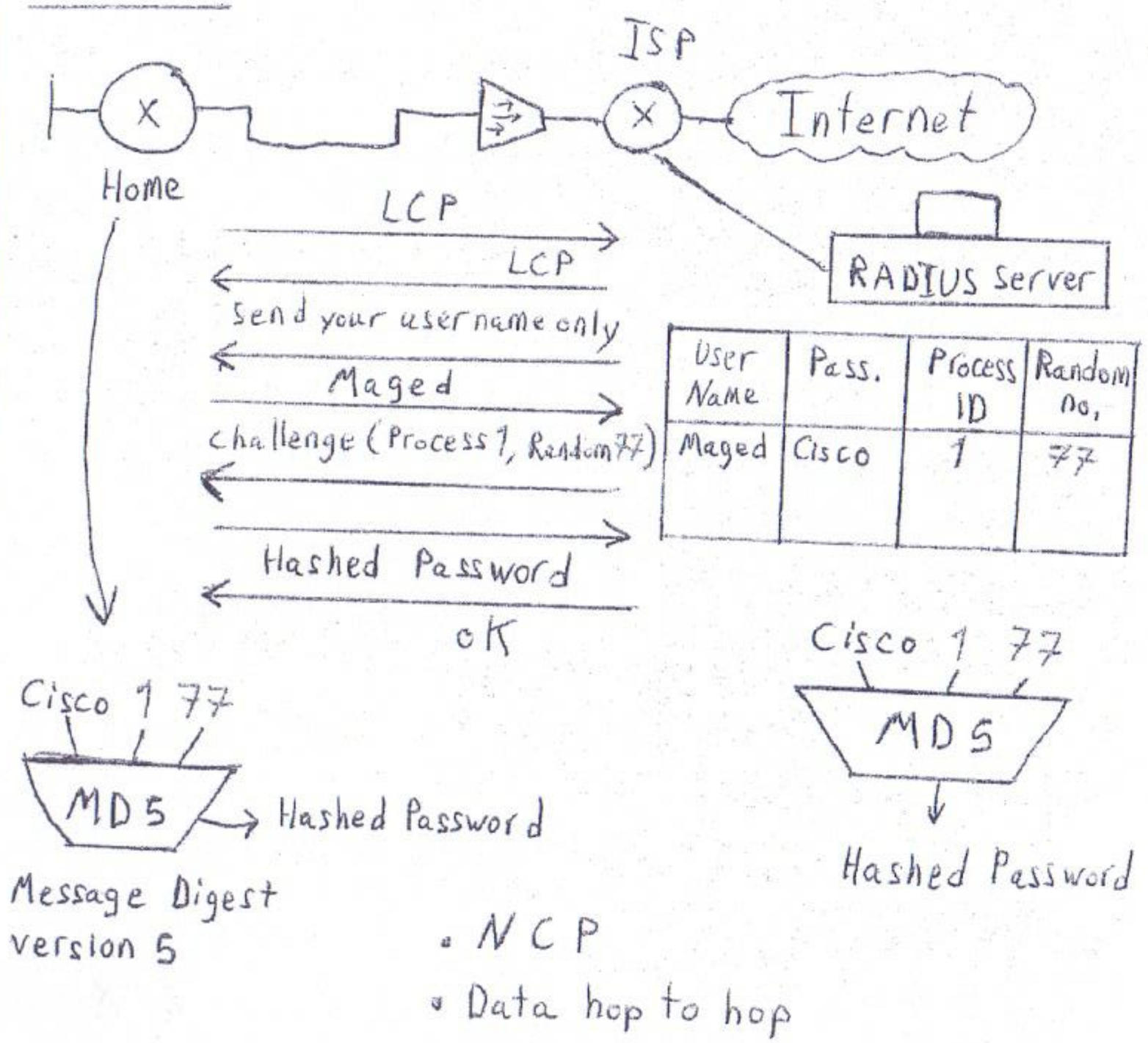
PAP:



Phase 2 : NCP

Phase 3 : Data from hop to hop

CHAP:



Message Digest version 5

- NCP
- Data hop to hop

Circuit Switching Protocals:

It is Point to point protocal.. ex: HDLC & PPP.

- **EnCapsulation:**

ISO HDLC (High level Data link Control):

Flag	Address	Control Operation	Packet	CRC

Cisco HDLC : used by default on all serial (WIC).

Flag	Address	Control Operation	Type IPV4 → 4 IPV6 → 6	Packet	CRC

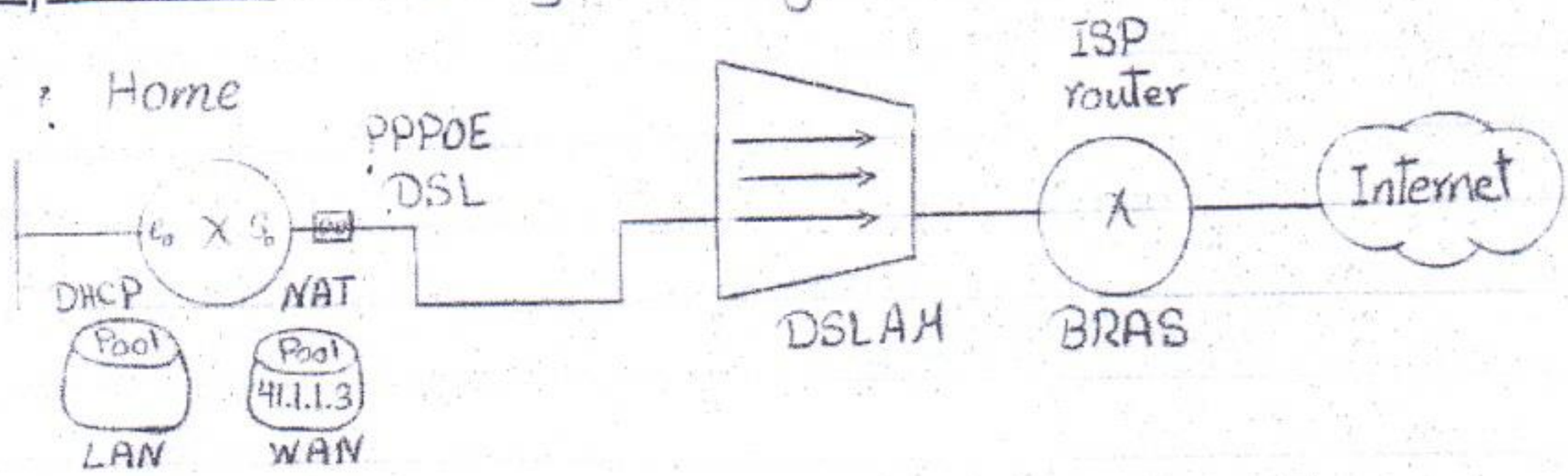
PPP (Point-to-Point Protocal) is standard protocal:

Flag	Address	Control Operation	Type IPV4 → 14 IPV6 → 16	Packet	CRC

- **Configuration:**

(Config) ※ interface ___
(Config-if) ※ no shutdown
(Config-if) ※ clock rate ___
(Config-if) ※ encapsulation PPP layer 2 protocal
(Config-if) ※ exit
(Config) ※ exit
※. Show ip interface brief.

• **Operation :** ※ debug PPP negotiation



Phase 1 : Neighbor Discovery :

LCP (link Contral Protocal) (open link) →

← OK LCP

→ options negotiations
ex : Authentication

Phase 2 : IP Discovery :

Network Contral Protocal

NCP (Give me real IPv4 address) →

← IPv4 is 41.1.1.3/32 (one IP)

} InCase use IPv4

(Give me real IPv6 address) →

← IPv6 is ....

} In Case use IPv6

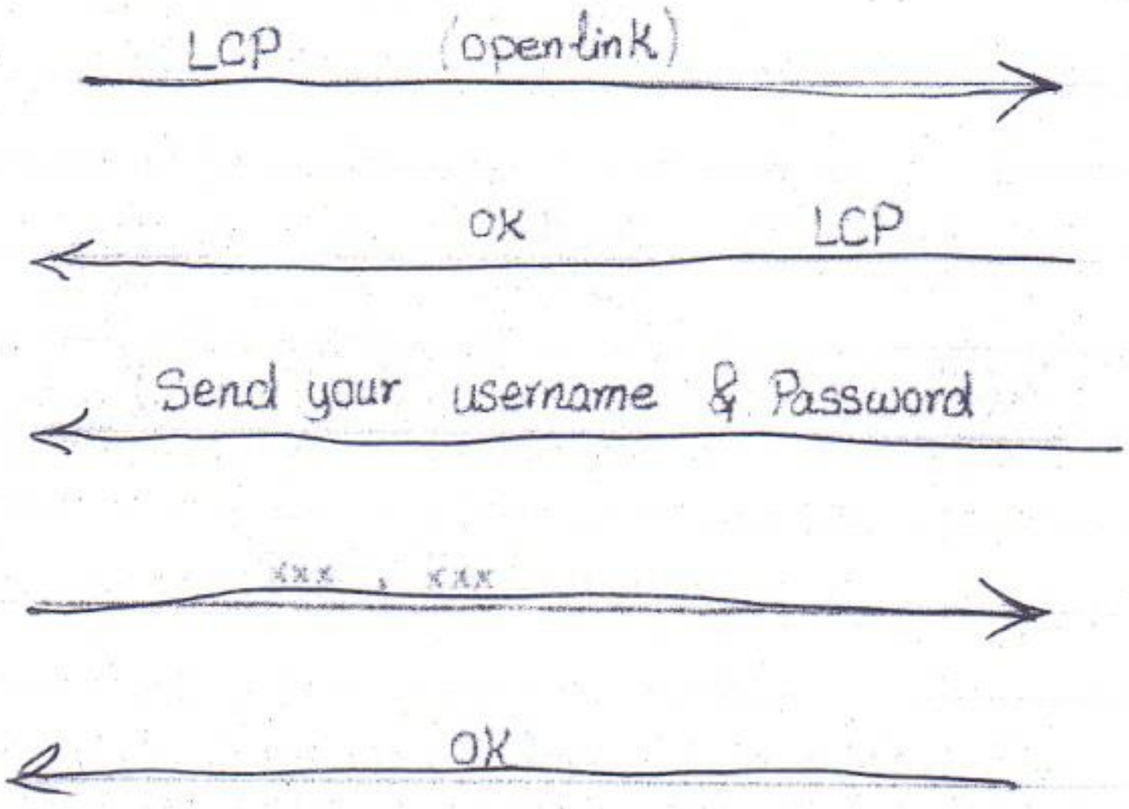
Phase 3 : Sending data hop to hop .

نظريه ليس ملك التحميل
علشان اتصل الداتا من غير التحميل

→ **Authentication :**

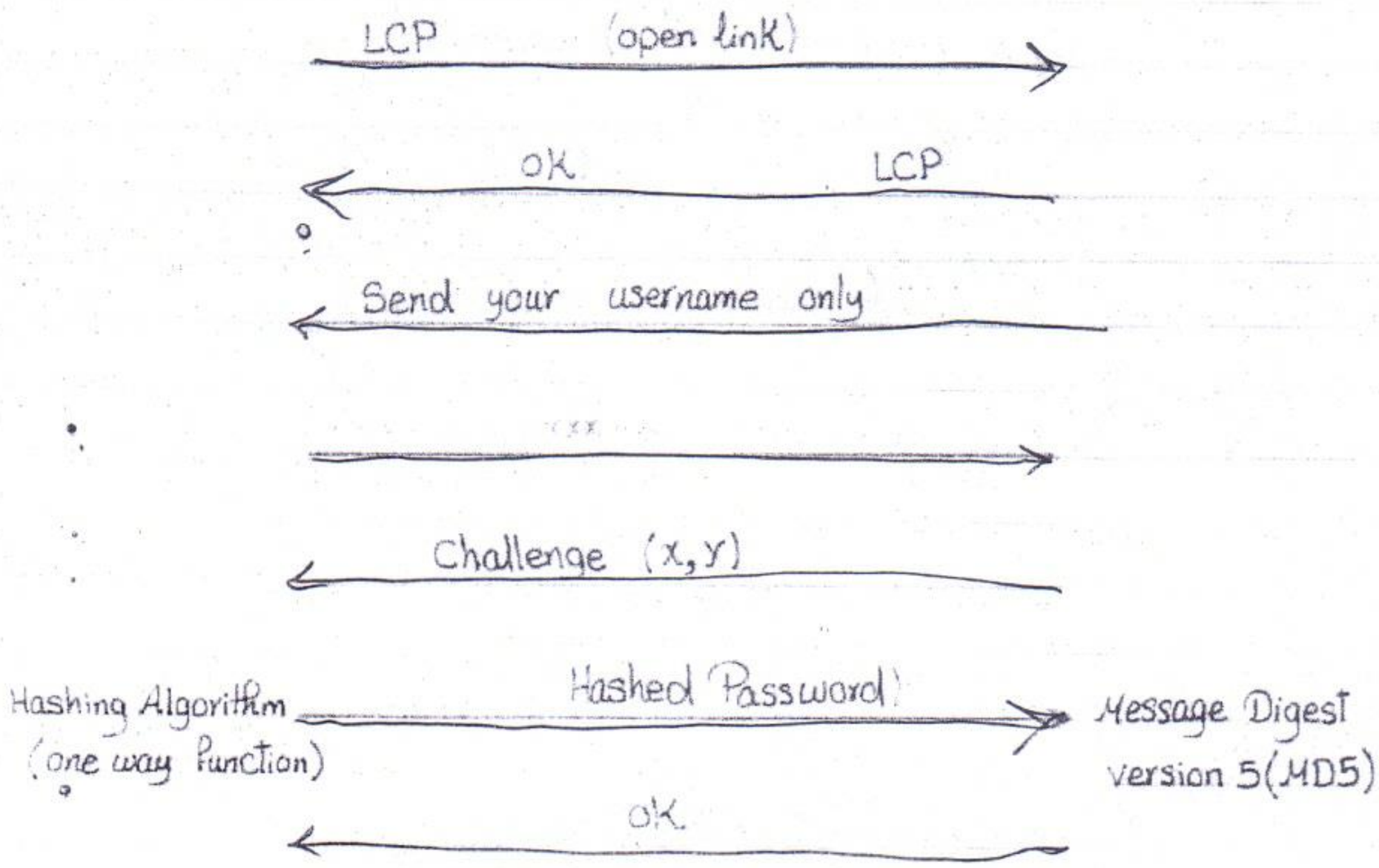
There are two type

- PAP: Point to Point Authentication Protocal



Disadvantage: password is send in clear text .

- CHAP: Challenge Handshake Authentication Protocal



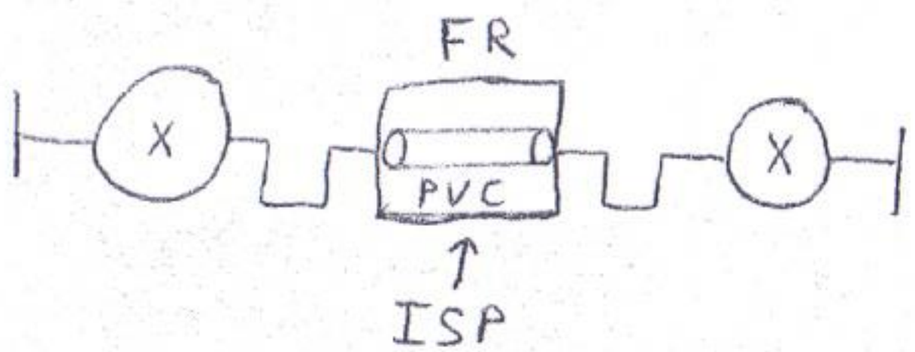
Session 8 /1

Frame Relay:

It is Point to Multipoint Packet Switching technology based on PVC (Permanent Virtual Circuits) = micro segments

FR Topologies:

1 Point-to-Point:

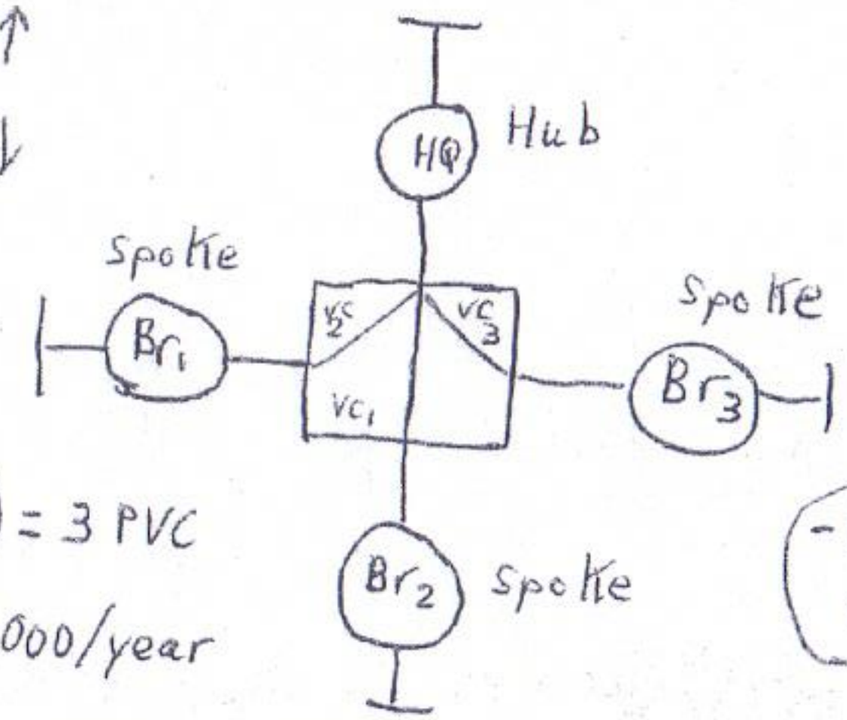


- links 2 routers only
- PVC = L.E 100,000 / year for 8 Mbps

2 Point-to-Multipoint: Star Topology = Hub & Spoke

HQ — Branches

Delay ↑
Cost ↓

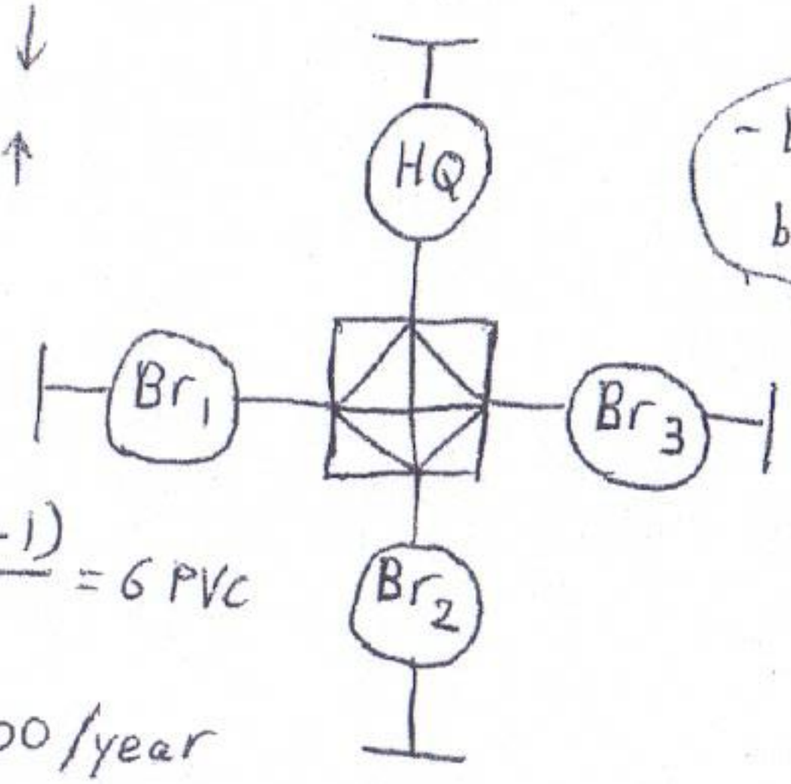


PVC = (n-1) = 3 PVC
= L.E 270,000/year

- links HQ to branches

3 Multipoint-to-Multipoint: Mesh Topology

Delay ↓
Cost ↑

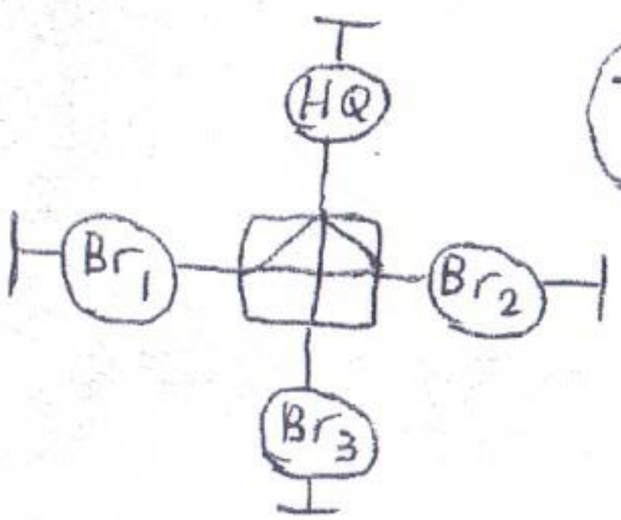


- links HQ and branches together

$PVC = \frac{n(n-1)}{2} = 6$ PVC

= L.E 500,000 /year

4 Partial Mesh: Flexible Topology



- links some branches together

Session 8 /2

FR Encapsulation: is called LAPF

(Link Access Procedure for FR)

Flag	Address	Control	Packet	CRC

→ not supported by Cisco

0111 1110

Address → VC id

Control → used in operation

- ATM → VPI/VCI (16 bit)
  (Virtual Path Id / Virtual Circuit Id)
- X.25 → X.25 (8 bit)
- FR → DLCI (10 bit)

(Data Link Circuit Id) = 0 - 1023
- Reserved: 0 - 15 & 1023 (for future)
- Available: 16 - 1022

* Cisco LAPF

Flag	Address	Control	Type	Packet	CRC

DLCI

4 → IP_{v4}

6 → IP_{v6}

```
(config)# interface S0
(config-if)# encapsulation frame-relay
```

* IETF LAPF

Flag	Address	Control	Type	Packet	CRC

40 → IP_{v4}

60 → IP_{v6}

```
(config)# interface S0
(config-if)# encapsulation frame-relay ietf
```

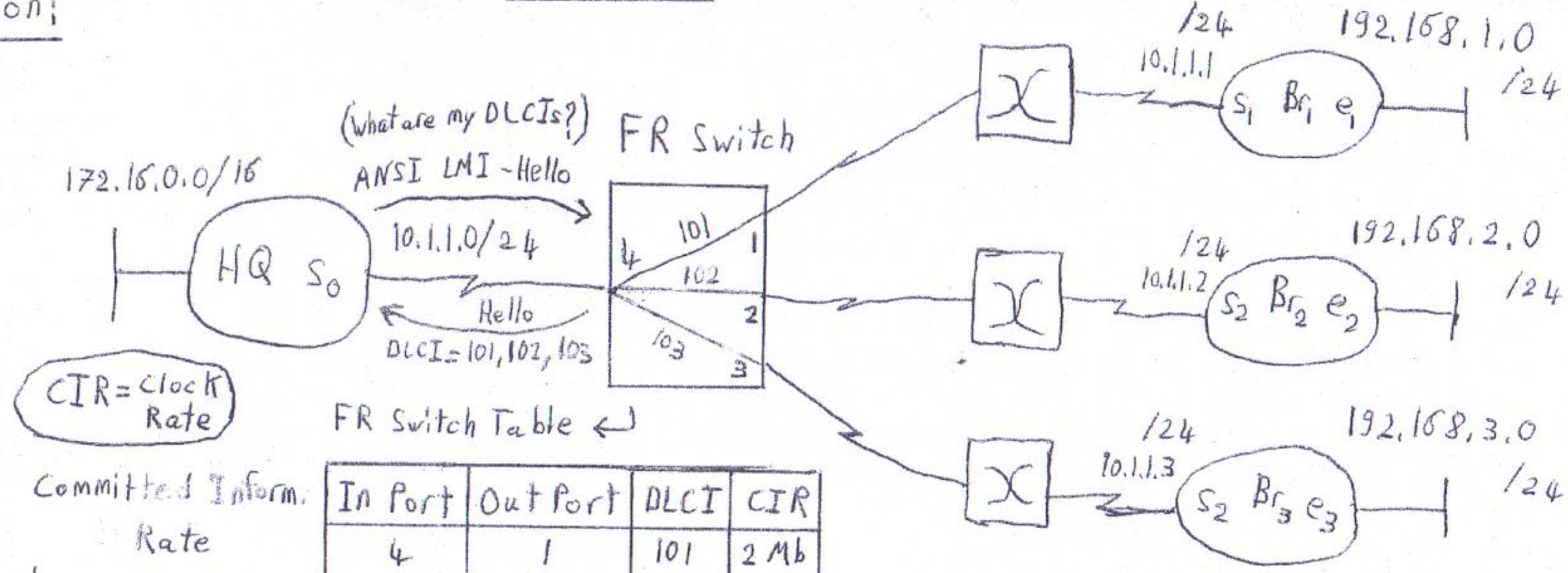
Session 8 /3

FR Operation:

@Startup:

(config)# inf S0

(config-if)# enc FR



CIR = Clock Rate

Committed Inform. Rate

FR Switch Table

In Port	Out Port	DLCI	CIR
4	1	101	2 Mb
4	2	102	4 Mb
4	3	103	2 Mb

1] Neighbor Discovery

"Exchange of Hello"

LMI : Local Management Interface

↓

ANSI LMI

2] IP discovery

use IARP:

(Inverse ARP)

IARP on DLCI 101 (What is your IP?) →

← Reply DLCI 101 ⇒ IP = 10.1.1.1 — Br_1

IARP on DLCI 102 →

← IP = 10.1.1.2 — Br_2

IARP on DLCI 103 →

← IP = 10.1.1.3 — Br_3

IARP Table

DLCI	IP
101	10.1.1.1
102	10.1.1.2
103	10.1.1.3

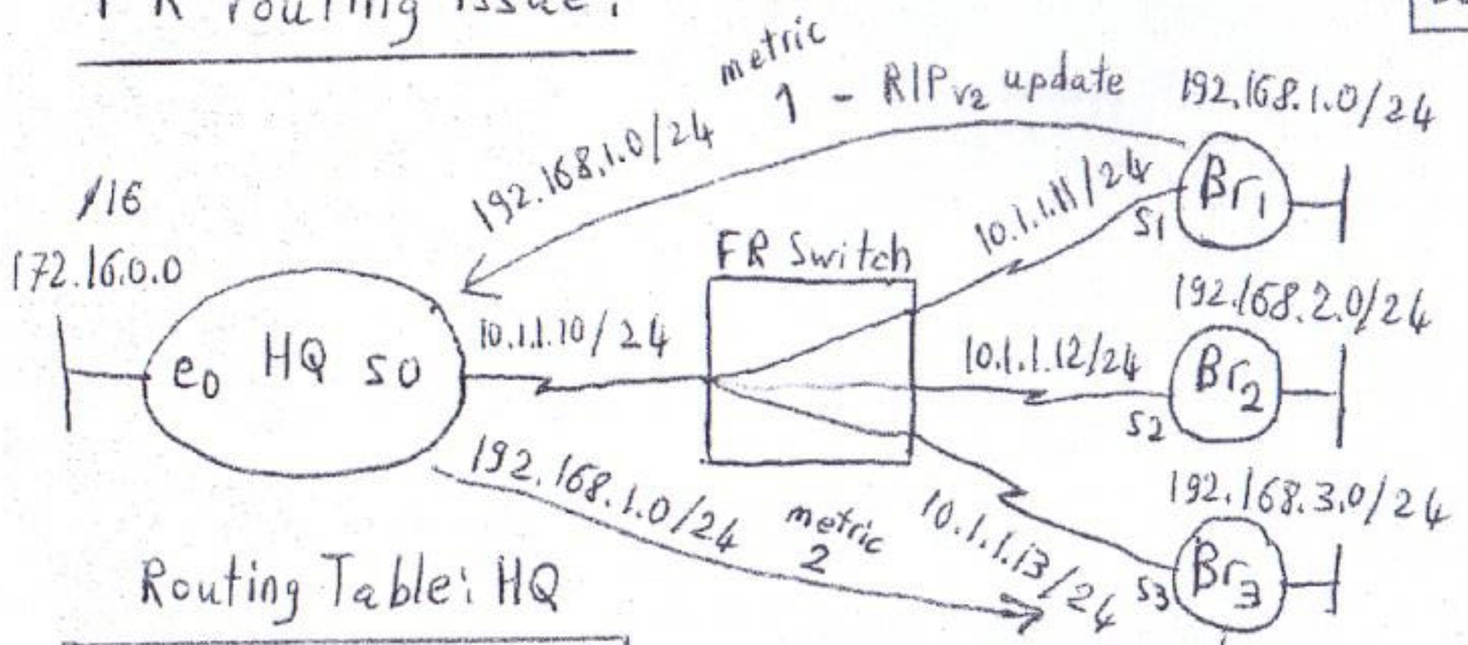
show frame-relay map

data from hop to hop

H	Packet	T

Session 8/7

FR routing issue:



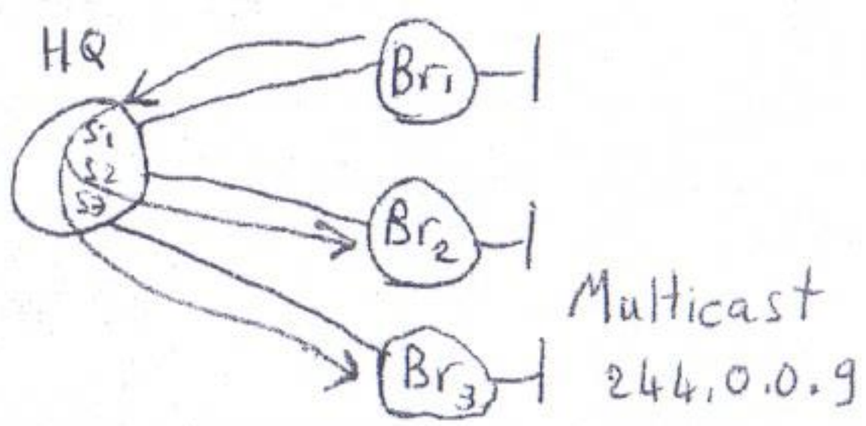
Routing Table: HQ

C	172.16.0.0/24	e0	
C	10.1.1.10/24	s0	
R	192.168.1.0/24	s0	1

C	192.168.3.0/24	e3	
C	10.1.1.13/24	s3	
R	192.168.1.0/24	s3	2

Split Horizon: Routes learnt from interface should never be advertised back on same interface.

Disadvantage: prohibits routing updates received on an interface from exiting that same interface. (although it saves resources)

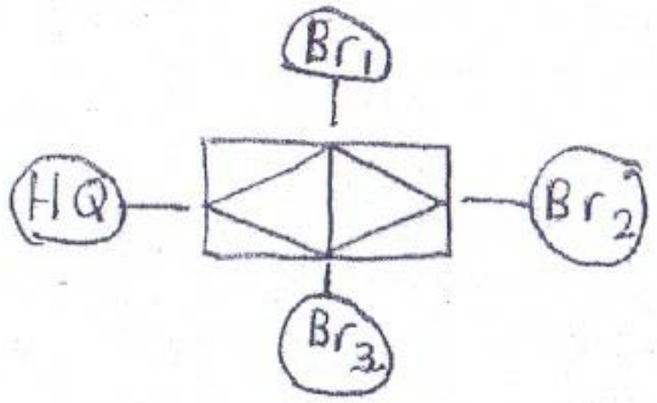


Solution:

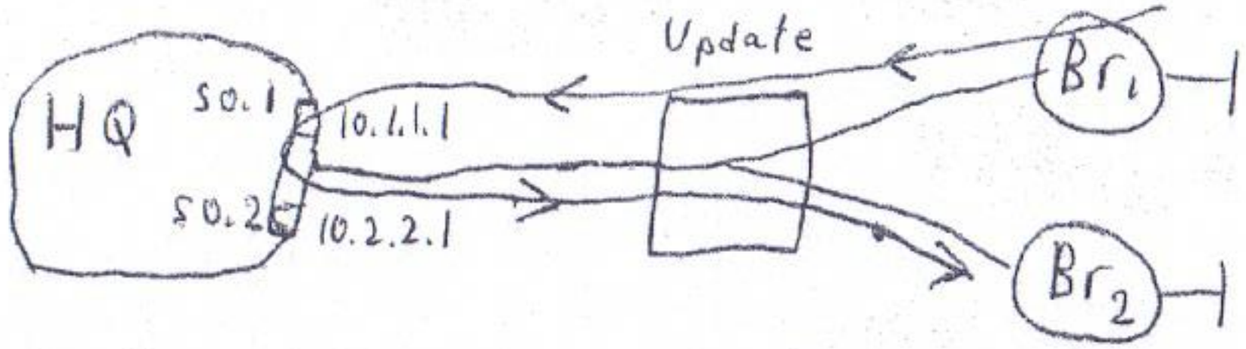
Waste resources

1. Disable Split Horizon (config-if)# no ip split horizon
2. Use Static Routing
3. Use Full mesh topology

2, 3, 4 → Use Split Horizon



4. Divide main interface into point-to-point subinterfaces.



HQ(config)# int. s0
HQ(config-if)# no shutdown
HQ(config-if)# no ip address
HQ(config-if)# enc. fr
HQ(config-if)# exit

HQ(config)# int. s0.1
(config-subif)# ip address ip mask

HQ(config)# int. s0.2
(config-subif)# ip address ip mask

Session 8/5

Private WAN

* switch forwards thousands of frames per second

* forwards millions of frames per second

Circuit Switching

* point-to-point topology
* address = no address
* ex: HDLC / PPP

Packet Switching

* Flexible Topology < P-2-P, P-2-M, M-2-M
* address:
  - X.25 (8 bit)
  - DLCI (10 bit)
  - VPI/VCI (16 bit)
* ex: X.25 - FR - ATM

Ethernet Switching

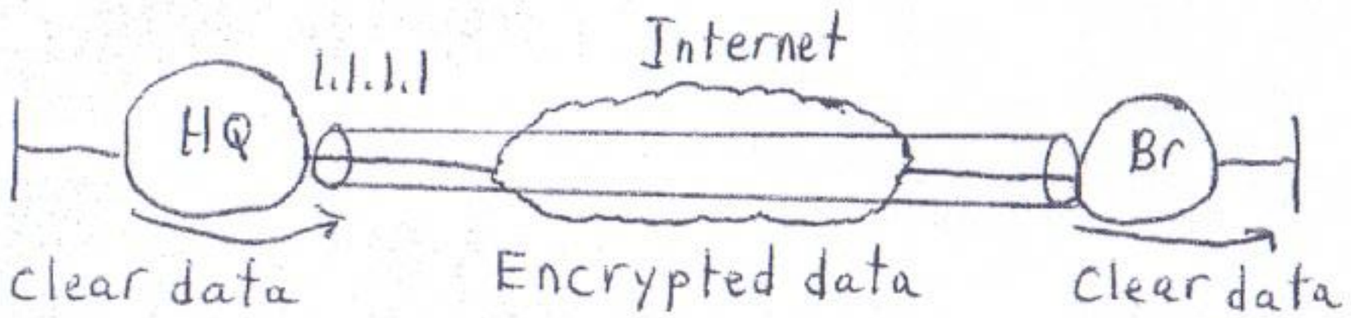
* using Fiber SMFC (8/125 μm) (100 Km)
* address:
  MAC address = 48 bit
  ex: Metro Ethernet (100 Gbps)

Label Switching

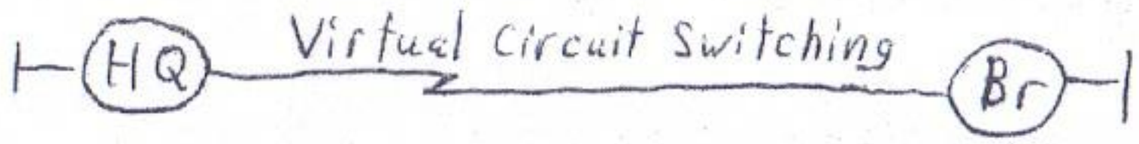
* Flexible Topology
* address: Label (20 bit)
* speeds: 100 Gbps
* low delay = low latency
* ex: MPLS: Multi Protocol Label Switching

VPN: Virtual Private Network

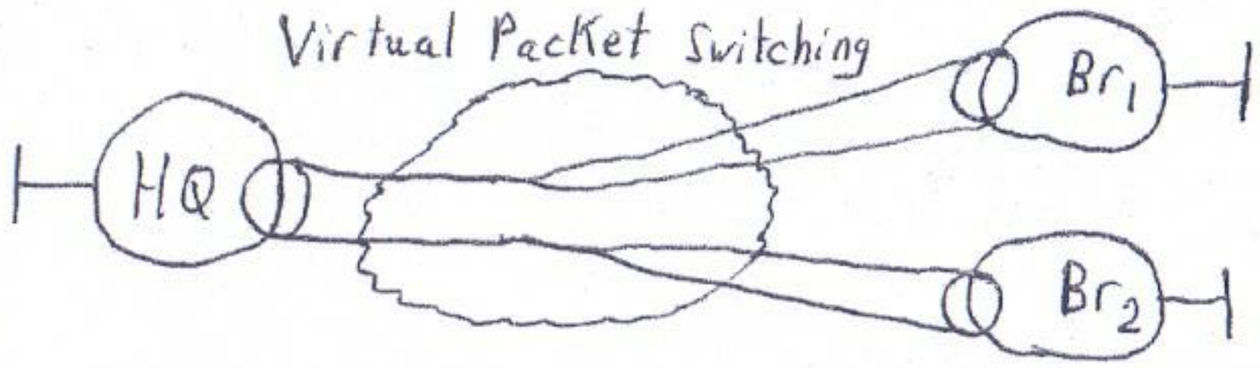
- It is building private WAN (HQ & Branches) over public WAN (Internet)
- Site to site Vpn



ex: GRE + IP sec



ex: DMVPN (Dynamic Multipoint VPN)



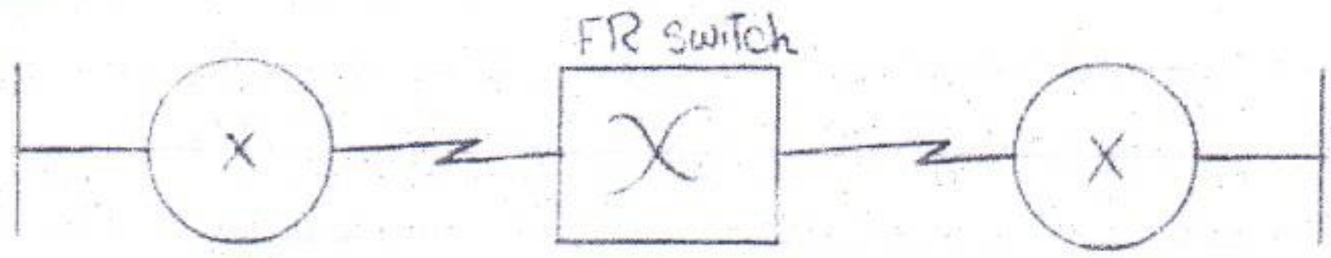
Frame Relay :

It is point-to-multiple packet switching technology based on PVCs (Permenant Virtual Circuits) ...

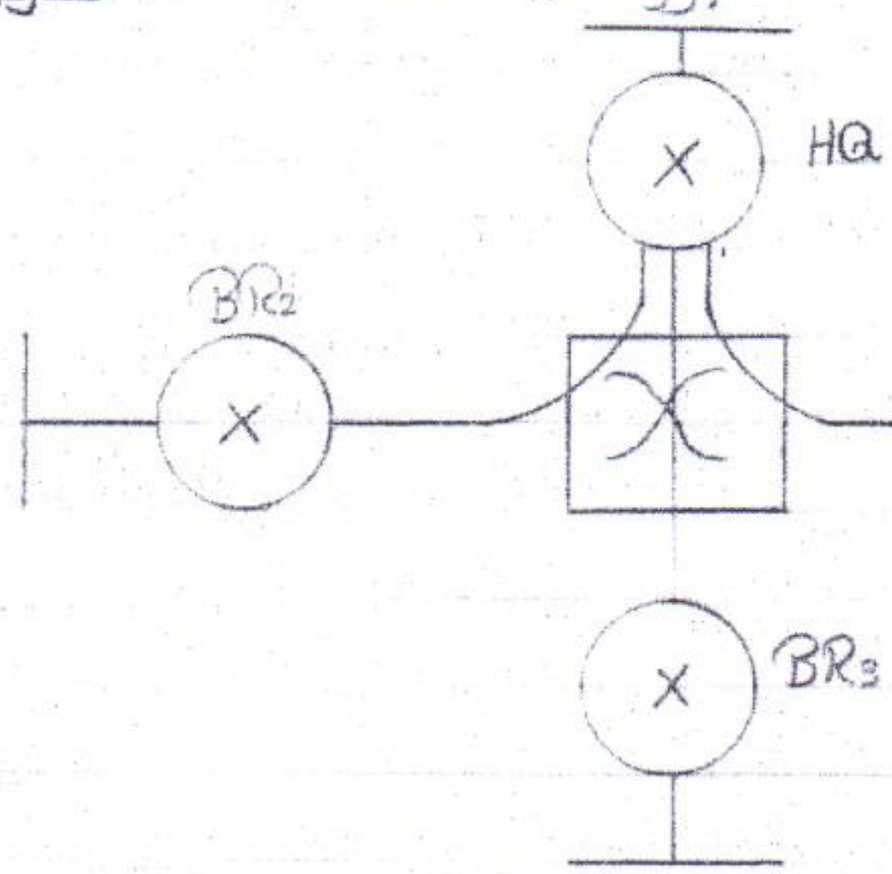
Microsegmentation in WAN

Frame Relay Topology :

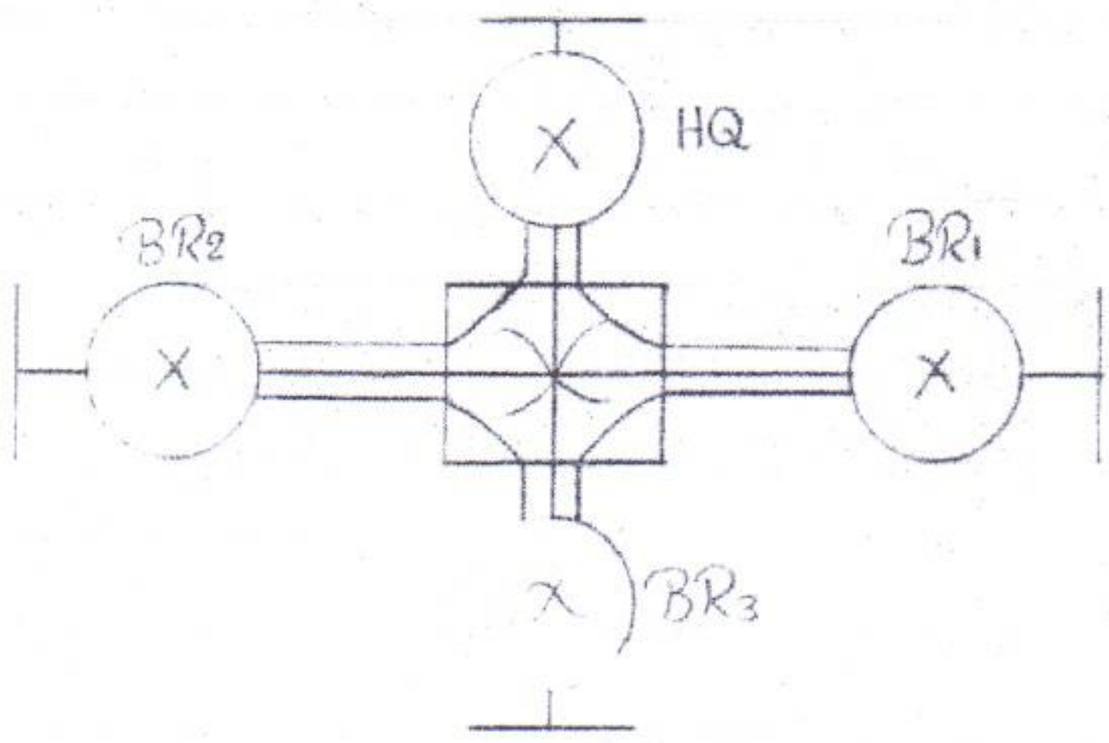
- **Point-to-Point :**



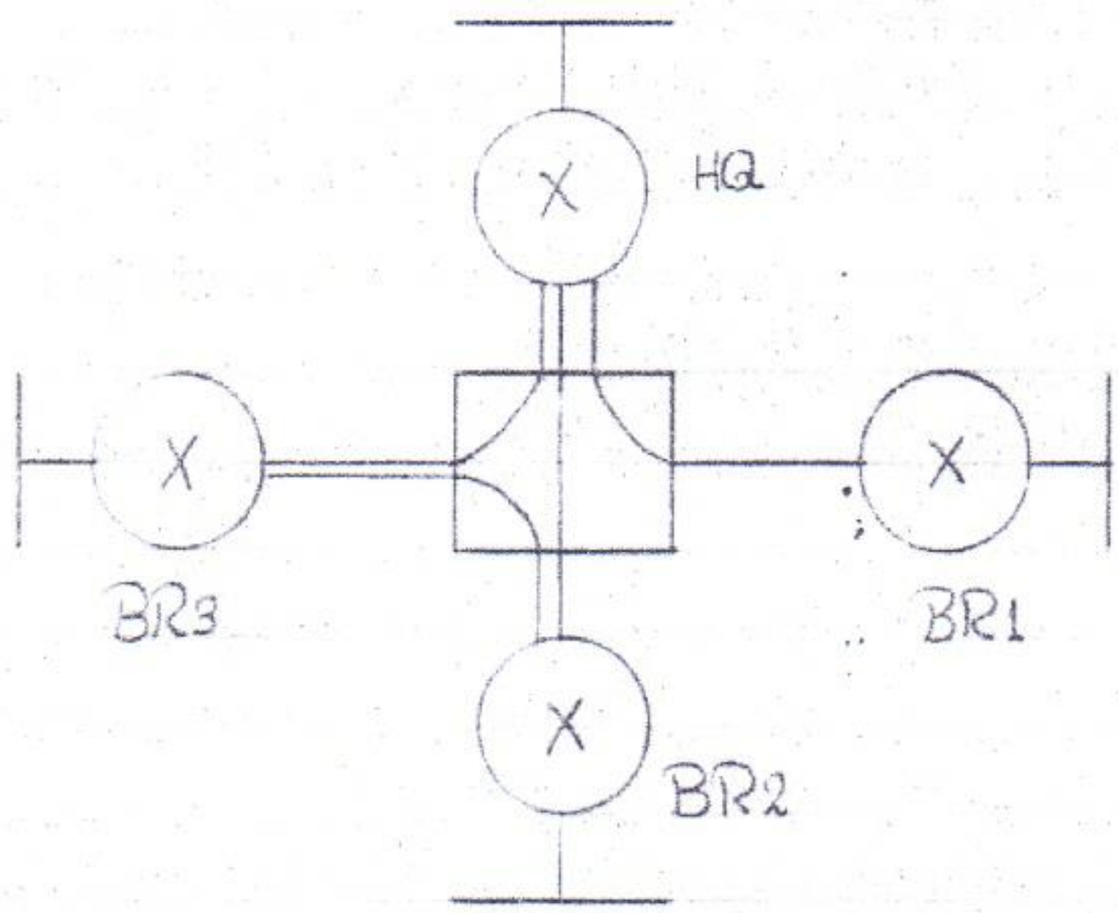
- **Star topology :** (hub & spoke topology)



- **Full mesh Topology :**



Partial mesh :



Frame Relay Encapsolation :

It is Called Link Access Procedure For FR (LAPF).

Flag	Address	Contral	Packet	CRC

- PVC ID
- For X.25 : 8-bit (X.25 number)
- For FR : 10-bit (DLCI - Data link Circuit ID) "0 : 1023" reserved 0 : 15 & 1023 .
- For ATM : 16-bit (VPI/VCI = Virtual Path ID/ Virtual Circuit ID) "0 : 65535" .

Cisco LAPF :

Flag	DLCI	Contral	Type	Packet	CRC

- 6 - IPV6
- 4 - IPV4

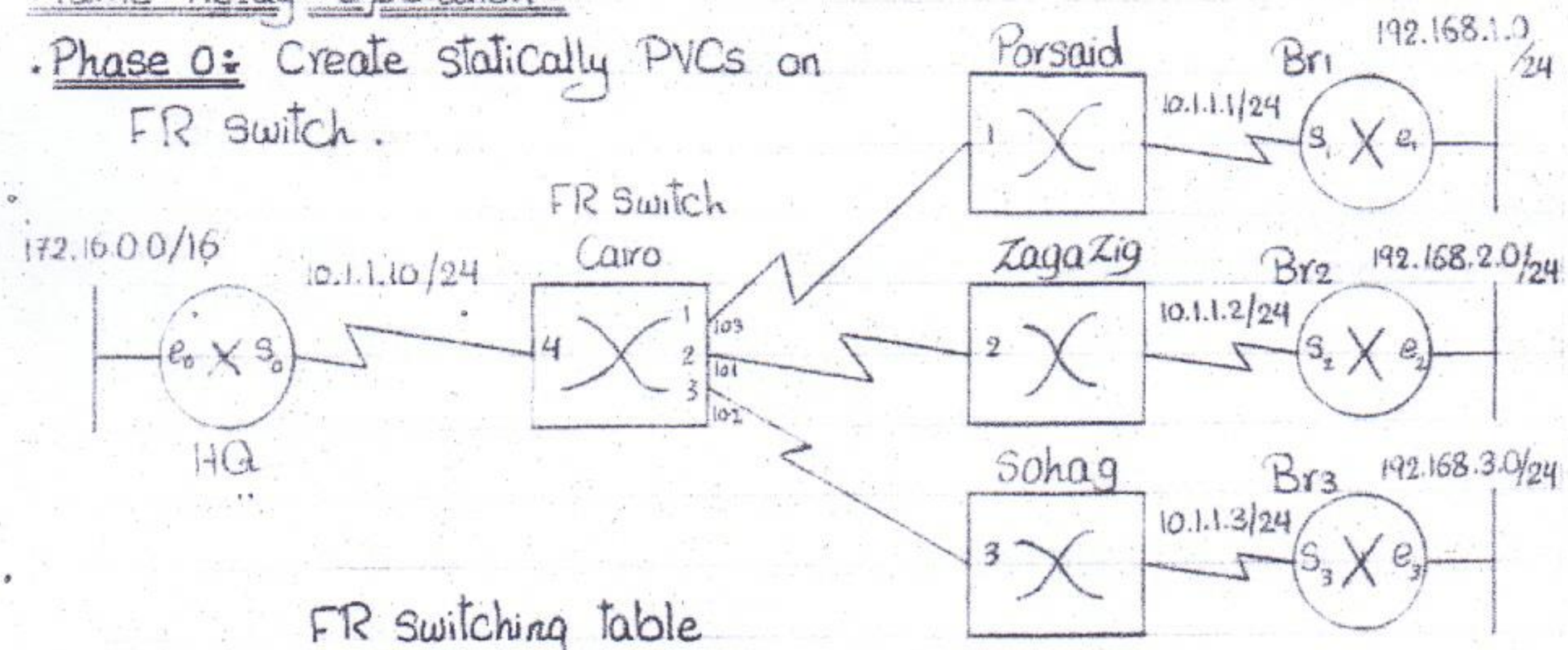
• IETF LAPF : standard

Flag	Address	Control	Type	Packet	CRC

Type:
- 60 - IPV6
- 40 - IPV4

Frame Relay Operation:

• **Phase 0:** Create statically PVCs on FR switch.



FR switching table
Cairo

In Port	In DLCI	Out Port	Out DLCI	CIR	Committed
4	101	2	101	2Mbps	Information
4	102	3	102	1Mbps	Rate = Clock
4	103	1	103	1Mbps	Rate

• **Phase 1 - Neighbor discovery:**

FR router will dynamically discovery its PVCs using LMI
- CISCO LMI
- ANSI LMI
- Q933a LMI

auto LMI discovery Cisco
"local Management Interface"

Phase 2 - IP discovery:

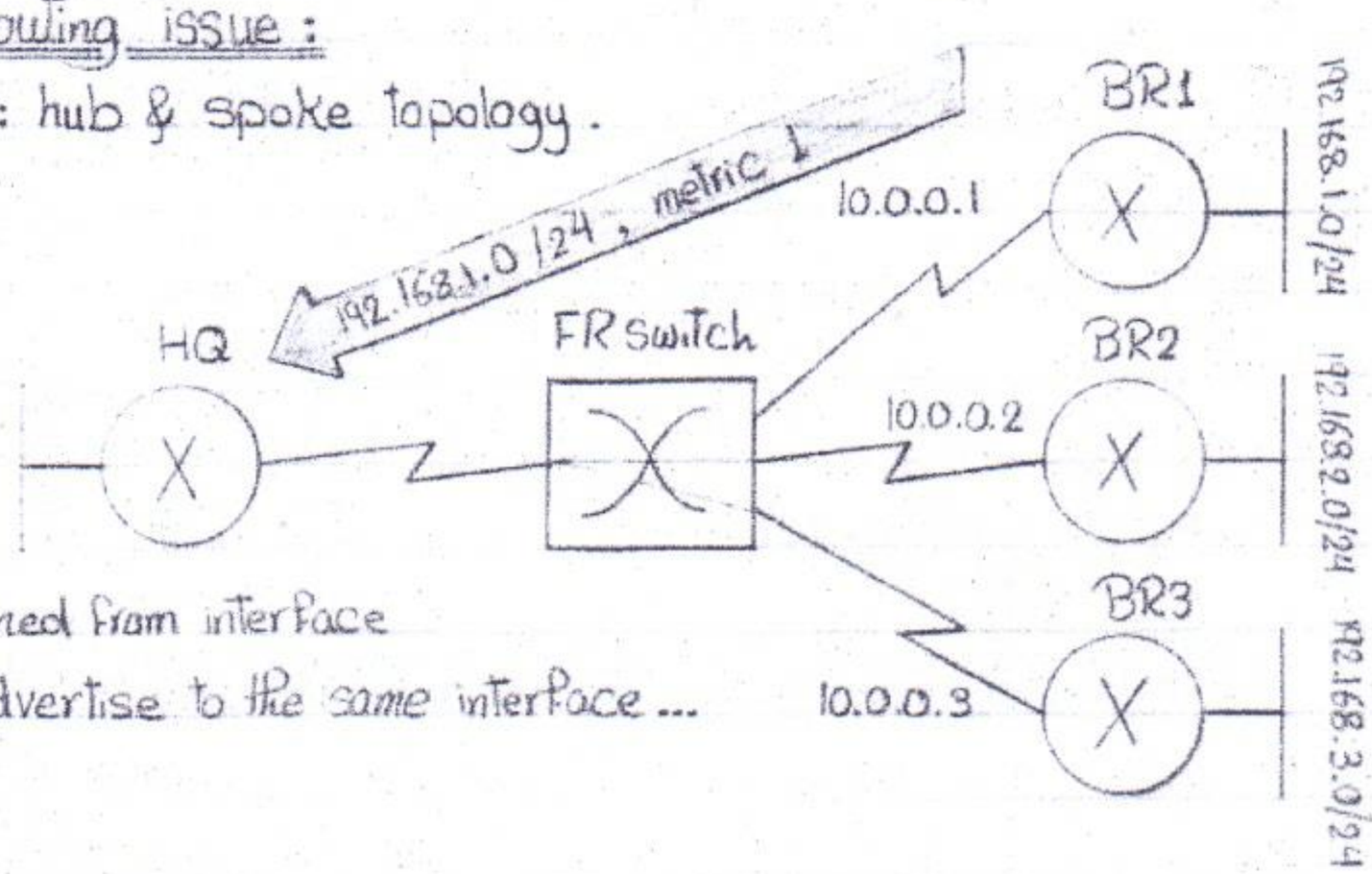
FR router map DLCI VS next hop IP using IARP "Inverse ARP".

FR map

DLCI	IP
101	10.1.1.2
102	10.1.1.3
103	10.1.1.1

Frame Relay routing issue:

star topology : hub & spoke topology.



Router learned from interface

can't be advertise to the same interface ...

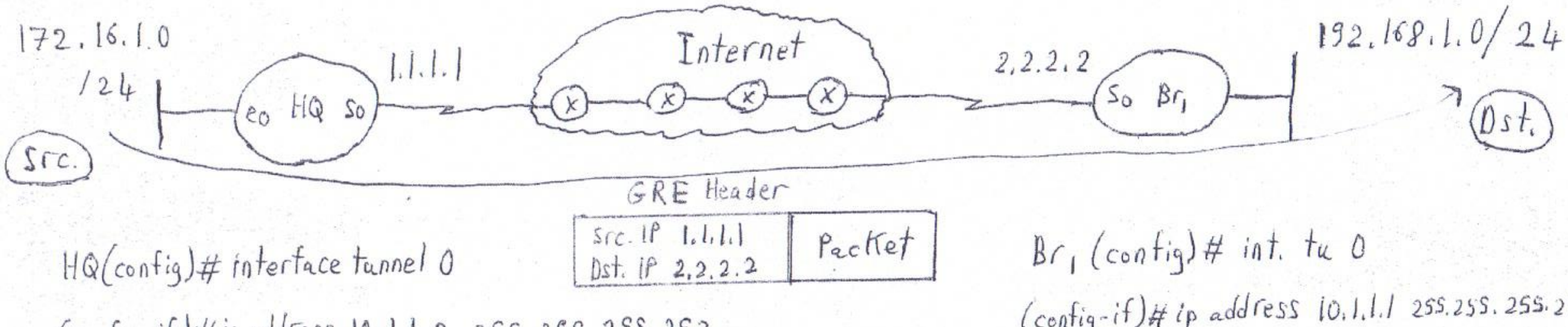
Solution:

- Disable Split horizon.
- Use static Routing.
- Use full mesh topology.
- Divide main interface into sub interfaces (Point-to-Point).

Session 9/1

VPN (Virtual Private Network)

It is building private WAN (Enterprise = HQ/Branches) through public WAN (Internet)



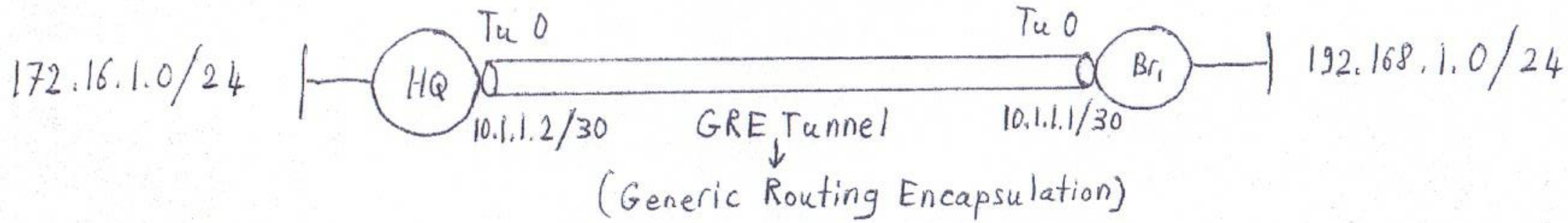
HQ(config)# interface tunnel 0
(config-if)# ip address 10.1.1.2 255.255.255.252
(" -if)# tunnel source 1.1.1.1
(" -if)# tunnel destination 2.2.2.2
(" -if)# tunnel mode gre
(" -if)# tunnel protection ipsec

default mode

Br1 (config)# int. tu 0
(config-if)# ip address 10.1.1.1 255.255.255.252
(" -if)# tunnel mode gre
(" -if)# tunnel source 2.2.2.2
(" -if)# tunnel destination 1.1.1.1
(" -if)# tunnel protection ipsec

Session 9/2

Point - to - Point



ipsec = ip packets security

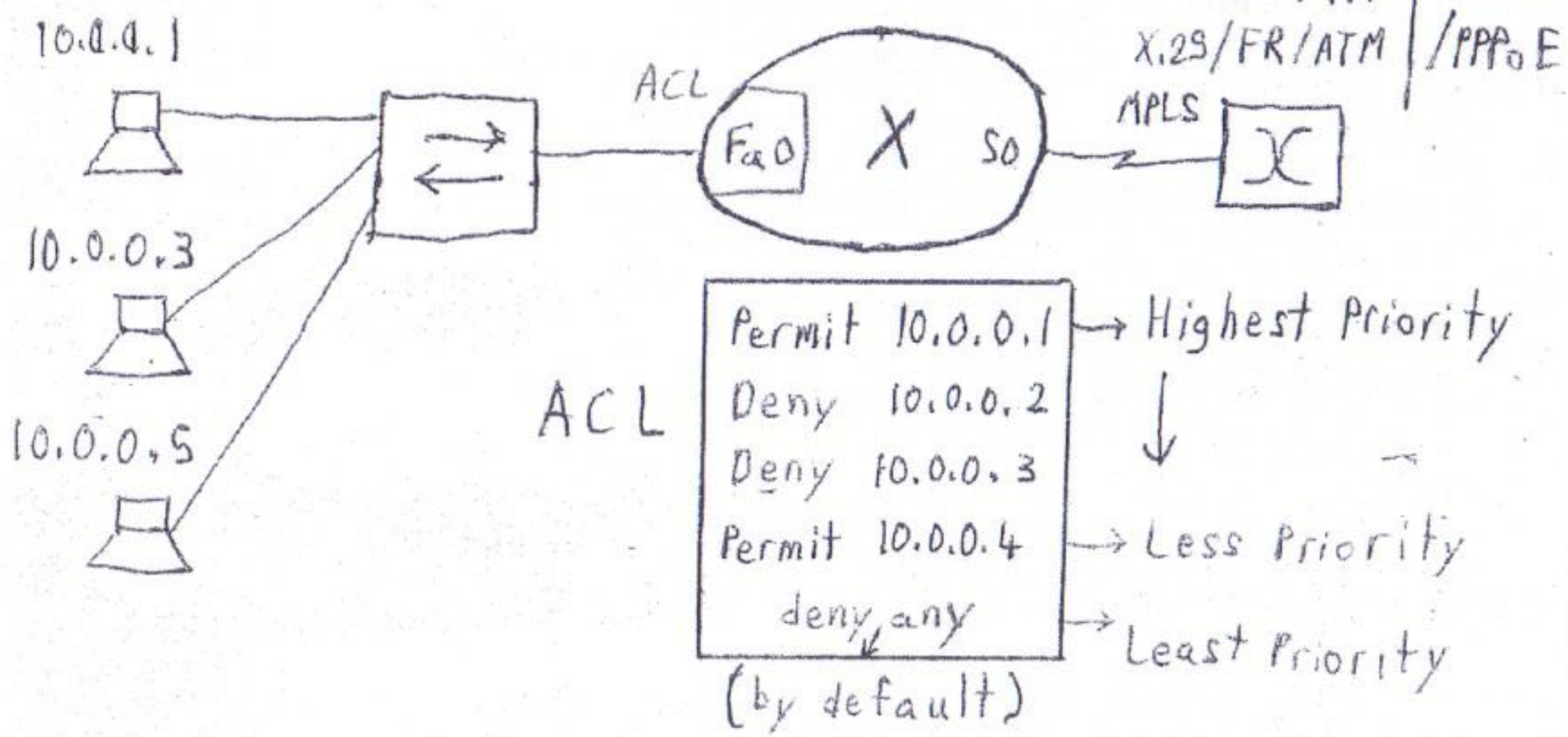
- **C** — Confidentiality
  - "Encryption"
  - DES : Data Encryption Standard
  - 3DES
  - AES : Advanced Encryption Standard
- **I** — Integrity
  - Data Copy Hashing
- **A** — Authentication
  - MD5
  - SHA
    (Secure Hash Algorithm)

Session 9/3

Router Security:

Access-List (Access Control List)

PPPoE: Public WAN FR: Private WAN



1. Create ACL
2. Activate ACL on Interface

IP ACL Types

* Standard IP ACL:

- Filter Data based on Src. IP only

- Numbered: ACL # (1-99) & (1300-1999)
  old
- Named: Any name
  new

* Extended IP ACL:

- Filter Data based on:

  Src. IP
  Dst. IP ⟶ Facebook, Youtube, ---
  Protocol ⟶ IPsec, GRE, ---
  Application ⟶ FTP, HTTP, ---

- Named: Any name
  new
- Numbered: ACL # (100-199) & (2000-2699)
  old

Session 9/4

Standard IP ACL:

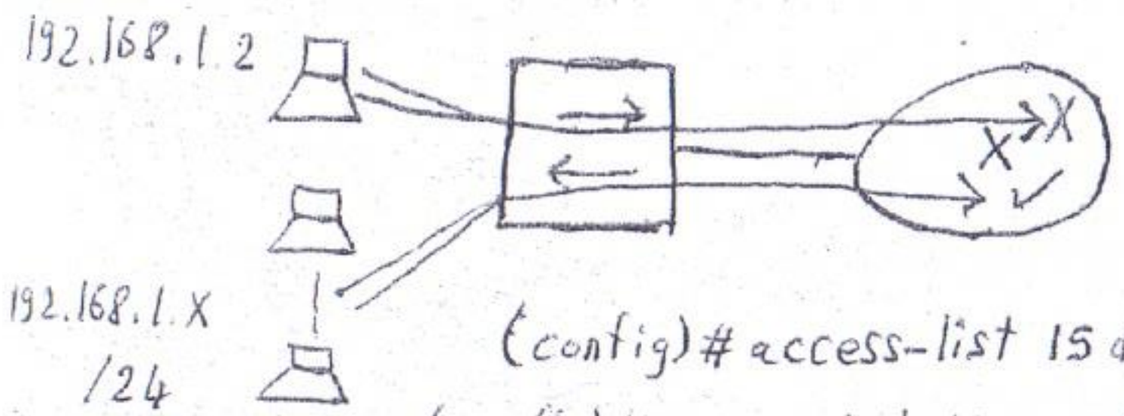
1 Create ACL: #show access-list

- Numbered:

(config)# access-list 1-99 {Permit/Deny} Src.IP W.C.M

default 0.0.0.0

* Wild Card Mask: Inverted Mask { 0 → exact match, 1 → don't care



(config)# access-list 15 deny 192.168.1.2 0.0.0.0

(config)# access-list 15 permit 192.168.1.0 0.0.0.255

If Subnet Mask /26 = 1111 1111. 1111 1111. 1111 1111. 1100 0000 = 255.255.255.192

Wild Card Mask = 0000 0000. 0000 0000. 0000 0000. 0011 1111 = 0.0.0.63

(= 255 - subnet mask)

- Named:

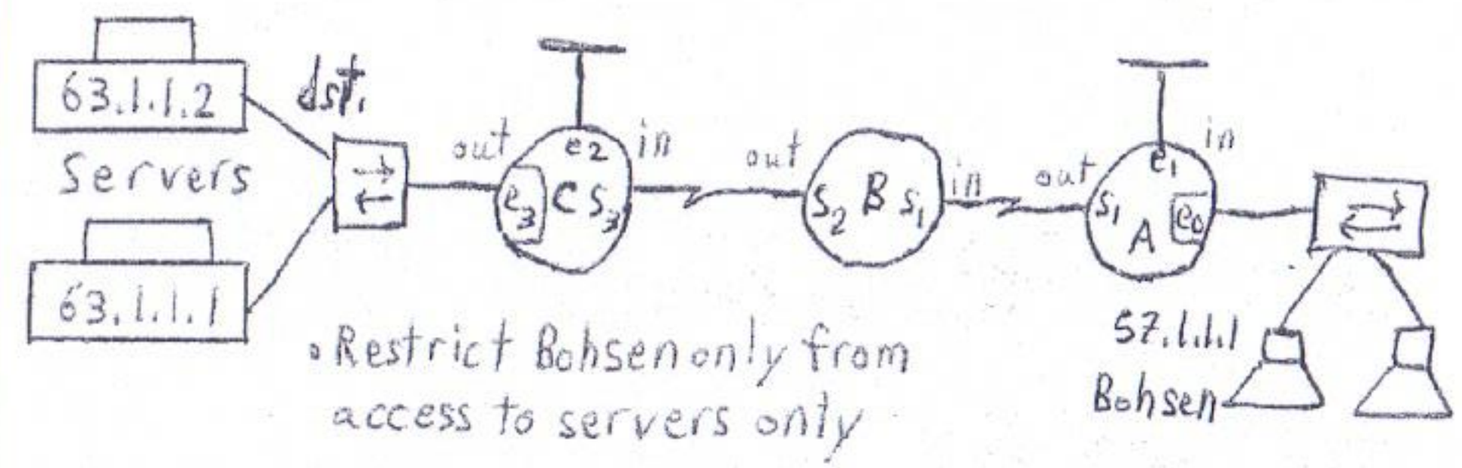
(config)# ip access-list standard name

(config-std-nad)# {Permit/Deny} src. ip w.c.m

2 Activate ACL: # show ip interface

(config)# interface ___

(config-if)# ip access-group # or name {in/out}



• Restrict Bohsen only from access to servers only

C(config)# ip access-list standard Bohsen

(config-std-nad)# deny 57.1.1.1 0.0.0.0

(config-std-nad)# permit any ⇒ 0.0.0.0 255.255.255.255

C(config)# int e3

(config-if)# ip access-group Bohsen out

Rule 1: ACL should contain at least 1 permit

Rule 2: Std ACL should be placed as close as possible to dst.

Session 9/5

Extended IP ACL:

- Filter Data based on
  - L3: IP_{v4}, IP_{v6}, ICMP, ...
  - L4: UDP, TCP
  - Src. IP / Dst. IP
  - L7 Application (name/port)

1 Create ACL: # show access-list

- Numbered:

(config)# access-list 100-199 {Permit/Deny} IP/TCP/UDP/.... (Any Protocol)

L3/L4 Protocol

src. ip w.c.m dst. ip w.c.m [eq. Port no./App name] (eq: equal)

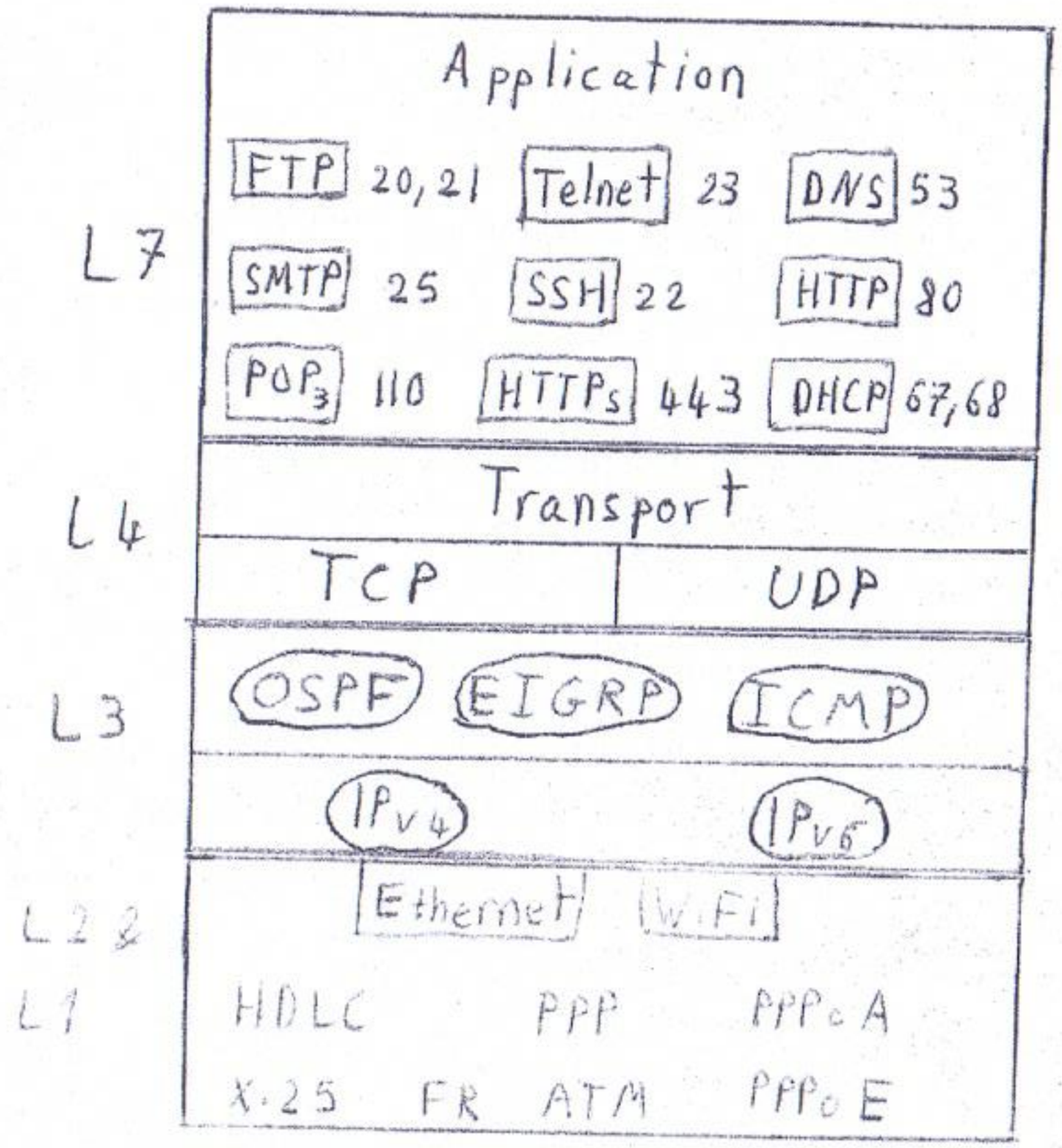
- Named:

(config)# ip access-list extended name

(config-ext-nacl)# {Permit/Deny} L3/L4 Protocol

src. ip w.c.m dst. ip w.c.m [eq. APP/Port no.]

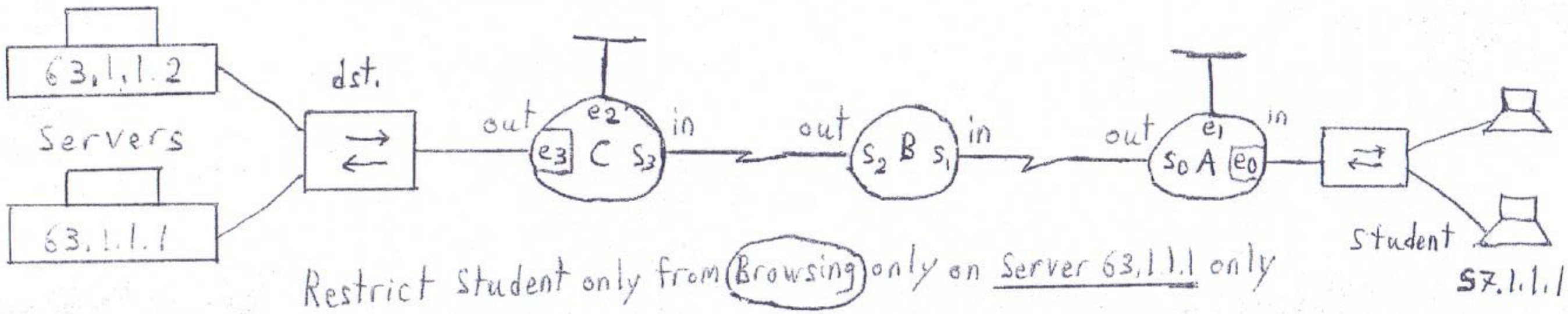
Application



* TCP: FTP - SMTP - POP_3 - Telnet - SSH - HTTP - HTTPs

* UDP: DNS - DHCP

Session 9/b



Restrict student only from Browsing only on Server 63.1.1.1 only

A(config)# ip access-list extended student

(config-ext-nacl)# deny tcp 57.1.1.1 0.0.0.0 63.1.1.1 0.0.0.0 eq 80

(src. ip, dst. ip, www)

(config-ext-nacl)# permit IP any any

(src, dst)

A(config)# interface e0

(config-if)# ip access-group standard in

Rule 3: Ext. ACL should be placed as close as possible to Src.

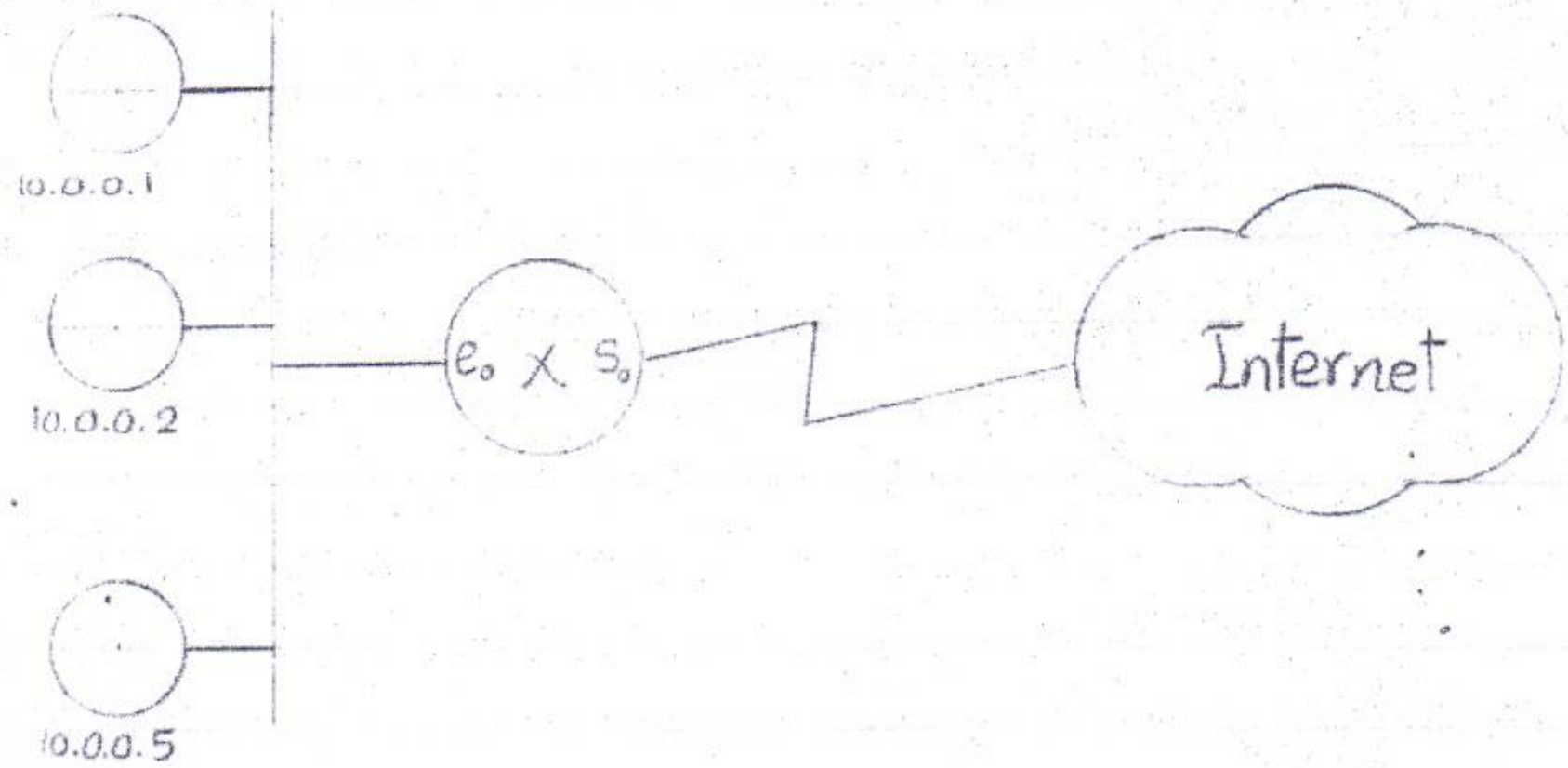
↓

To save Resources

Rule 2 → dst.

Rule 3 → src.

Router Security - ACL (Access Control List) :



1. Create ACL :

Permit	10.0.0.1	Highest Priority
Deny	10.0.0.2	
Deny	10.0.0.3	
Permit	10.0.0.4	Low Priority
Deny	any	least priority written by router (imaginary line)

اللى مش مكتوب
مش بيكتب

2. Activate list on interface .

3. IP ACL Types :

IP Standard ACL		IP extended ACL	
old	New	old	New
numbered	name	numbered	name
1:99 or 1300:1999	any name	100:199 or 2000:2699	any name
Filter based on Source IP only		Filter based on Protocal or SRC IP & DST IP or Application	

IP standard ACL (IOS software):

- It filters data based on source IP only.

1. Create list:

- numbered.

(Config) # access-list 1:99 {permit/deny} SRC IP [WCM]

→ (Config) # access-list 15 deny 192.168.1.2 0.0.0.0 one IP
→ (Config) # access-list 15 permit 192.168.1.0 0.0.0.255 Rang IPs

- name.

(Config) # ip access-list extanded or standard name
(Config-std-nacl) # {Permit/Deny} SRC IP [WCM] → Option default 0.0.0.0

→ (Config) # ip access-list standard Cisco
(Config-std-nacl) # deny 192.168.1.2 0.0.0.0
→ (Config) # ip access-list standard Cisco
(Config-std-nacl) # permit 192.168.1.0 0.0.0.255

2. Activate list on interface:

(Config) # int e0
(Config-if) # ip access-group # or name {in/out}

(Config) # int e0
→ (Config-if) # ip access-group 15 in
OR → (Config-if) # ip access-group Cisco in

IP extended ACL :

Filters data based on TCP|IP Protocal or source IP & Destination IP or Application name & port no. (optional) ...

1. Create ACL :

. numbered .

(Config)# access-list 100:199 {permit/deny} TCP/IP Protocal src IP+WCM dst IP+WCM [eq. Port no. / App. no.] ← option

→ (Config)# access-list 101 permit IP 0.0.0.0 255.255.255.255
any

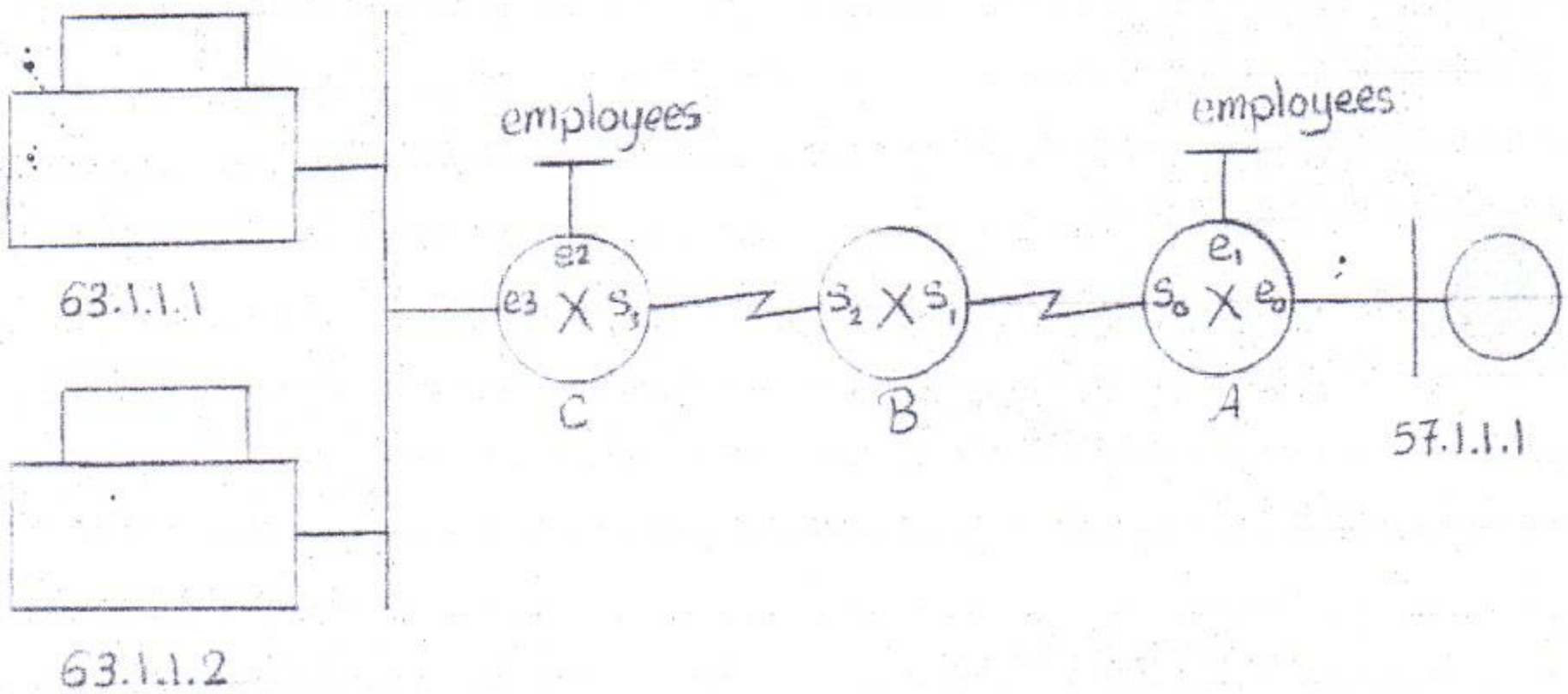
→ (Config)# access-list 101 deny TCP host 57.1.1.1 host 63.1.1.1
eq 80 / WWW

. name .

(Config)# ip access-list extended name
(Config-ext-nacl)# {permit/deny} TCP/IP Protocal src IP + WCM dst IP + WCM [eq. Port no. / App. no.]

(Config)# ip access-list extended Cisco
→ (Config-ext-nacl)# deny TCP host 57.0.0.1 host 63.1.1.1 eq. 80 / WWW
→ (Config-ext-nacl)# permit IP any any

Rule 1 : ACL should contain at least 1 permit.
Rule 2 : Standard ACL should be placed as close possible to dst.
Rule 3 : Extended ACL should be placed as close possible to Src.



ex1: Restrict Bohsen only from access to servers subnet only.

@ C router:

(Config) ※ ip access-list standard Bohsen
(Config-std-nacl) ※ deny 57.1.1.1 0.0.0.0 or host 57.1.1.1
(Config-std-nacl) ※ permit any
(Config) ※ int e3
(Config-if) ※ ip access-group Bohsen out
※ show ip interface
※ show access-list
※ show ip access-list

ex2: Restrict Bohsen only from browsing only on server 63.1.1.1 only.

@ A router:

(Config) ※ ip access-list extended Bohsen
(Config-ext-nacl) ※ deny TCP host 57.1.1.1 host 63.1.1.1 eq. 80/www
(Config-ext-nacl) ※ permit IP any any
(Config) ※ int e0
(Config-if) ※ ip access-group Bohsen in.

Session 10 / 1

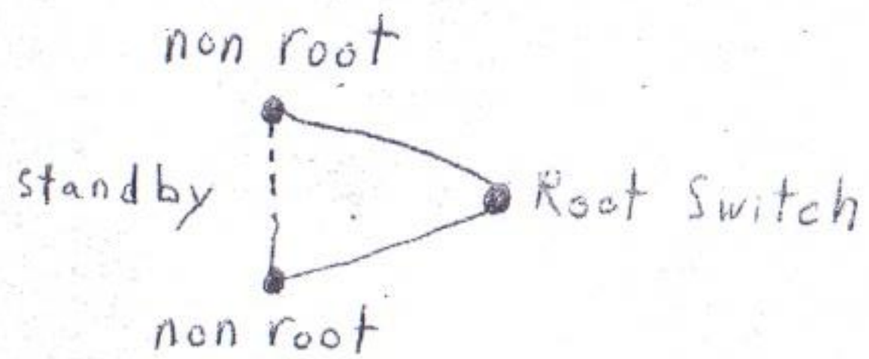
LAN Switching (Ethernet Switching)

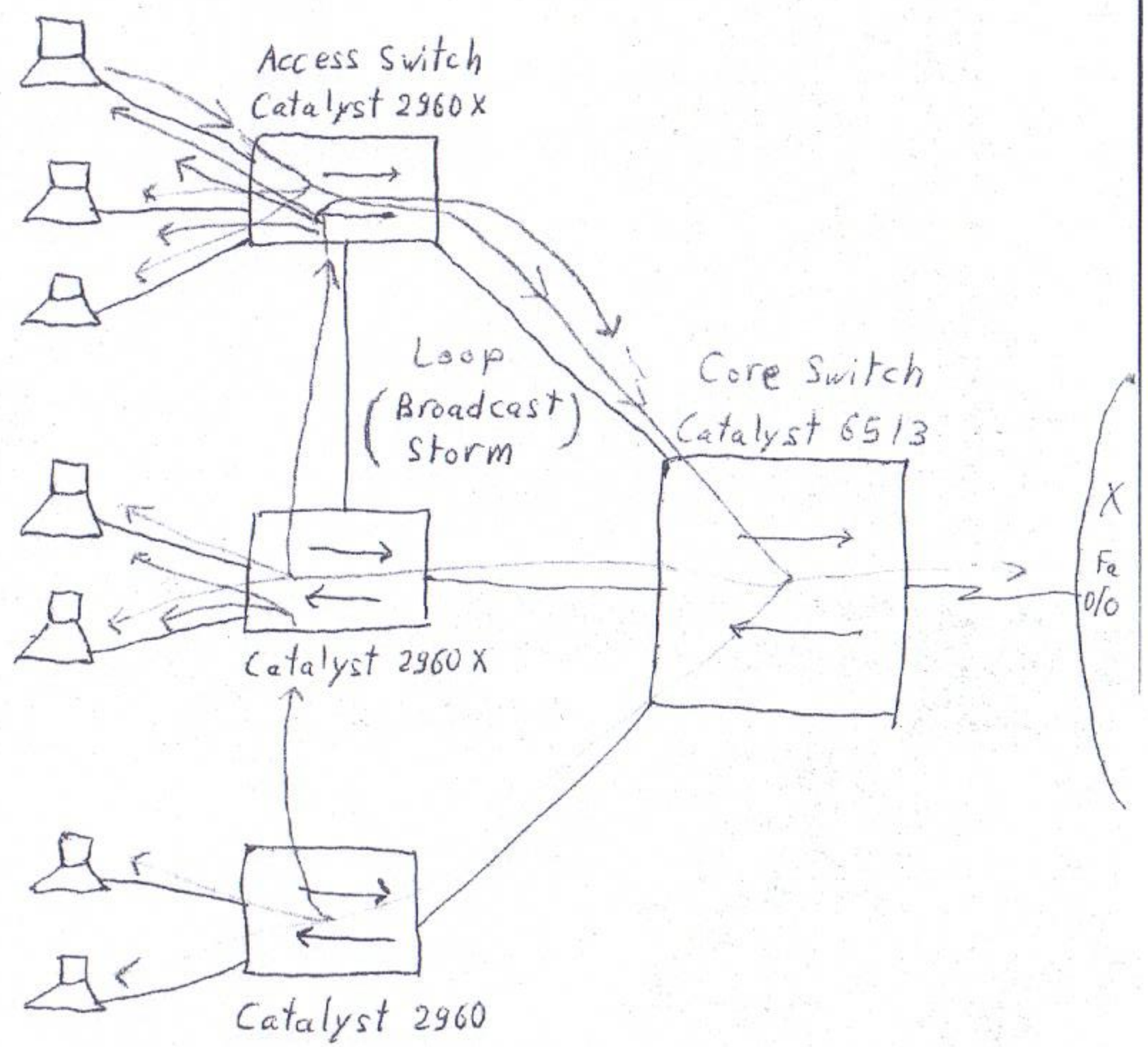
- STP ⟶ Star Topology

Spanning Tree Protocol (IEEE 802.1d)

d → dijkstra

- STA ⟶ Spanning Tree Algorithm





BUM ⟶ Flood

↓

Broadcast

DHCP ARP

Session 10/2

STP

@Startup: no need for configuration (Plug & Play)

1 Neighbor Discovery: Handshaking

Each Switch will send BPDU (Bridge PDU - Hello)

Switch Frame

Switch ID	Port ID	Accumulated Path Cost

2 Electing Root Switch: (Root Bridge)

Switch has the least switch ID

Switch Priority 0 – 65,535	System MAC
2 byte	6 Byte

default: 32,768

Core(config)# spanning-tree vlan 1-4094 priority less than 32,768

OR

Core(config)# spanning-tree vlan 1-4094 root primary

3 Electing Root Port (RP):

It is the best port on non root switch that can reach the root switch

RP is: CSP

A Port having least accumulated path cost based on Bandwidth BW

B Port connected to least Switch ID

C Port connected to least Port ID

4 Electing Designated Port (DP):

It is the best port on each link that can reach the root switch

DP is: least CSP

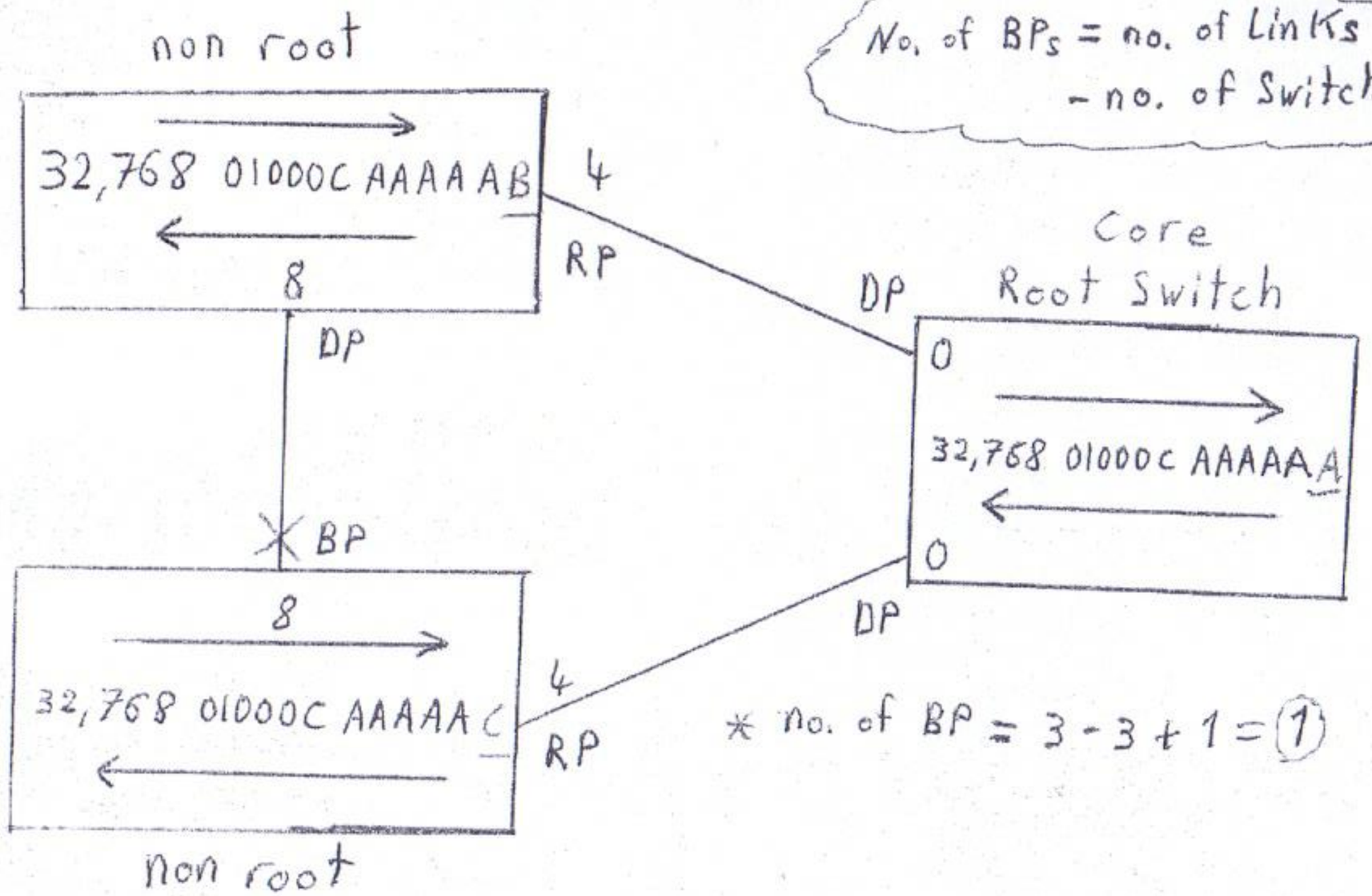
5 Choosing Blocked Port (BP):

Ports that are neither RP nor DP

Session 30/3

(A) < (B) < (C)
10 11 12

No. of BPs = no. of Links − no. of Switches + 1



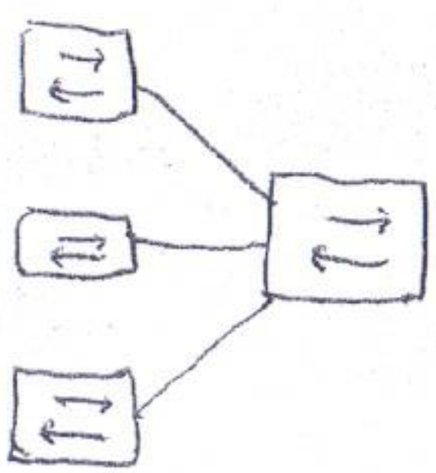
* no. of BP = 3 − 3 + 1 = (1)

- Assume all links between switches are giga Ethernet

IEEE

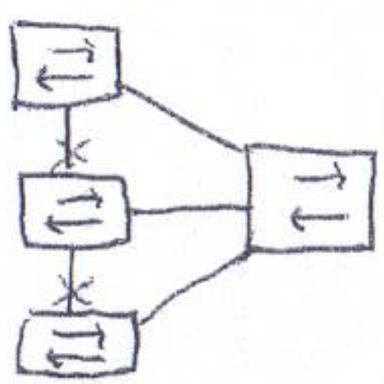
BW	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2
100 Gbps	1

ex:



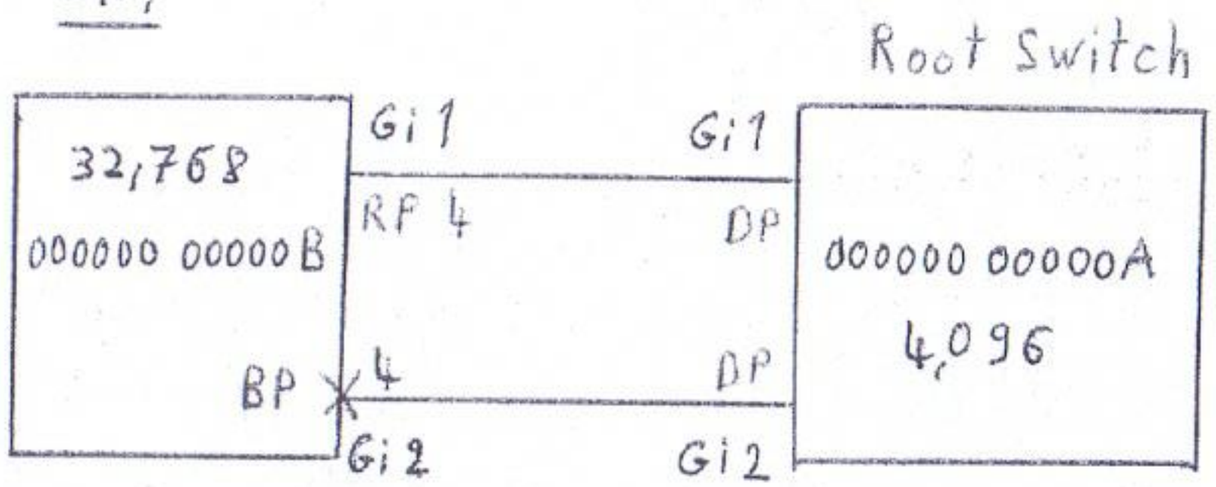
* no. of BP = 3 − 4 + 1 = (0)

ex:



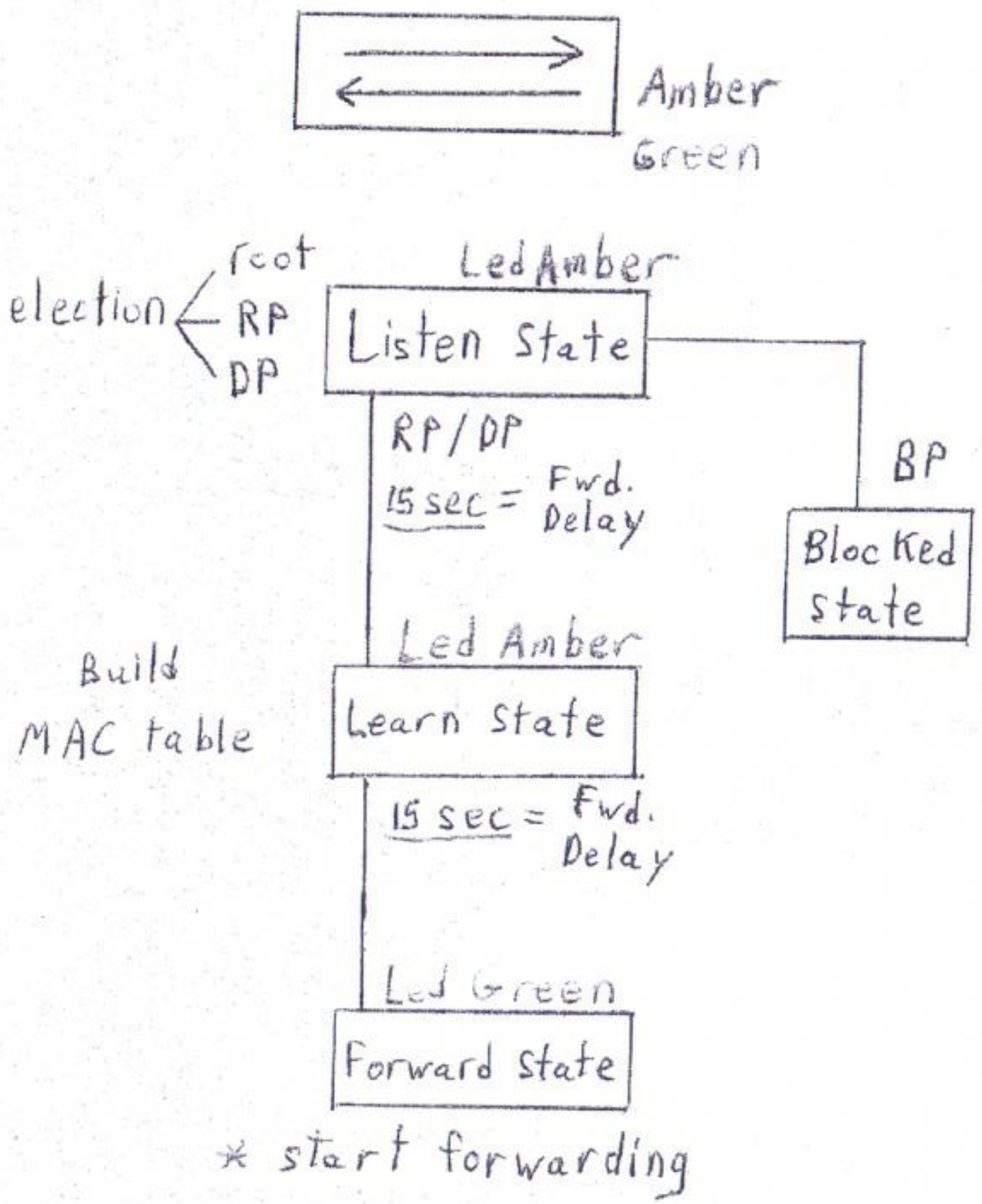
* no. of BP = 5 − 4 + 1 = (2)

ex:



Session 20/4

STP Port States:



* start forwarding

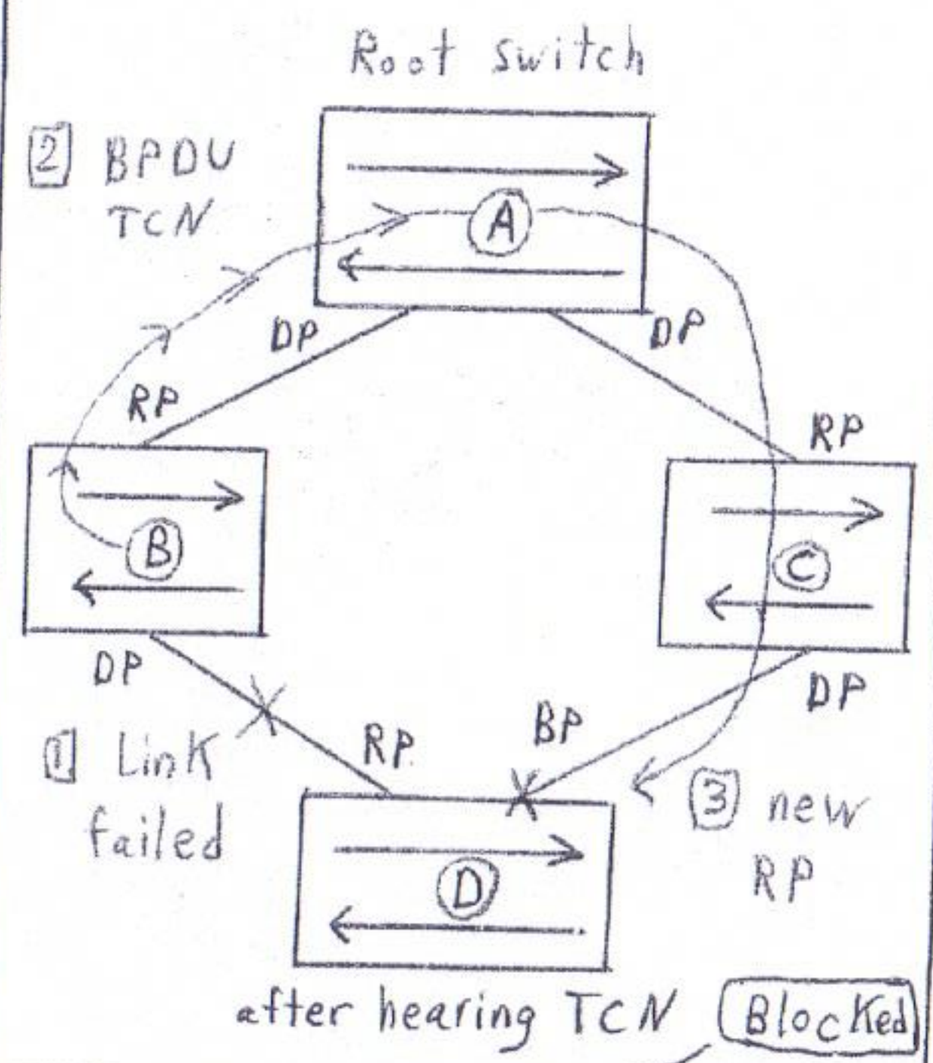
convergence time ≅ 30 sec

* Only root switch sends BPDU every 2 sec.

@ change!

1 Direct change:

(Cable failure)



Listen 15 sec

new RP

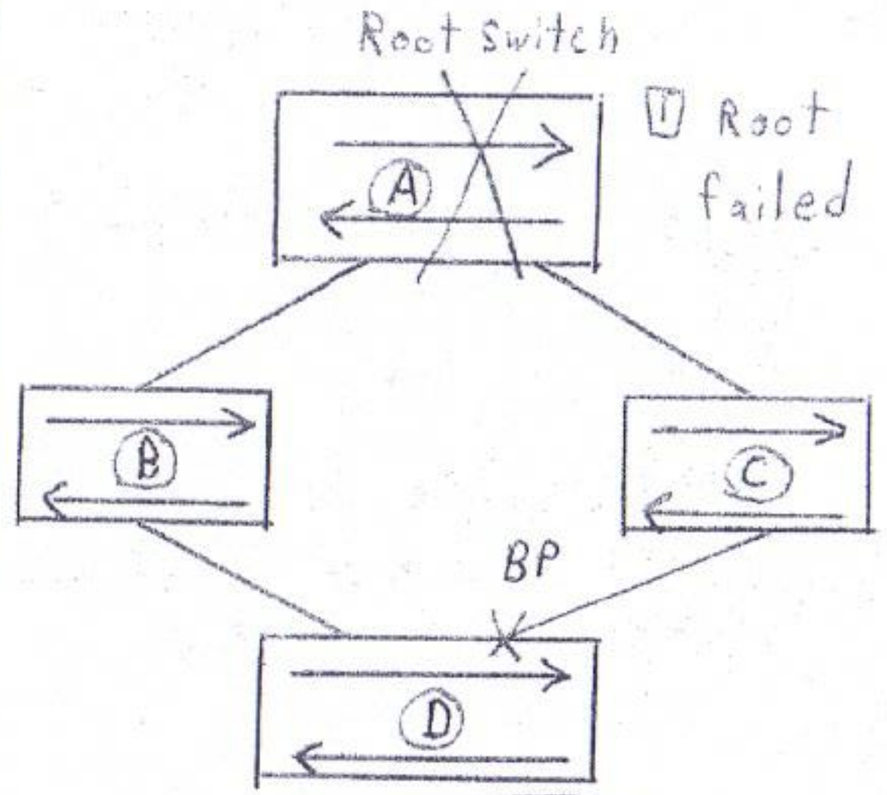
Learn 15 sec

Forward

reconvergence time ≅ 30 sec

TCN: Topology Change Notification

2 Indirect change: (root switch failure)



15 sec

Listen

max age (10 hello) = 20 sec

Blocked

15 sec

Learn

Forward

Convergence time = 50 sec

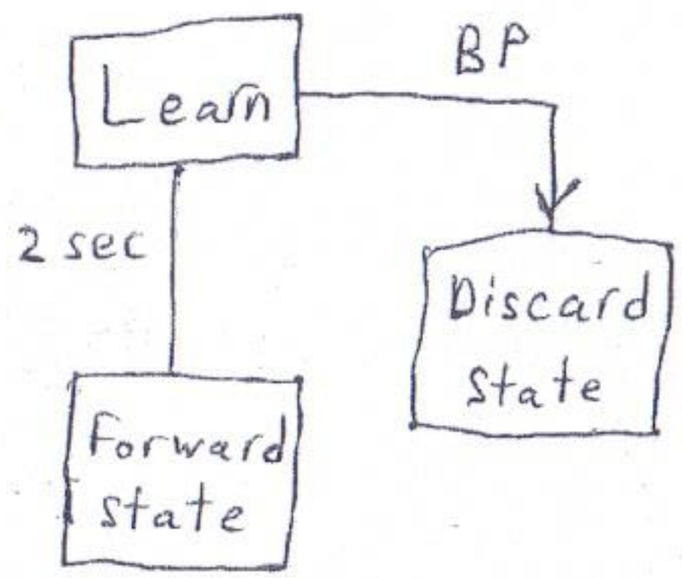
Enhanced STP-Cisco

Session 10 / 5

RSTP (Rapid STP) = IEEE 802.1w = STP v2

1. They introduced new states

- election
- build MAC table



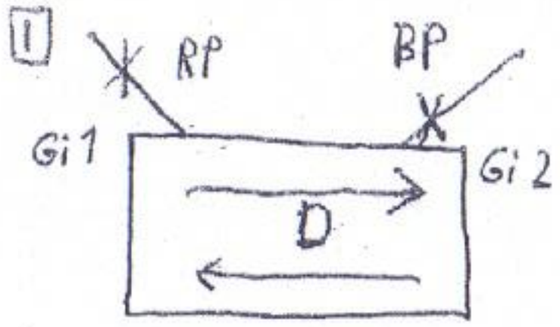
convergence time ≅ 2 sec

2. If root switch failed (3 hello = 6 sec)

convergence time ≅ 8 sec

3. They introduced Alternate Port & BackUp Port for each RP & DP.

1



(all RP) → new RP

Topology Table

1

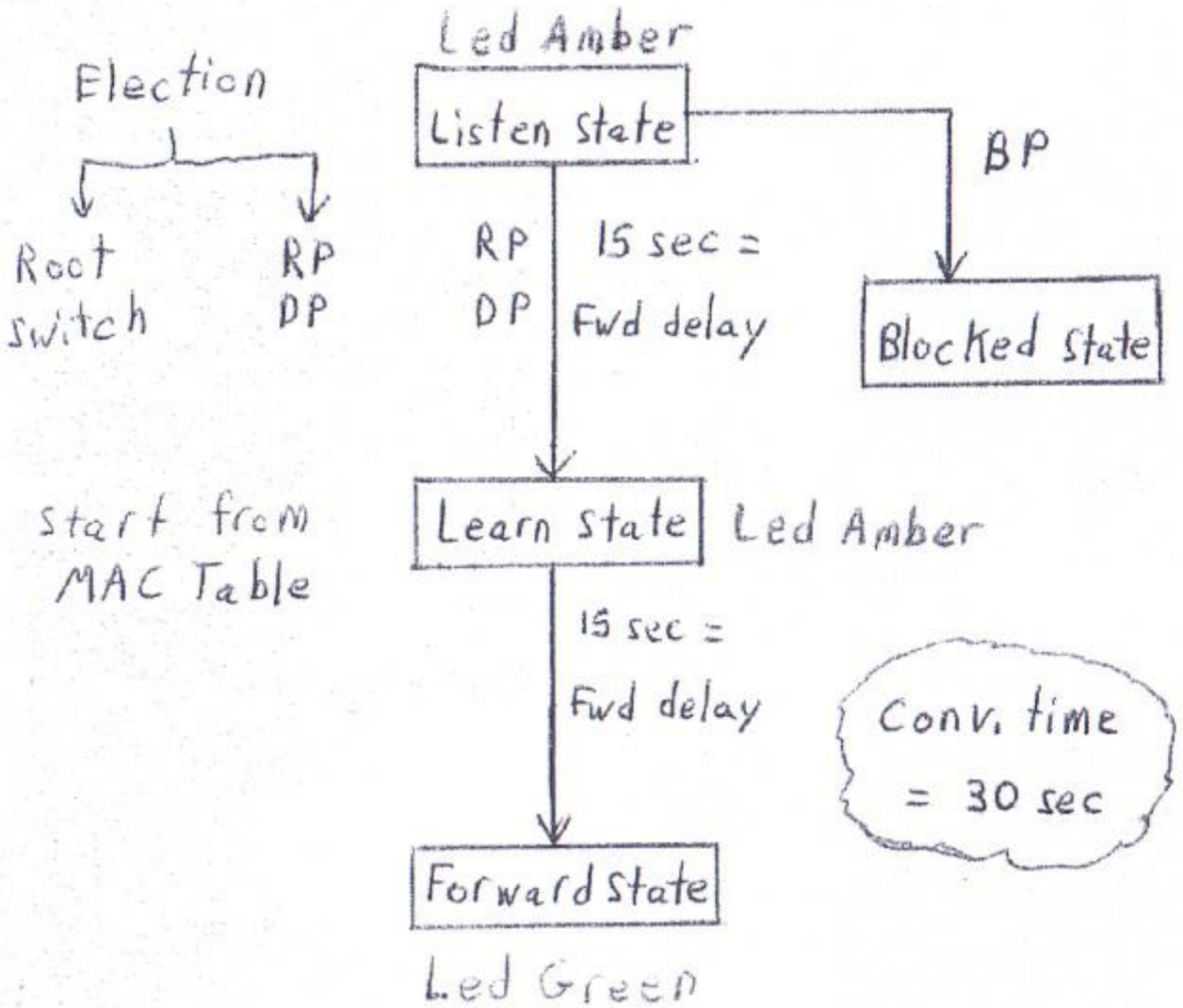
~~Gi1 is RP~~
Gi2 is ~~all RP~~ →

Convergence time ≅ 0 sec

Session 10 /6

STP States:

Led Amber
↓
Led Amber
↓
Led Green



@ Convergence:

only root switch send BPDU every 2 sec

STP Portfast:

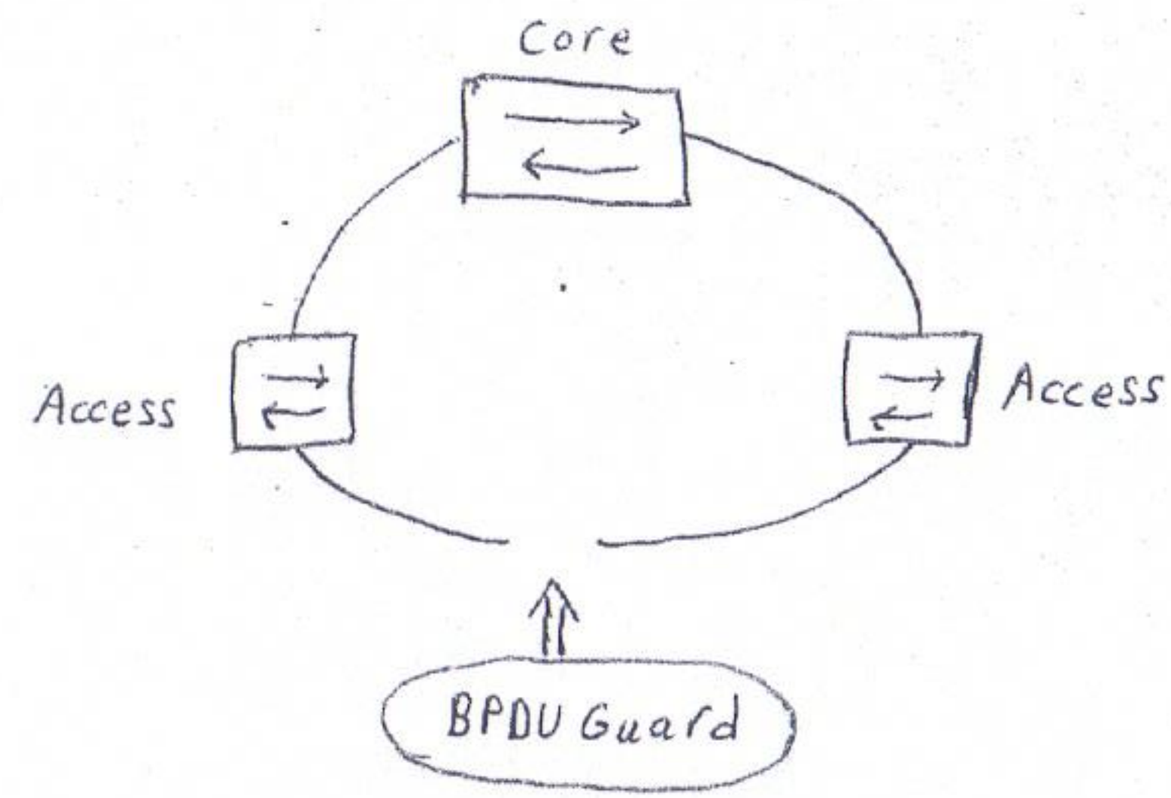
- Port that jumps to forward state at once
- Ports connected to end device

(config)# interface range fa 1-24

(config-if-range)# spanning-tree portfast

(config-if-range)# spanning-tree bpdu guard

* Port that receives bpdu will error-disable shutdown.

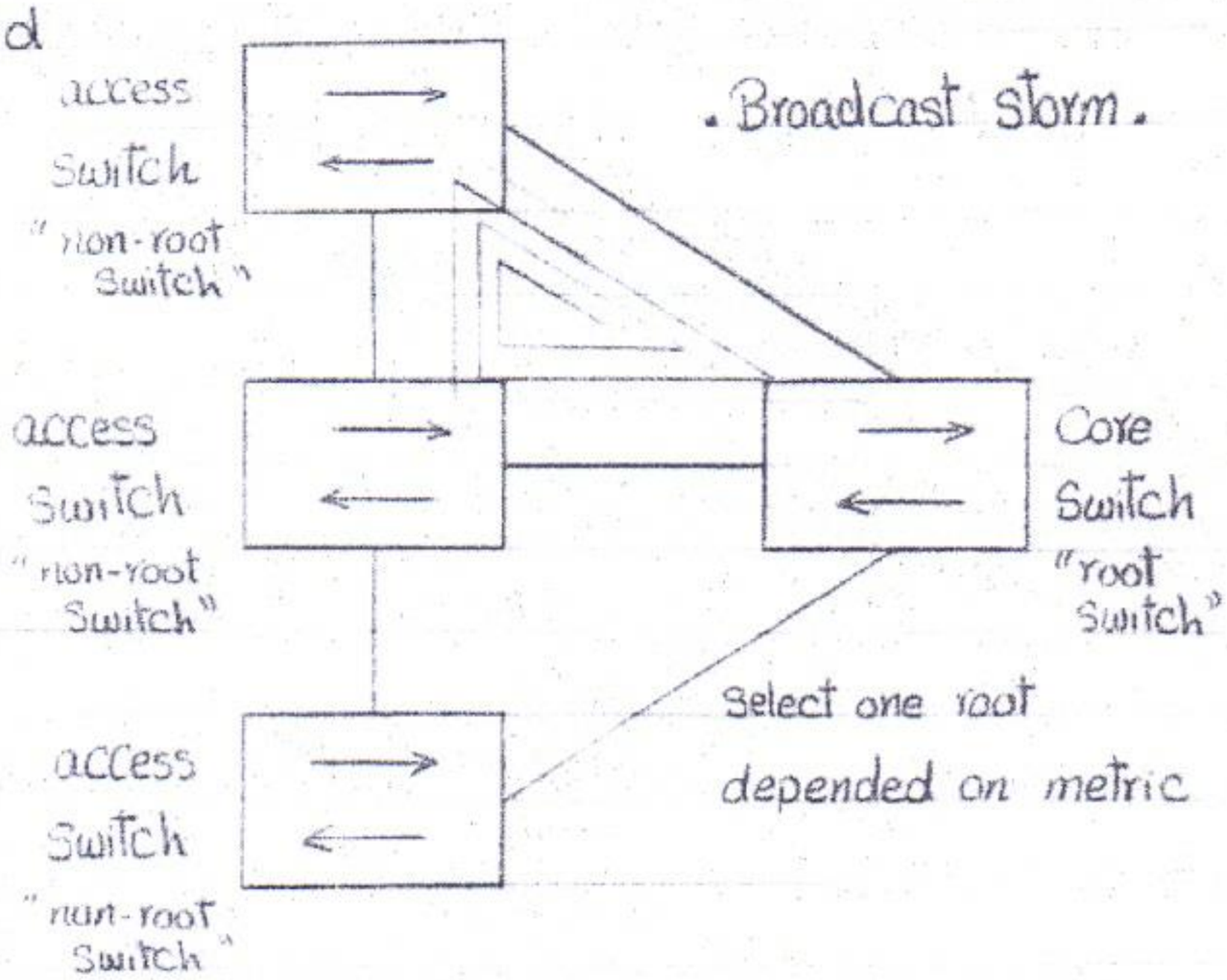


LAN Switching:

Spanning-Tree Protocal (STP):

By Dijkstra

STP → IEEE 802.1d



@ Start up: just after Configuration Plug & Play

1 Neighbor Discovery:

Hello Flooding = BPDU Flooding = Bridge PDU = L2 Frame

each 2 sec, each switch will send BPDU

3-byte

Switch ID	Accumulated Path Cost	Port ID

2 Electing Root switch:

Root switch is switch having least switch ID.

2 byte	6 byte
STP Priority 0-65535	System MAC

default: 32768

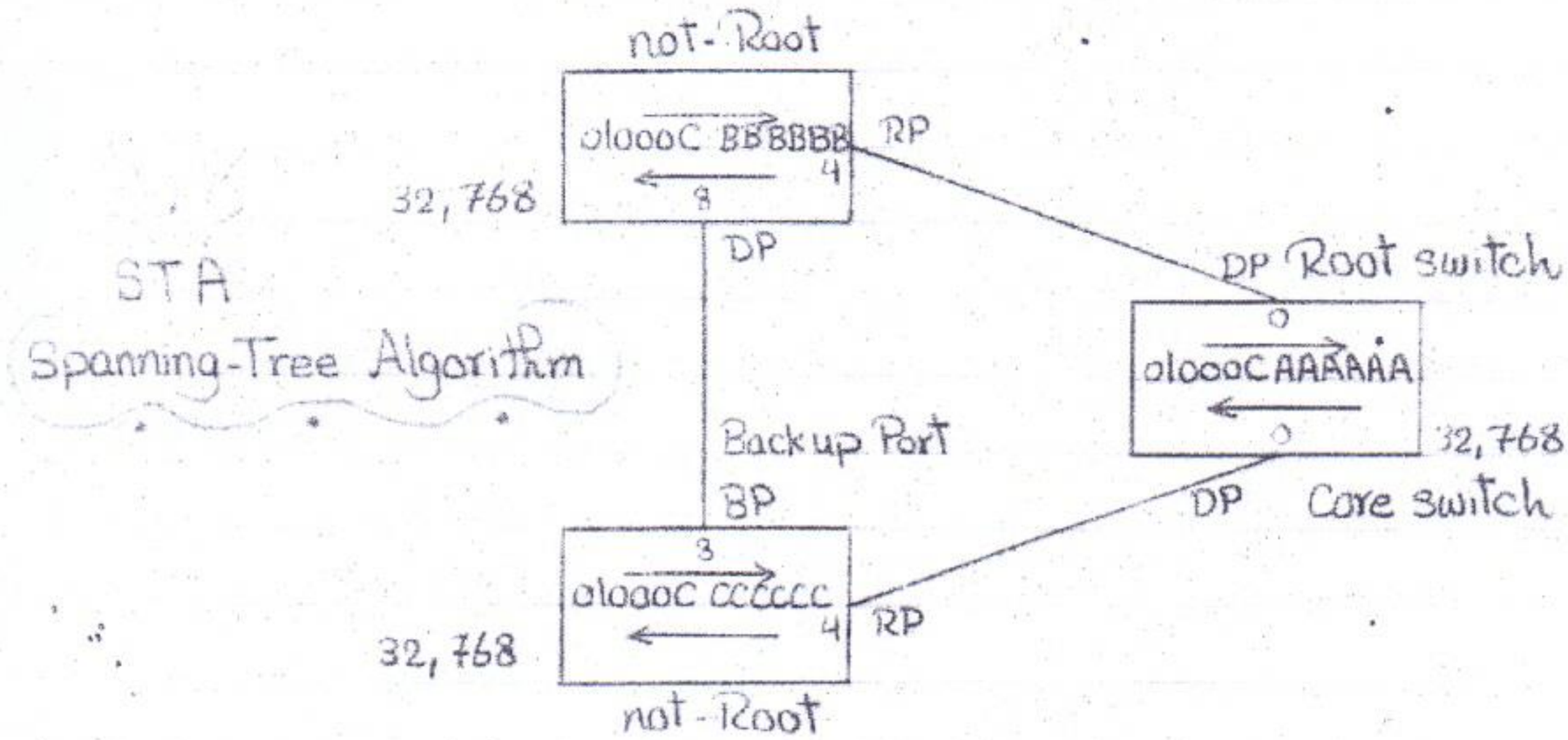
→ Switch ID 8 byte

@ Core switch :

→ (Config)# Spanning-tree vlan 1:4094 priority 0:65535

OR

→ (Config)# Spanning-tree vlan 1:4094 root priority



→ # Show spanning-tree

[3] Electing Root Port (RP) :

It is the best port on non-root switch that can reach the root switch.

RP is : least CSP

a. least accumulated path cost based on BW.

b. least switch ID.

c. least port ID.

BW	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Assume all links are Giga ethernet

4] Electing Designated Port (DP):

It is the best port on link that can reach root switch.

DP is: least CSP

a. least accumulated path cost based on BW.

b. least switch ID.

c. least Port ID.

5] Blocked Port (BP):

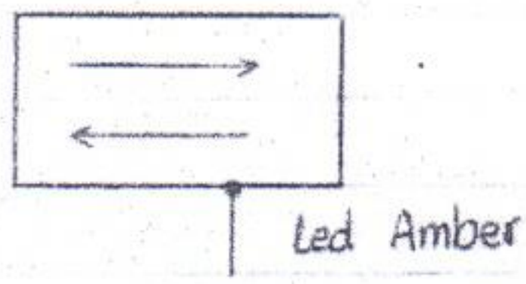
Ports that are neither RP nor DP.

Number of BPs = no. of links − no. of switches + 1.

STP Port states:

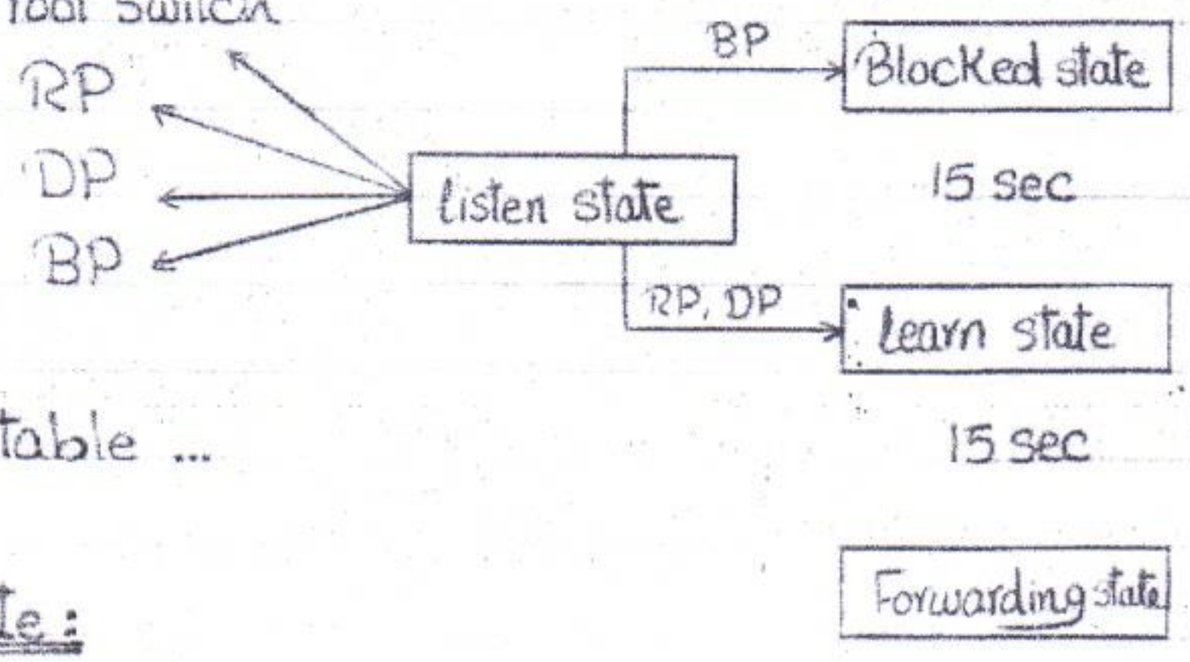
Disable state:

Led off & No Cable Connected ...



Blocked state:

Form election root switch



Learn State:

Forming MAC table ...

Forwarding state:

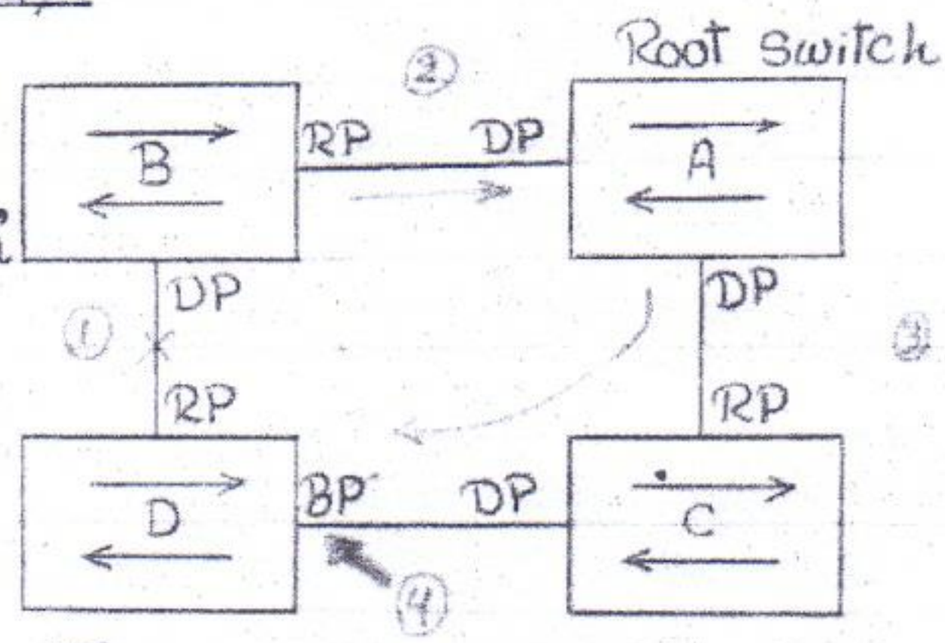
Start forwarding data ...

→ * debug spanning-tree events

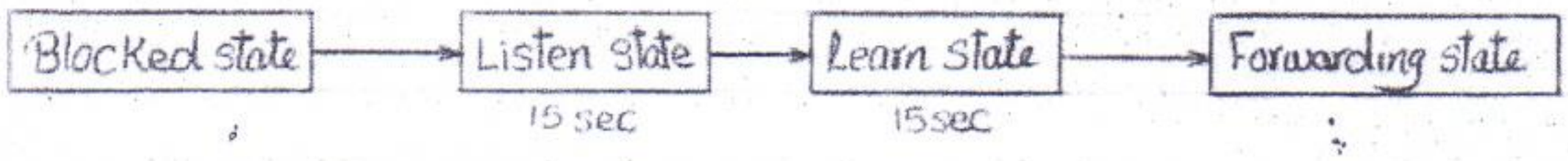
@ Change:

[1] Direct Change (link Failed):

1. Failed link.
2. BPDU TCN
   "Topology Change Notification"
3. BPDU TCN.
4. Change state from BP to RP.

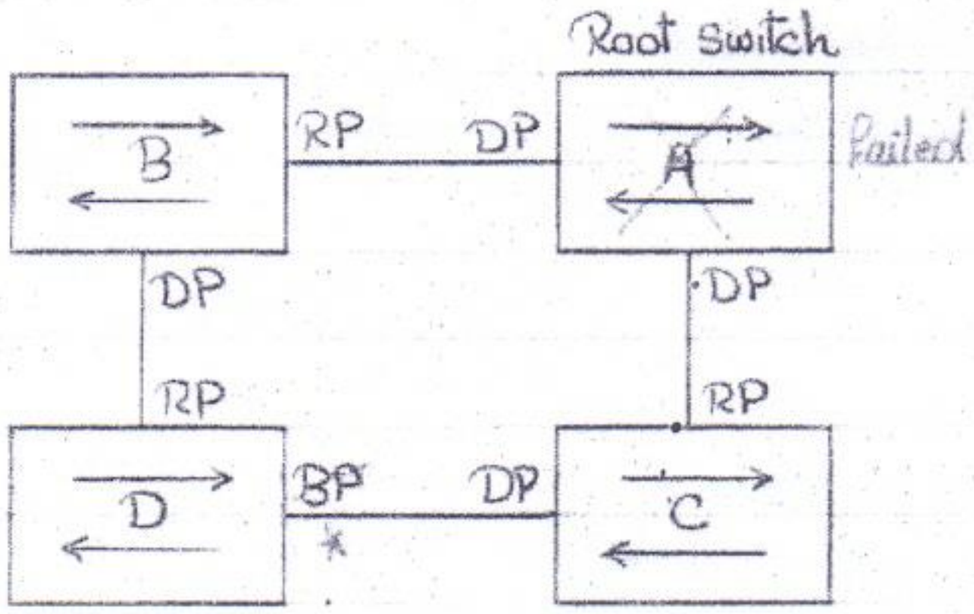


Conversion Time ≃ 30 sec



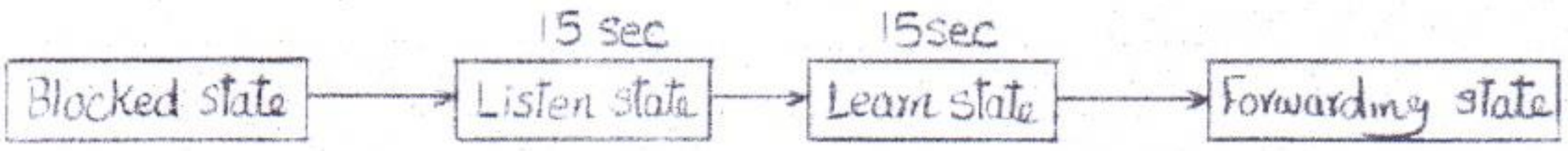
[2] Indirect Change:

1. Failed root switch.
2. Change state from BP to RP.



Max. age = 10 Hello = 20 sec.

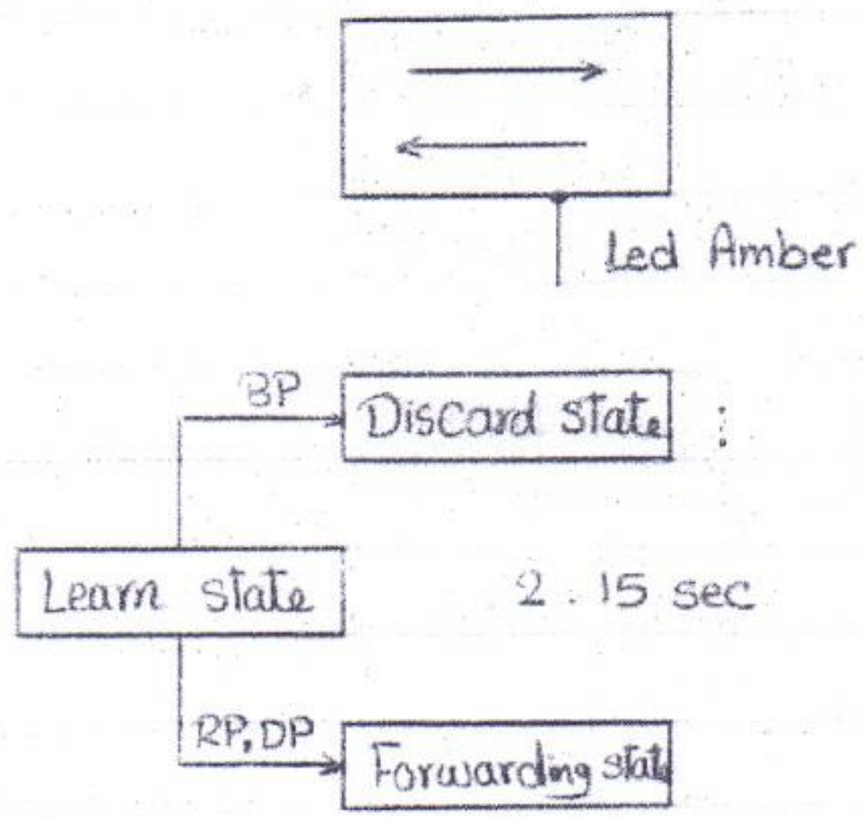
Conversion Time ≃ 50 sec



Rapid Spanning-Tree Protocal (RSTP):

- STP ver.2 ≡ IEEE 802.1w .

RSTP Port states :

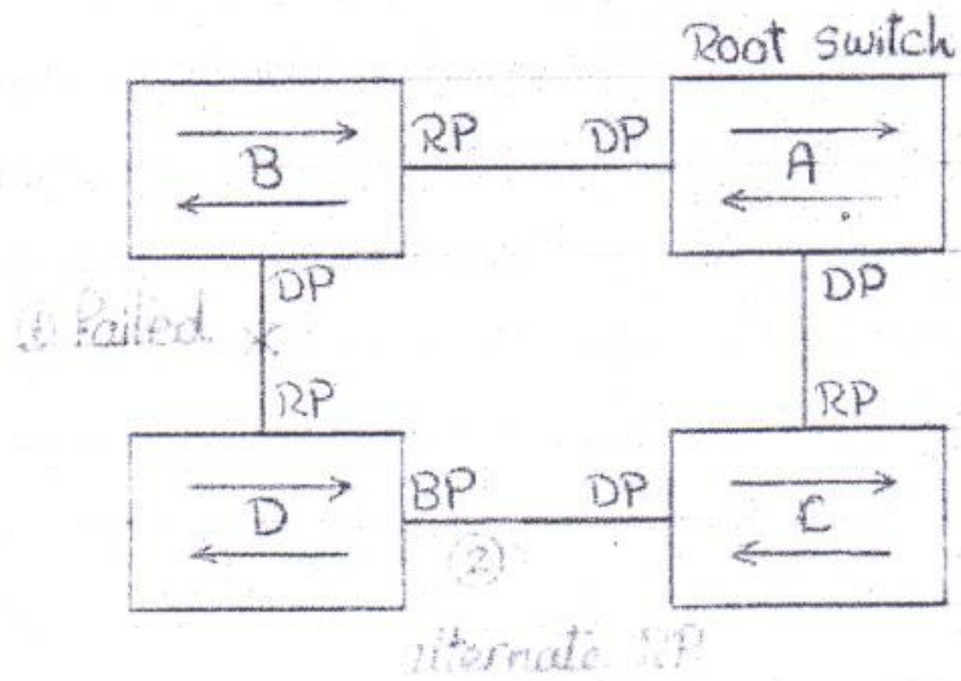


They introduced alternate Port & Back up ports for every RP & DP ...

@ Change :

1 Direct Change :

Conversion Time = 0 sec



2 Indirect Change :

Max. age = 3 Hello = 6 sec .

Conversion Time = 8 : 21 sec ...

Session 11/1

VLAN : Virtual LAN ⇒ IEEE 802.1q → queen

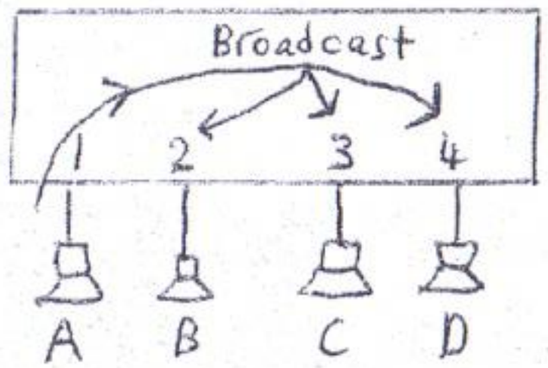
It is dividing main LAN into Sub LANs,

called VLAN (1-4094) : VLAN ID = 12 bit (0-4095)

0 & 4095 → reserved

1002 - 1005 → reserved for the Past (Token Ring / FDDI)

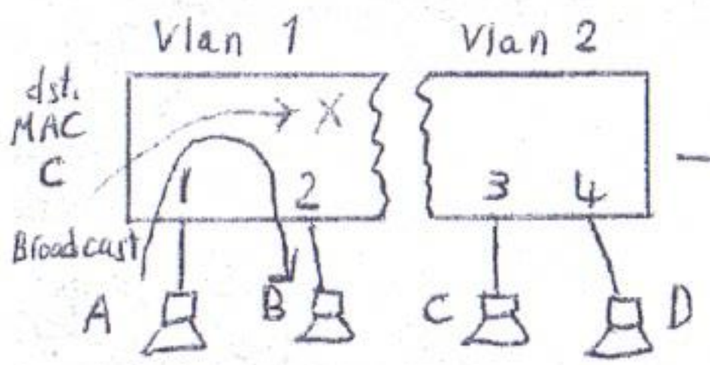
For Ethernet, we use 1-1001 & 1006-4095



MAC Table

MAC	Port	Vlan
A	1	1
B	2	1
C	3	1
D	4	1

show mac-address-table

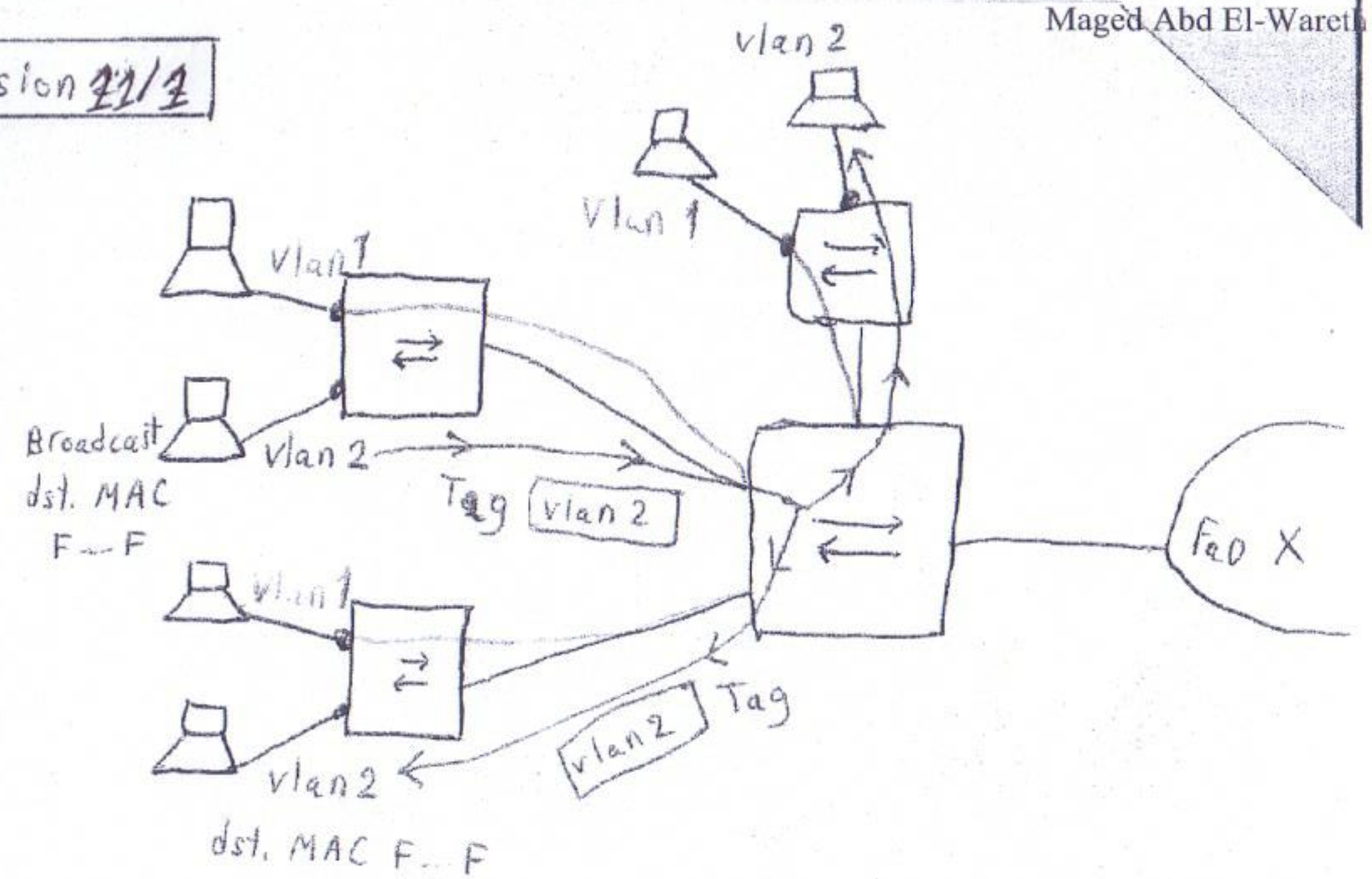


MAC	Port	Vlan
A	1	1
B	2	1
C	3	2
D	4	2

(config) # interface range fa 3-4

(config-if-range) # switchport mode access → connected to PC

(config-if-range) # switchport access vlan 2



LAN

one Broadcast domain

VLAN

Each VLAN = Broadcast domain

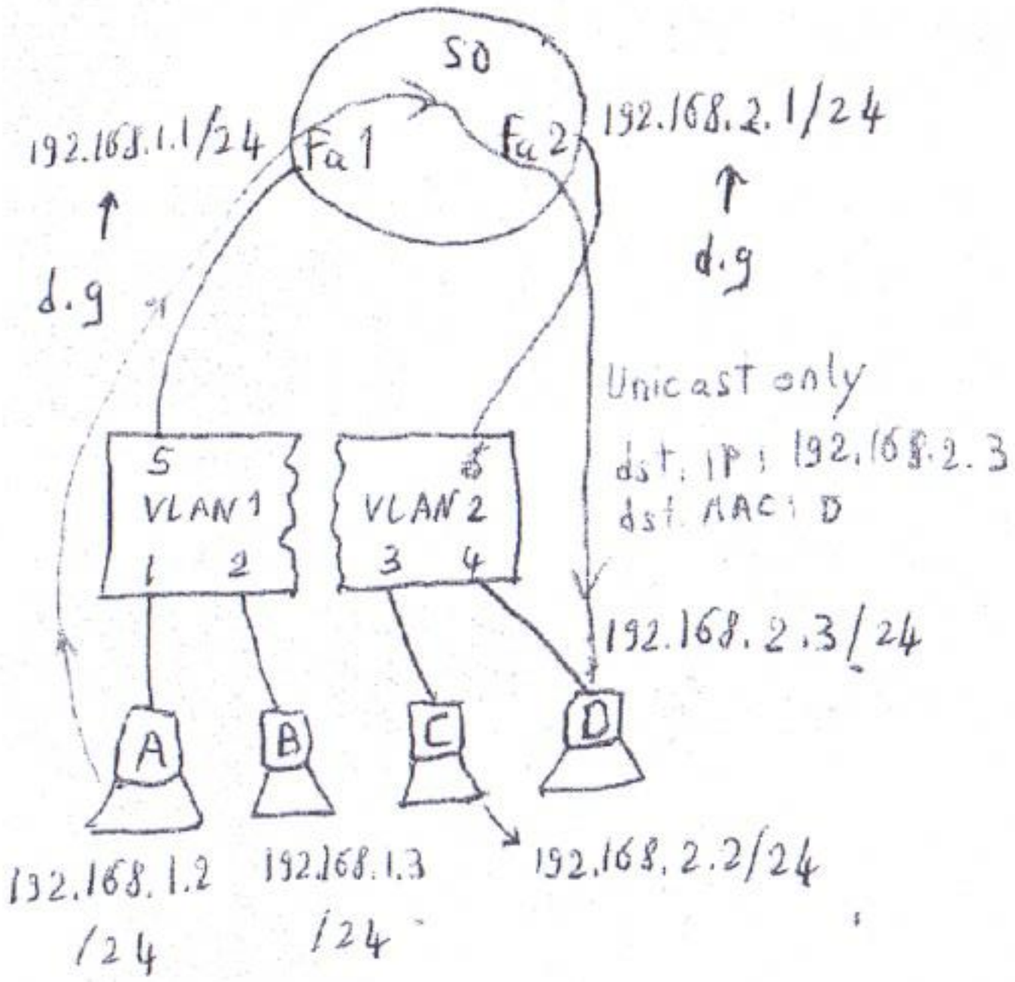
* Before VLAN : more Broadcast → more Flood → Congestion high
* After VLAN : less Broadcast → less Flood → Contine Congestion

LAN Problem	Collision	L2 Loops	Congestion
Solution	Switch	STP / RSTP	VLAN

Inter VLAN Routing:

Session 11/2

1 Traditional Solution: 2%



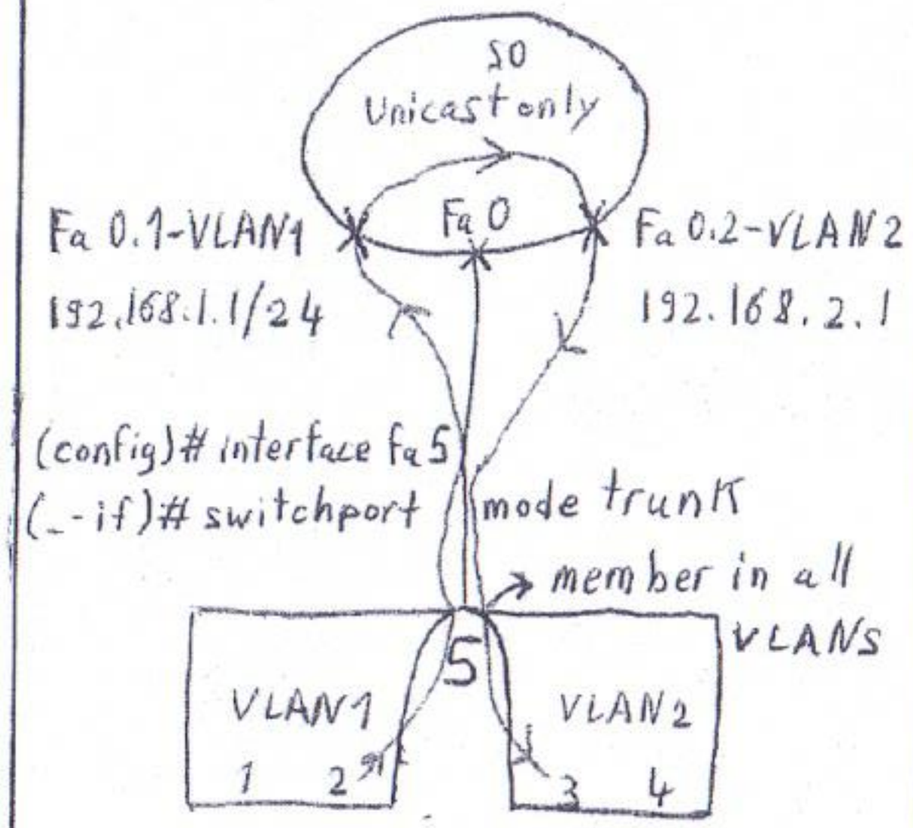
Routing Table

C	192.168.1.0	/24	Fa 1
C	192.168.2.0	/24	Fa 2

(config)# router rip
(config-router)# version 2
(config-router)# network 192.168.1.1
(config-router)# network 192.168.2.1
(config-router)# no auto-summary

(config)# no router rip ⇒ Remove all commands

2 ROAS (Router on A stick): 78%



On Router

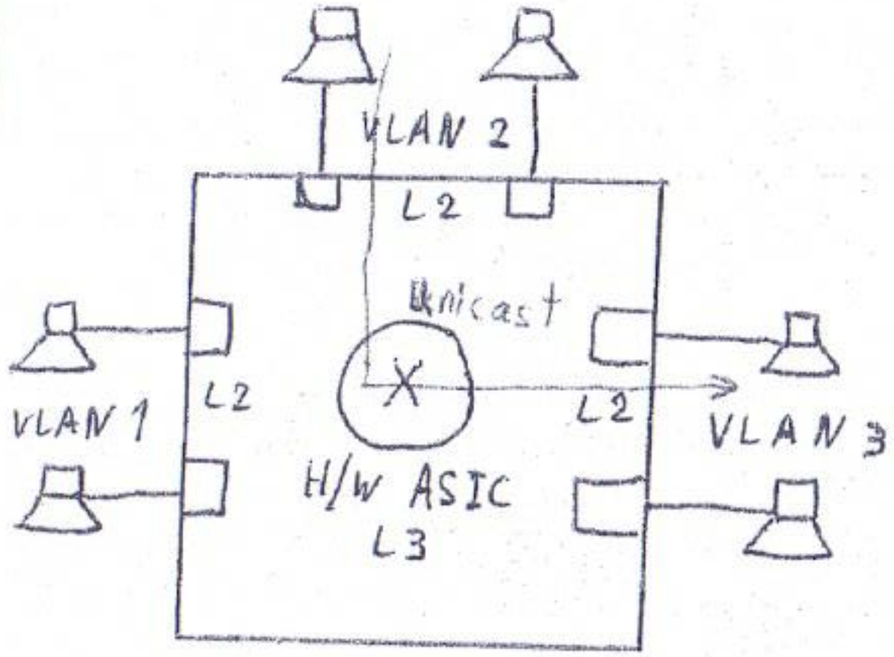
(config)# interface Fa 0
(config-if)# no shutdown
(config-if)# no ip address

(config)# int. Fa 0.1
(config-if)# encapsulation dot 1q 1
(...-if)# ip address 192.168.1.1 255.255.255.0

(config)# int. Fa 0.2
(config-if)# encapsulation dot 1q 2
(..-if)# ip address 192.168.2.1 255.255.255.0

3 MLS (Multilayer Switch): 20%

(L2 & L3 switch)



H/W ASIC

CEF = Cisco Express Forward

FIB = Forwarding Information Base
H/W Router

Session 11/13

VLAN Configuration:

1 Create VLAN database: (vlan.dat)

on each router

(config)# vlan 2

(config-vlan)# name HR → optional

VTP: Vlan Trunk Protocol

Synchronize vlan.dat

ADM (Add, Delete, Modify) on Cisco switches

(config)# vtp domain CIB
name

2 Activate VLAN on Switchport: manual (static)

(config)# interface fa 2

(config-if)# switchport mode access — connected to PC

(config-if)# switchport access vlan 2 — in only one VLAN

3 Trunk Conf.: connected to other switch/router

(config)# int. Gi 1 → in all vlans

(config-if)# switchport mode trunk

(config-if)# switchport trunk encapsulation dot1q

(config-if)# switchport trunk native vlan default is 1

#show int. trunk

vlan.dat

vlan 1 default
vlan 2 HR

in flash memory

#show vlan

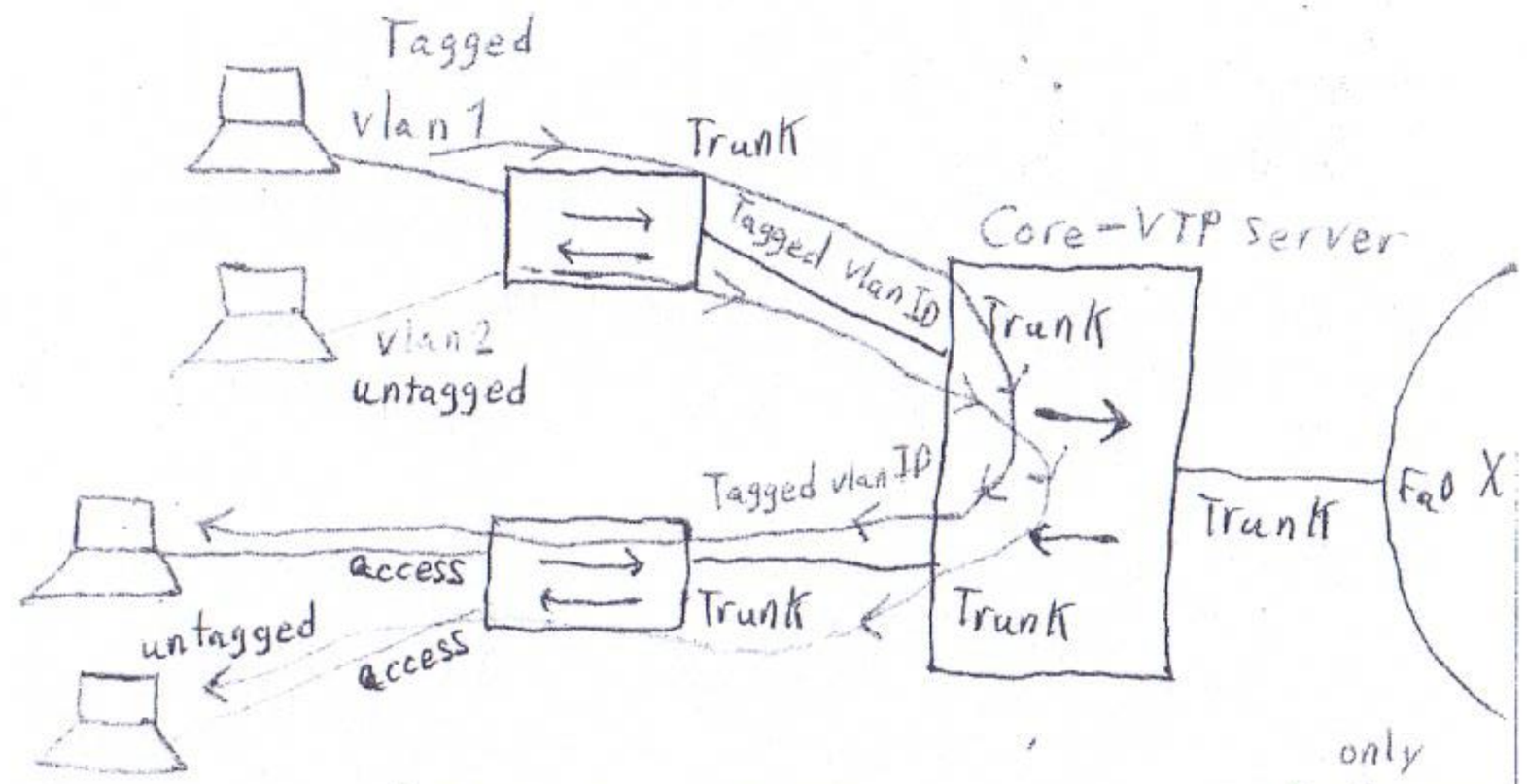
IEEE 802.3 - (Untagged)

Pre	dst. MAC	Src. MAC	Type	Packet	CRC

IEEE 802.1q/dot 1q - (Tagged)

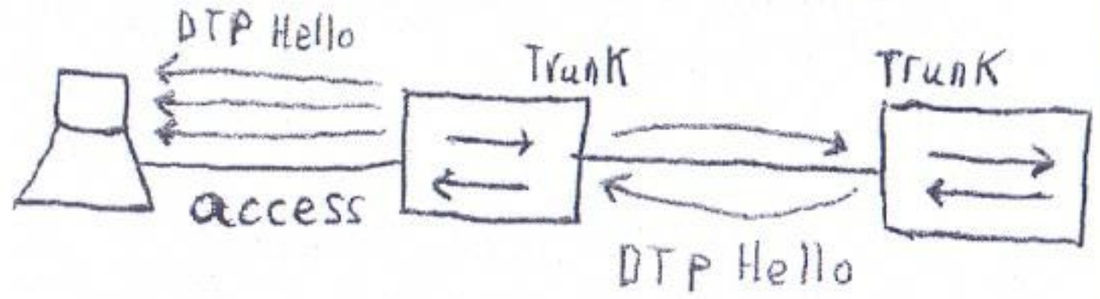
Pre	dst. MAC	Src. MAC	4 byte	Type	Packet	CRC

vlan ID - 12 bit



DTP (Dynamic Trunk Protocol): only in Cisco switches

* negotiate whether port is access/trunk
* plug & play on Cisco switches only



Port Fast :

Port connected to PC. Port jump to Forwarding state immediately.

(Config)# interface Fa 0/5
(Config-if)# spanning-tree portFast
(Config-if)# spanning-tree bpduguard → if portFast received a BPDU, it should shutdown

OR

(Config)# interface range Fa 0/1-23
(Config-if-range)# spanning-tree portFast
(Config-if-range)# spanning-tree bpduguard

LAN Switching :

Disadvantage :

- Collision → Switches (Microsegmentation & Buffering).

No. of collision domain on switch = No. of ports used (Separate Collision domain) ... All in one broadcast domain.

- Loop → STP & RSTP.
- Congestion → VLAN Queen of switching

كتير بعمل Flood كتير Broadcast
يدي Congestion حطيت

VLAN (Virtual LAN) :

It's divide main LAN into Sub-LANs called VLANs.
VLAN has an ID from 12-bits (0-4095) → 0 & 4095 reserved for future
VLAN standard IEEE 802.1q.
Each VLAN equal Broadcast domain.
→ 1002 : 1005 reserved for Past

(Config)# interface range Fa0/3-4
(Config-if-range)# switchport mode access
(Config-if-range)# switchport access vlan 2 "Vlan 1 is native Vlan"
show mac-address-table

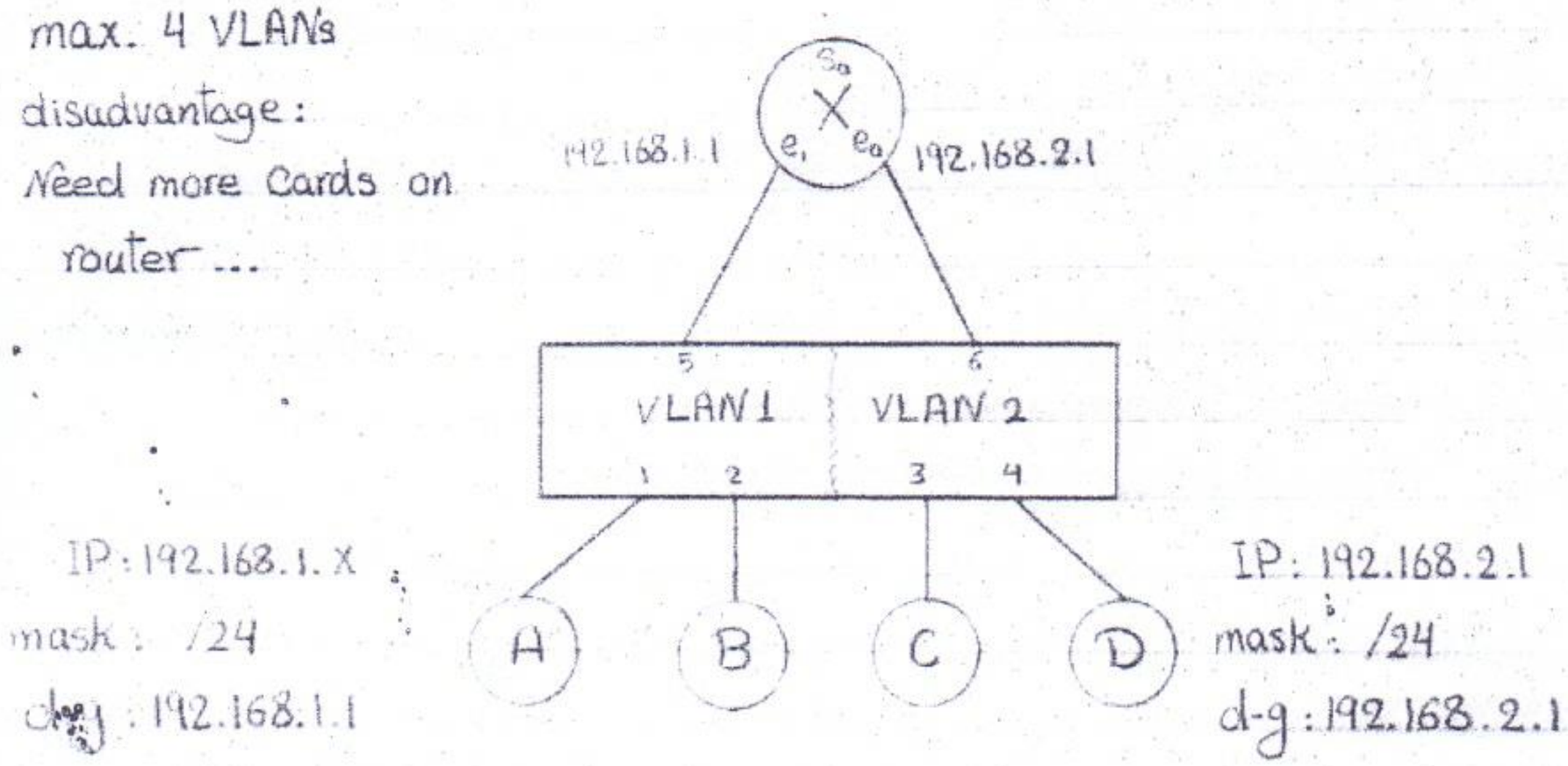
Inter VLAN:

1. Traditional solution : 2%

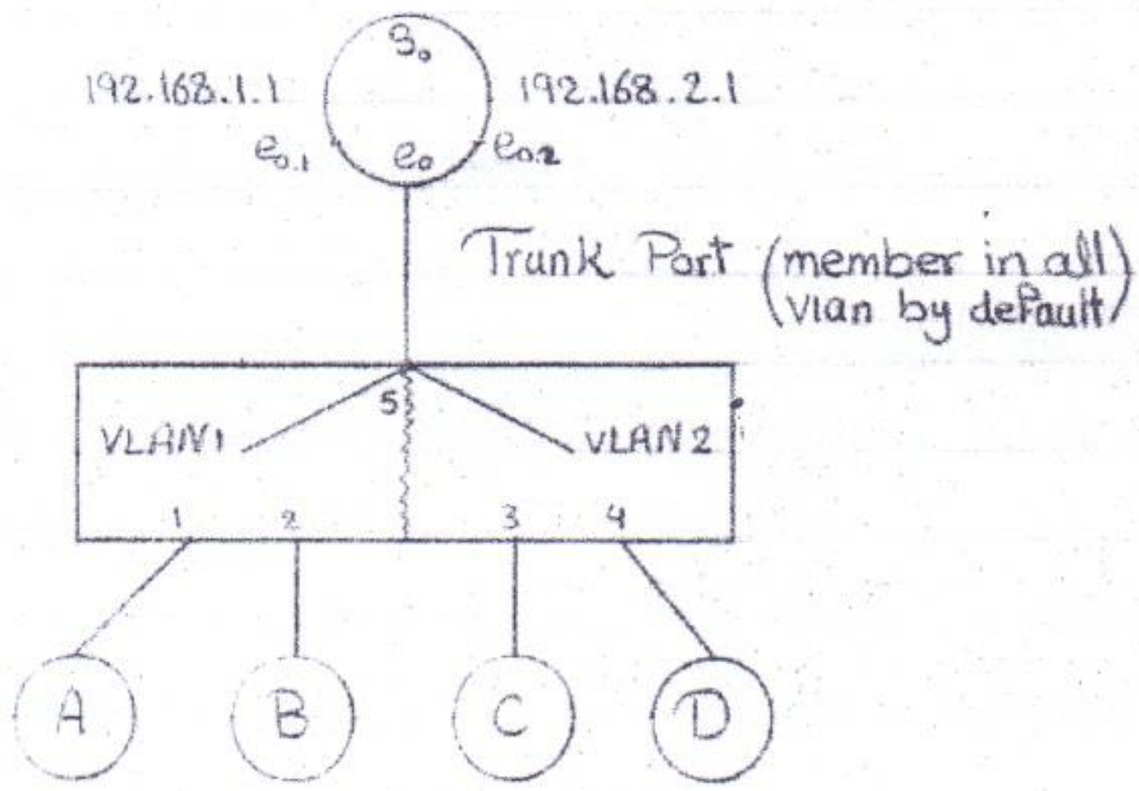
max. 4 VLANs

disadvantage:

Need more Cards on router ...



2. Router on a stick (ROAS): 78%



@ switch

(Config) ※ int Fa 0/5

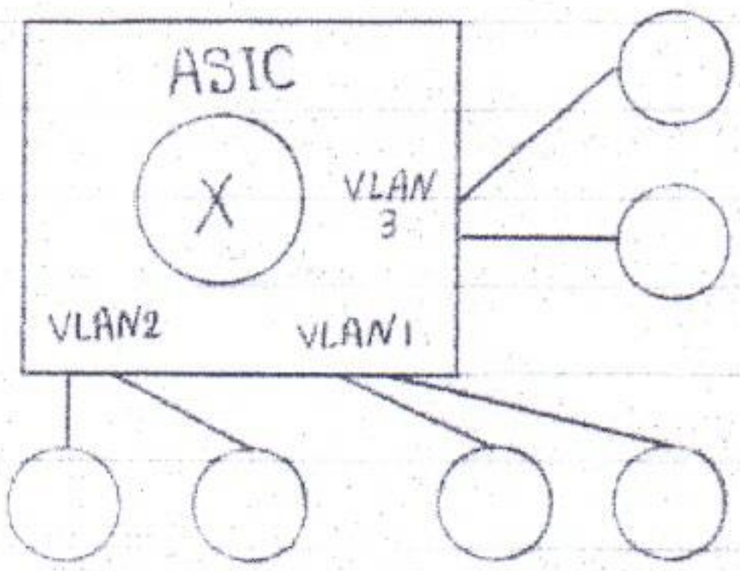
(Config-if) ※ switchport mode trunk

@ router
(Config)※ interface e0
(Config-if) ※ no shutdown
(Config-if) ※ no ip address

(Config) ※ interface e0.1
(Config-subif) ※ encapsulation dot 1q 1
(Config-subif) ※ ip address 192.168.1.1 255.255.255.0

(Config) ※ interface e0.2
(Config-subif) ※ encapsulation dot 1q 2
(Config-subif) ※ ip address 192.168.2.1 255.255.255.0

3. <u>Layer 3 switch :</u> in Core only
MLS (Multi Layer Switch)
This ASIC is called CEF (Cisco Express Forwarding) that forms H/W routing table called FIB (Forwarding Information Base).



<u>VLAN Configuration:</u>
1. <u>Create Vlan data base :</u>

(Config) ※ VLan ___
(Config-vlan) ※ name ___ ⟹ optional

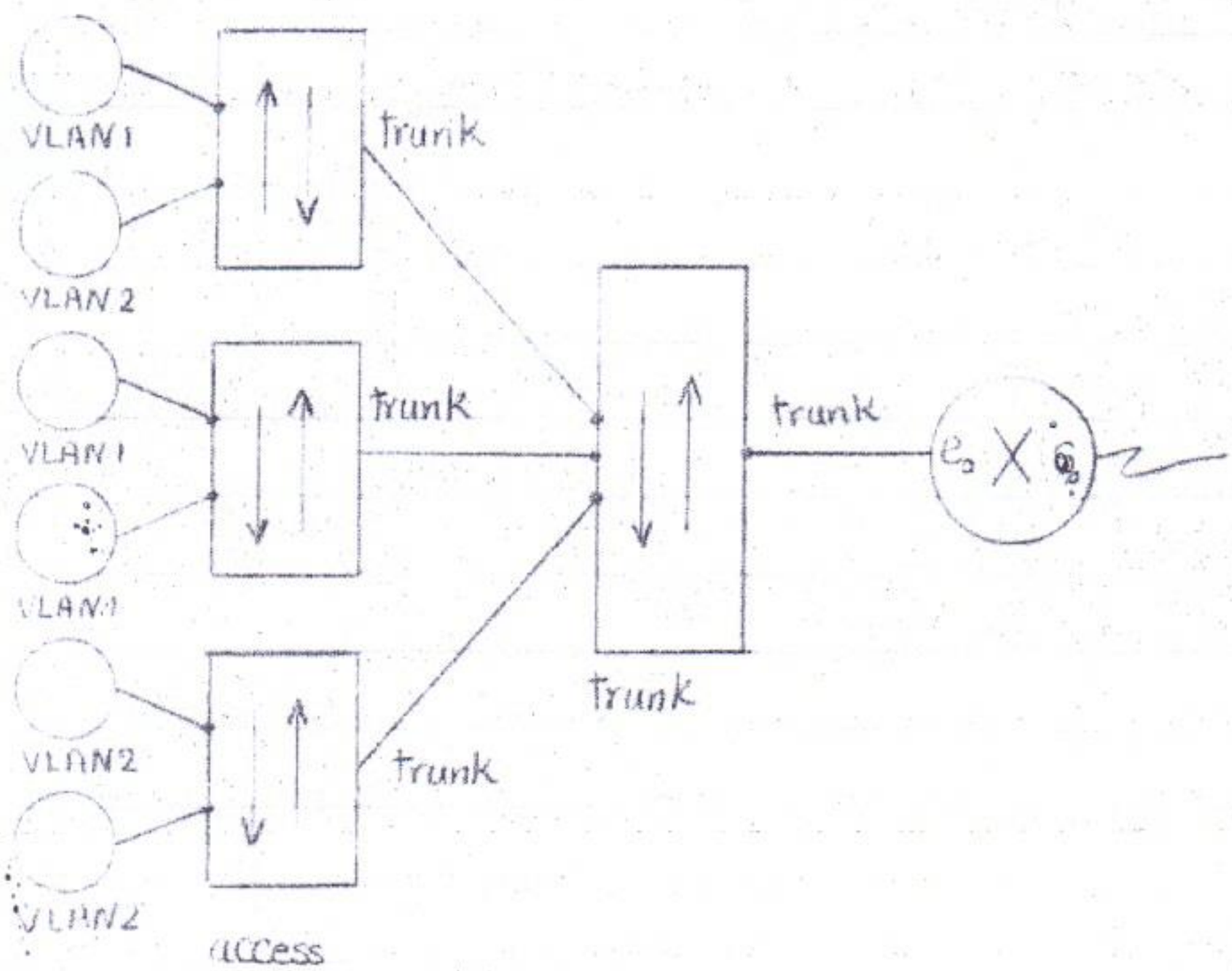
VTP (VLAN Trunking Protocal) used to <u>synchronize</u> vlan.dat
For Cisco only. ADM (Add, Delete, Modify)

2. Activate VLAN on switchport:

(Config)# interface ____
(Config-if) # switchport mode access vlan #

3. Trunk Configuration:

(Config)# interface ____
(Config-if) # switchport mode trunk
show interface trunk



untagged Frame

tagged Frame

Pre	DST MAC	SRC MAC	Type	Packet	CRC

4-byte

Pre	DST MAC	SRC MAC	dot1q tag	Type	Packet	CRC

VLAN Configuration :

- CCIE is server used for distribute configuration to all switches by software VMPS (VLAN Membership Policy Server) ...

- VTP (VLAN Trunking Protocal)
  (Config) ※ VTP domain name

Dynamic trunk Protocal (DTP): Cisco only

- Protocal plug & play on Cisco switches only, negotiate whether port should be access or trunk & if trunk, negotiate whether to use ISL / dot 1q.

(Config-if) ※ switchport mode dynamic desirable

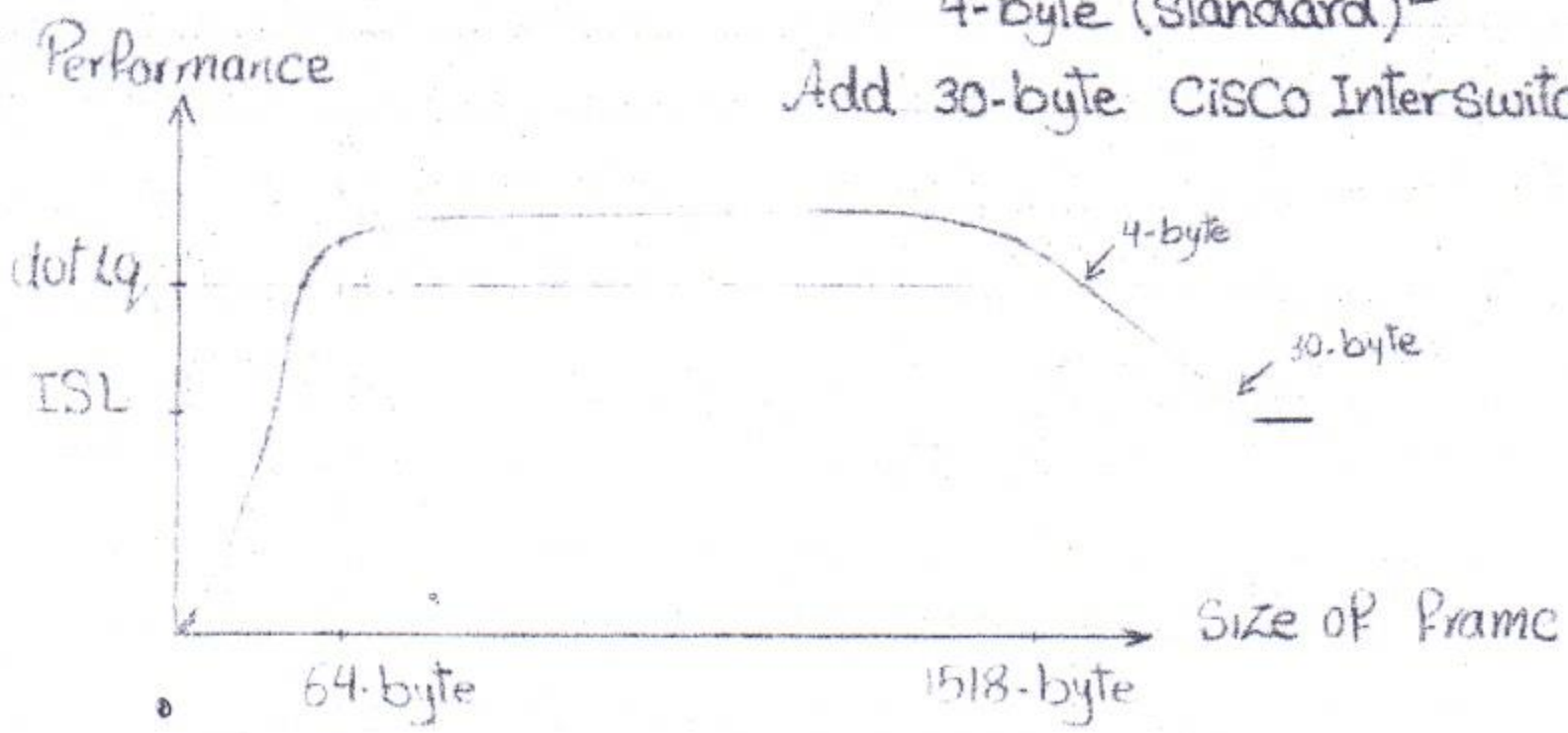
DTP modes :
- desirable
- Auto
- ON
- off

Old Cammand :

(Config-if) ※ switchport trunk encapsulation {dot 1q / ISL}

4-byte (standard)

Add 30-byte Cisco Interswitch link



By default is VLAN 1 is called <u>native VLAN</u>
(untagged VLAN)

(Config-if)# switchport trunk native Vlan #

<u>Managing the switch remotely :-</u>

Virtual telnet

(Config)# line <u>vty</u> 0 <u>15</u> max. number of users can telnet on the same time -1

(Config-line)# password <u>xxxx</u>

(Config-line)# login

to use SSH instead of telnet

(Config-line)# transport input SSH

(Config)# interface <u>VLAN 1</u>

↳ switch virtual interface

(Config)# no shutdown

(Config)# ip address <u>ip of switch</u> <u>Mask</u>

(Config)# ip default-gate way <u>ip of router</u>

then you can now telnet & Ping the switch ...