CISCO

Implementing Cisco Switched Networks(SWITCH)

Prepared by
ENG: Ahmed Abdallah

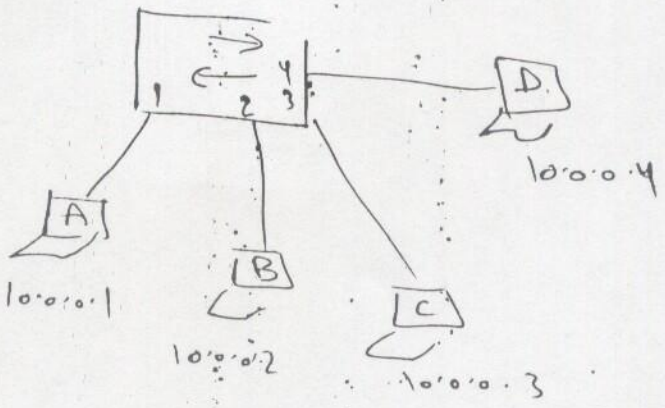
80
621/010

switching

- switch is a Layer 2 device
- switch learn MAC-address and Form MAC-address table
- switch is a single broad cast domain and multi collision domain

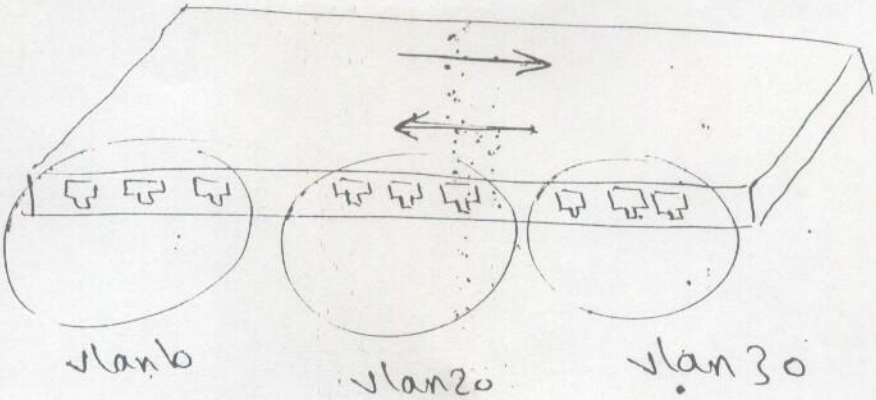
1	A
2	B
3	C
4	D

MAC address table



(# show mac-address table)

VLAN [virtual LAN]



- The basic cl's of vlan is to make multi B.C domain by logically devide The switch into multi independent switches
- VLAN provide segmentation & security

---

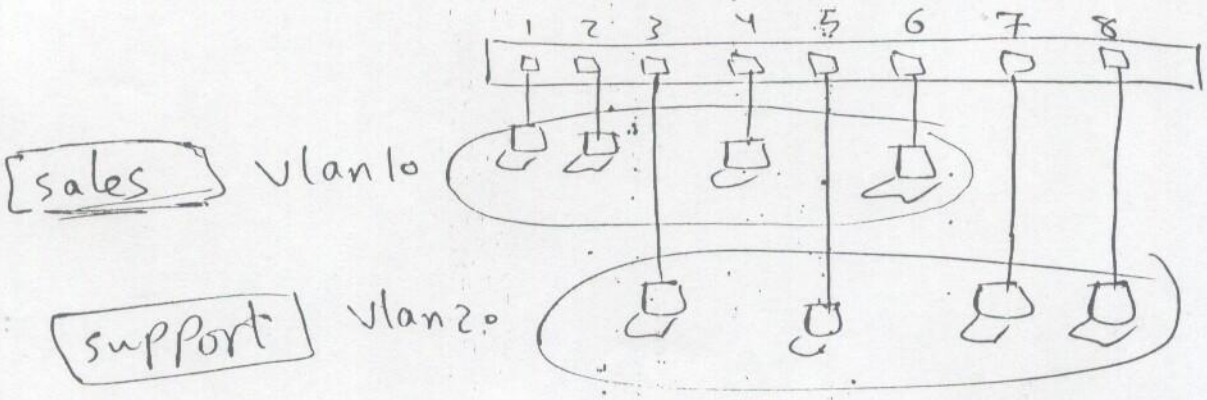
* VLAN membership *

how make a PC member in a VLAN?

→ we have 2 ways

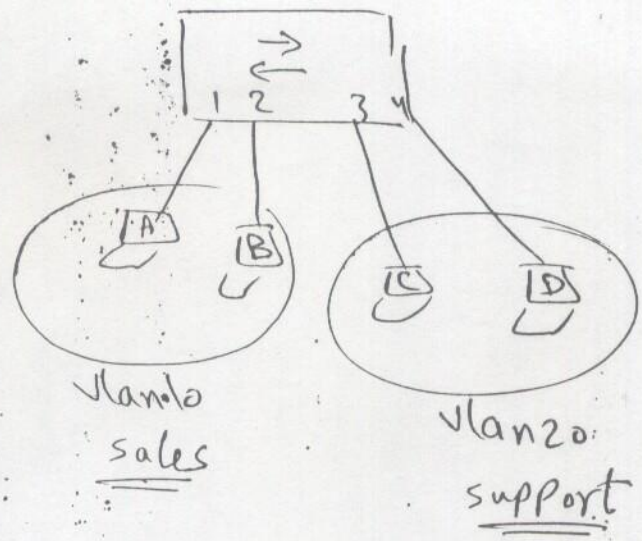
1. static membership ⇒ [Port based]

- assign a certain Port to a certain VLAN



example

(config) # vlan 10
-vlan) # name sales
(config) # vlan 20
vlan) # name support
(config) # interface range Fo/1 0-2



(config-~~if-range~~)# switchport
→ mode access
)# switch port access-vlan 10

(config) # interface range Fo/3 0-4
if-range)# switchport mode access
)# switchport access vlan 20

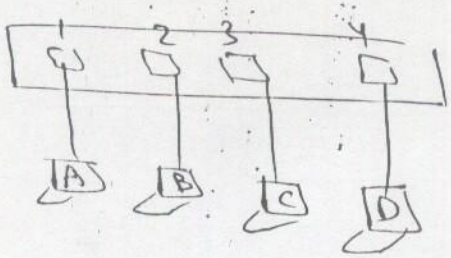
~~# show vlan~~

troubleshooting

show vlan

2 Dynamic membership ⇒ [MAC based]

assign a certain MAC to a certain VLAN by using VMPS "VLAN membership server"



MAC	Vlan
A	Vlan10
B	Vlan20
C	Vlan10
D	Vlan20

A, C يظلوا في vlan10 مهما تغير البورت الذي يتم توصيلهم عليه

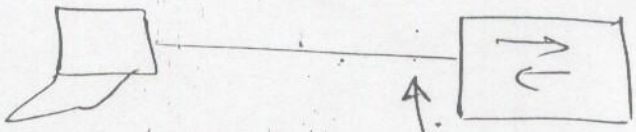
ملحوظة: يتم عمل VMPS على ال switch ~~وكلكم~~ ولكن ليس مقرر عليكم دراسته

---

* VLAN Port Connection type *

① access Port: member in one VLAN

ex: PC connected with sw

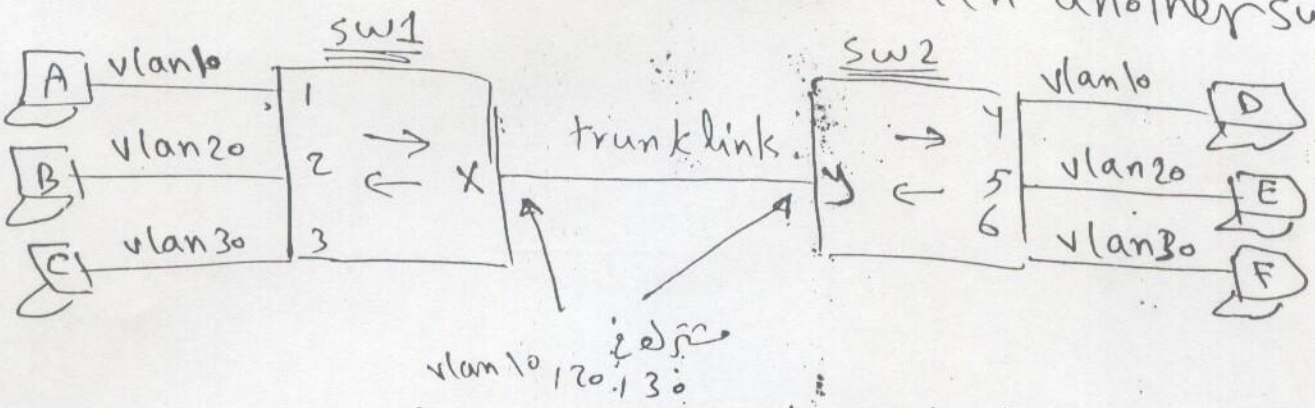


access port

if) #switch port mode access

② **trunk Port**: member in all vlans

ex: switch connected with another switch



if) #switch port mode trunk

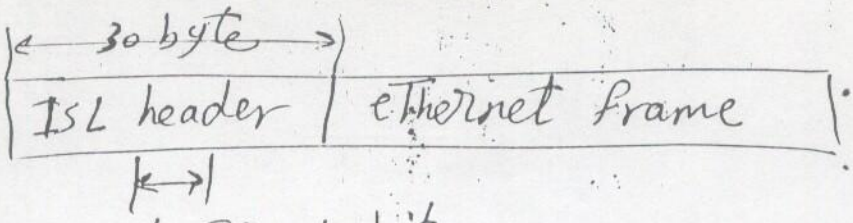
Problem: if A send a broadcast frame from port 1 search for vlan 1 "found nothing", so it make it out of port x and when it reach sw2 it will forward it to all ports (to all vlans in sw2)

solution: "Tagging" → trunk port add a feild that identify the src vlan ID to the frame.

⇒ we have 2 types of tagging → IEEE 802.1q, → ISL

① ISL (inter switching link)
⇒ cisco proprietary

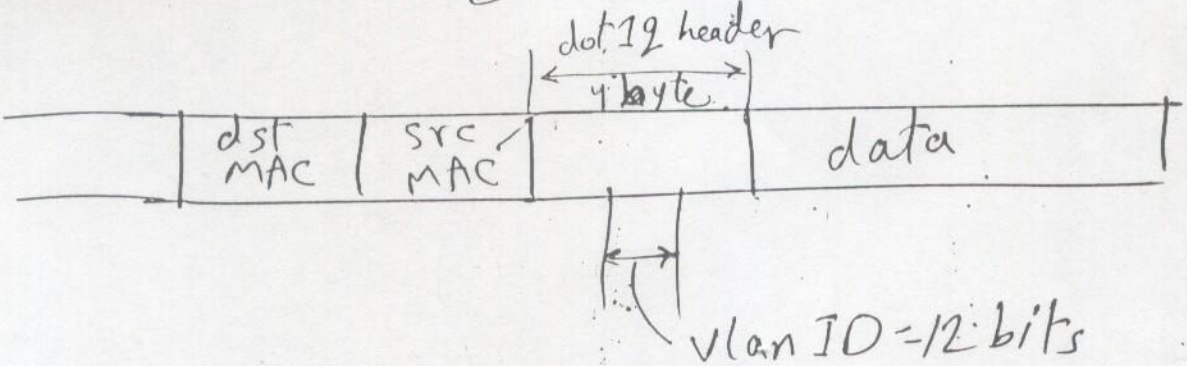
- tagging by 30 byte



---

② IEEE 802.1q "dot 1 q"

- tagging by using 4 byte "after The src MAC"



* ملحوظة ①: يفضل استخدام الـ dot 1q لأنه
① يعمل على كل السويتشات (سيسكو وغيرها)
② حجمه صغير عكس ISL
③ The dot 1q header is built in The frame

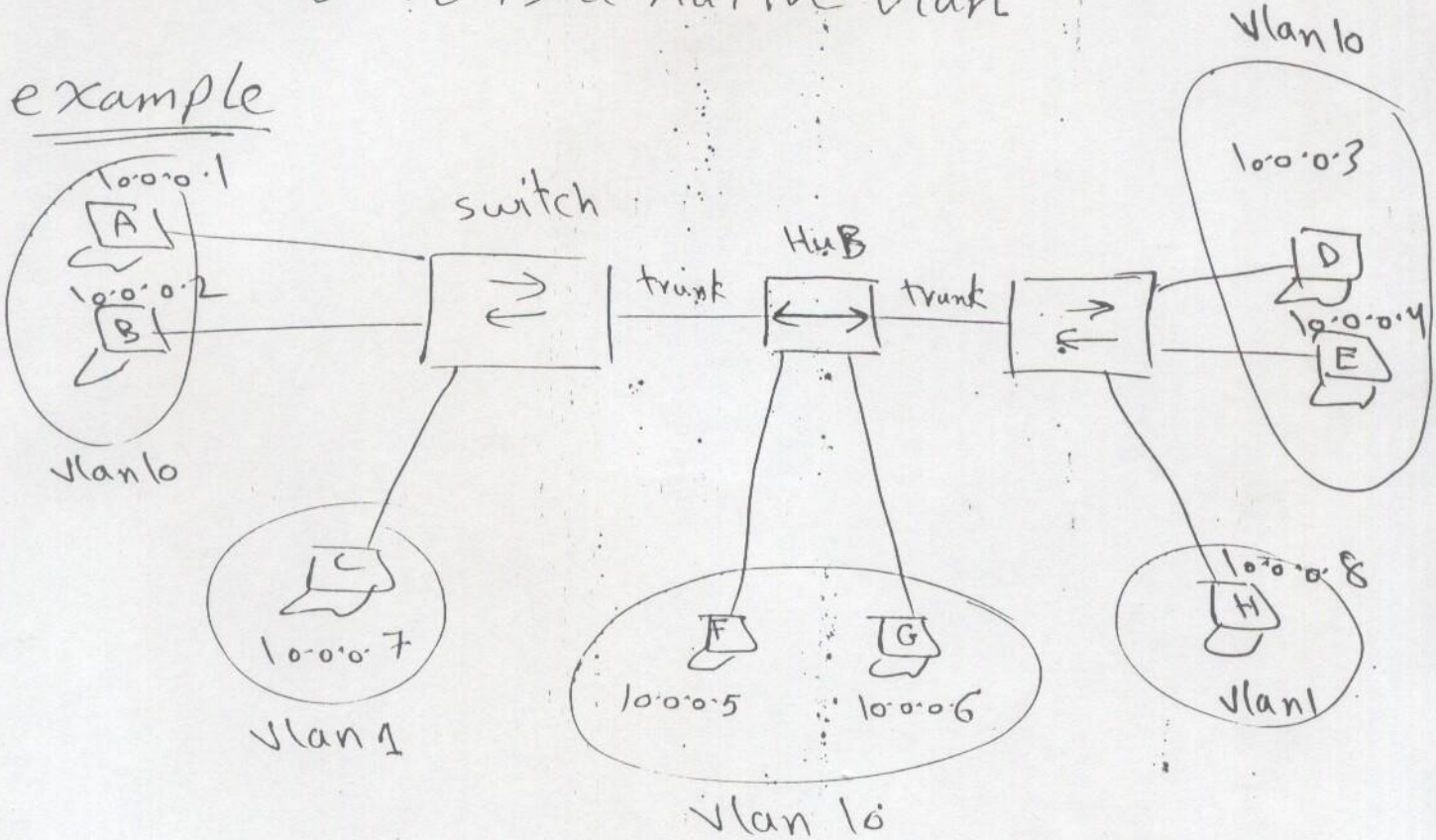
* ملحوظة ②: عندما يأتي الـ switch يصبح تكوين كل الـ port في vlan1

native VLAN

ال vlan الأصلي

- by defaulft vlan 1 is The native vlan
- all frames from vlan 1 don't tagged when it pass from a trunk link because it is a native vlan

example

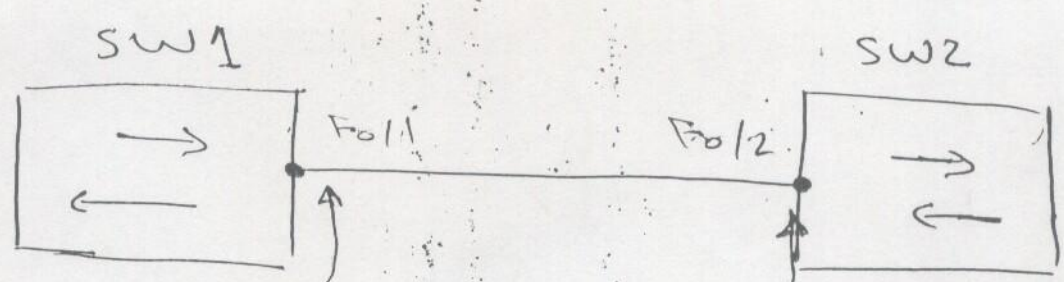


I need all PC's in vlan 10 can see each other --- you can??

→ you can find The solution in This command

(if) # switchport trunk native vlan 10

DTP [Dynamic trunking Protocol] and switch Port mode interfaces



sw1 \ sw2	Dynamic auto	Dynamic desirable	trunk	access
Dynamic auto	access	trunk	trunk	access
Dynamic desirable	trunk	trunk	trunk	access
trunk	trunk	trunk	trunk	not recommended
access	access	access	not recommended	access

trouble shoot

show interface Fo/1 switchport

VTP [VLAN trunking protocol]

<u>overview</u>: in large organizations managing VLANs on large number of switches is difficult

- <u>VTP</u>: (cisco proprietary)
  - ↳ it is an easy adminstration method to transfer information about VLANs between switches in the same domain

- <u>VTP domain</u>
  - it is an area with common VLAN requirements "all switches support same $f^{\underline{n}}$ & policy"
  - switch can member in only one VTP domain
  - default VTP domain name is ≡ "Null"

<u>VTP functions</u>: add, remove & modify for VLANS

<u>note</u>: to configure VLAN

1- create VLAN → can be advertised by VTP <u>Msgs</u>

2- name VLAN [optional] → can be advertised by VTP <u>Msgs</u>

3- assign ports to VLAN

- switch in VTP domain can be one of 3 modes

1- <u>server</u>: send VTP <u>msg</u> to order <u>clients</u> to create or remove VLANs on them

2- <u>client</u>: receive VTP <u>msg</u>

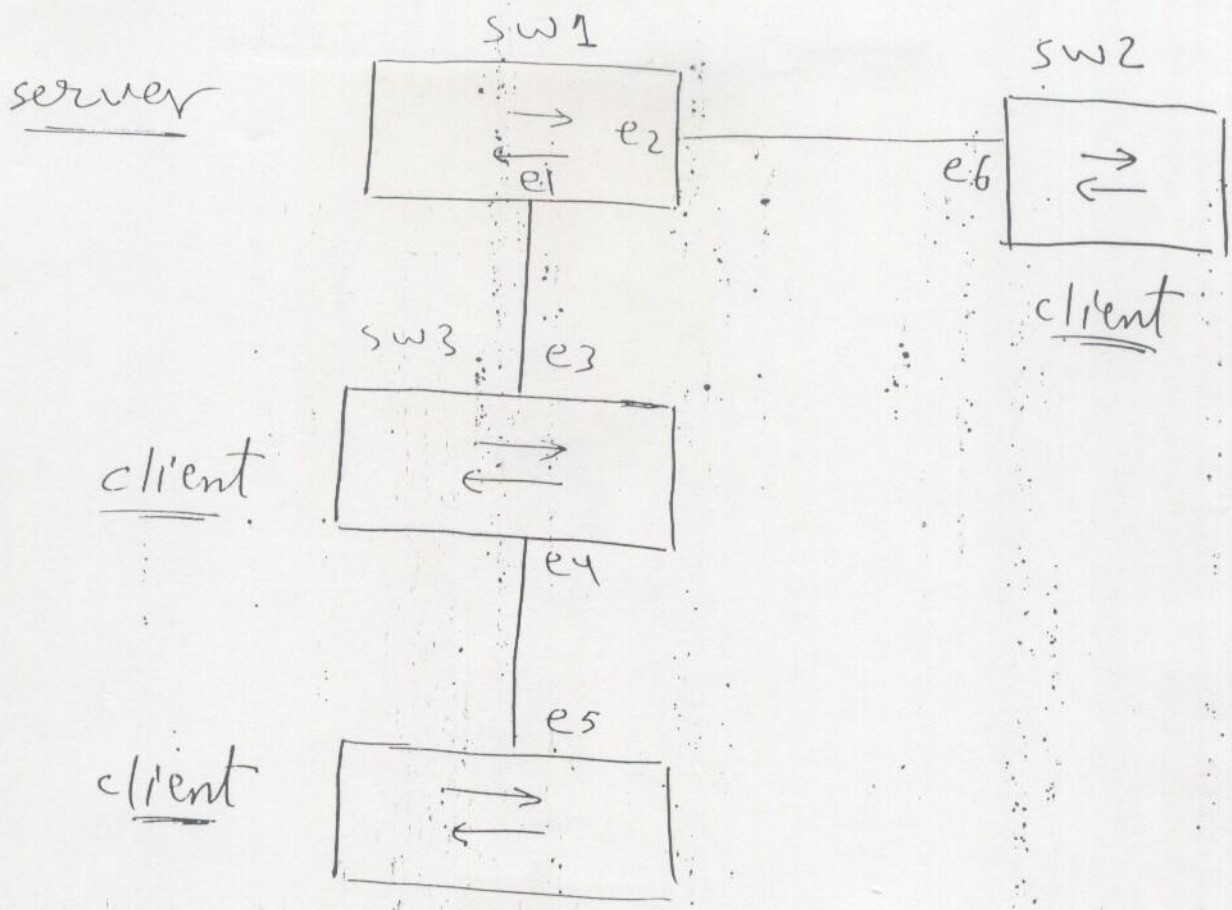
3- <u>transparent</u>: he can propagate VTP <u>msg</u> but he didn't have order from any one and didn't order any one

Feature	server	client	transparent
• can add, delete & modify vlans	✓	×	✓ But on itself only
• can generate VTP msg	✓	×	×
• can propagate VTP msg	✓	✓	✓
• can accept change in VTP msg	✓ لو فيه server آخر	✓	×
• default VTP mode	✓	×	×
• save configuration	✓ save in NVRAM	× save in RAM	✓ save in NVRAM

Hint: in case we have 2 servers in same domain, VTP msgs go between them & will be affectable

• VTP msg include a field called revision number "by default = 0" & it increases by 1 with each configuration command so, if any msg reach a switch with revision number < that on it, it will be forwarded without being affected by it

VTP LAB



١- عندما يأتي sw من المصنع فإنه يكون في (server mode)

٢- إذا أردنا إنشاء أكثر من vlan فمن الطبيعي أن أدخل على كل sw وأعرف له هذه ال vlans ولكن في cisco sw's الوضع مختلف

٣- نجعل أحد هذه ال sw's في (server mode) والباقي في (client mode)

٤- إذا أردت عمل create أو delete أو modify لأي vlan فأعمله على (server sw) وأتوماتيكياً سوف يتم إرسال (VTP msg) إلى كل ال clients فتقوم هي الأخرى بإنشاء هذه ال vlans عندها

```
sw1(Config) # vtp domain cisco
sw1(config) # vtp password a1
sw1(config) # vtp mode server
                       client
                       transparent
sw1(config) # int e1
sw1(config-if) # switch port mode trunk
sw1(config-if) #switchport trunk encapsulation dot1q
```

نفذ نفس الخطوات السابقة على int e2

```
sw2(config)# vtp domain cisco
sw2(config) # vtp password a1
sw2(config)# vtp mode client
sw2(config)# int e6
sw2(config-if) # switch port mode trunk
sw2(config-if)# switchport trunk encapsulation dot1q
```

وكذلك على باقي الـ switches الأخرى

والآن اعمل create لـ vlan وأعطيها أي اسم (طبعاً على server)

```
sw1(Config)# vlan 10
sw1(Config-vlan) # name HR
```

ثم نفذ الأمر #show vlan

على أي switch سواء server أو client سوف تجد عمل creation للـ vlan10 وبالتالي الاسم HR

trouble shooting

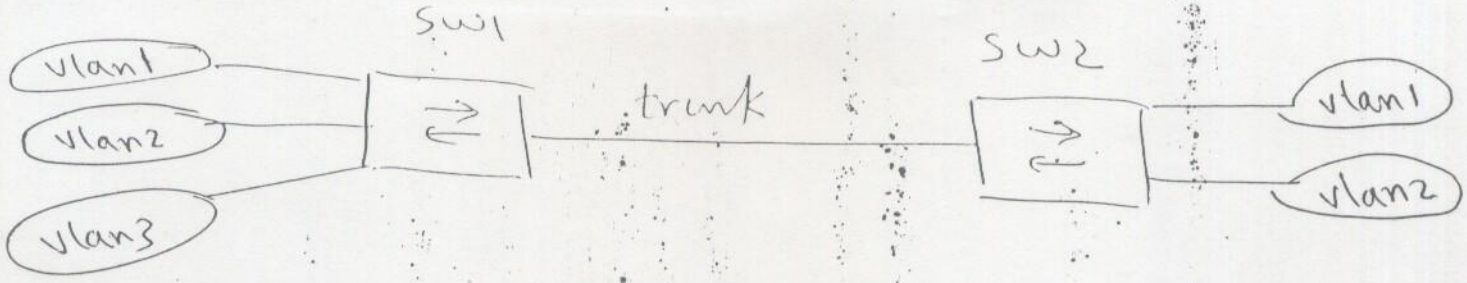
show vlan

show vtp status → display vtp information

show int f0/3 switch port

↑ to see if int f0/3 access or trunk

* VTP Pruning *



Problem:

although sw2 not contain vlan3 so, if vlan3 on sw1 send a broadcast it will path through trunk link to sw2

" link overhead + tagging process"

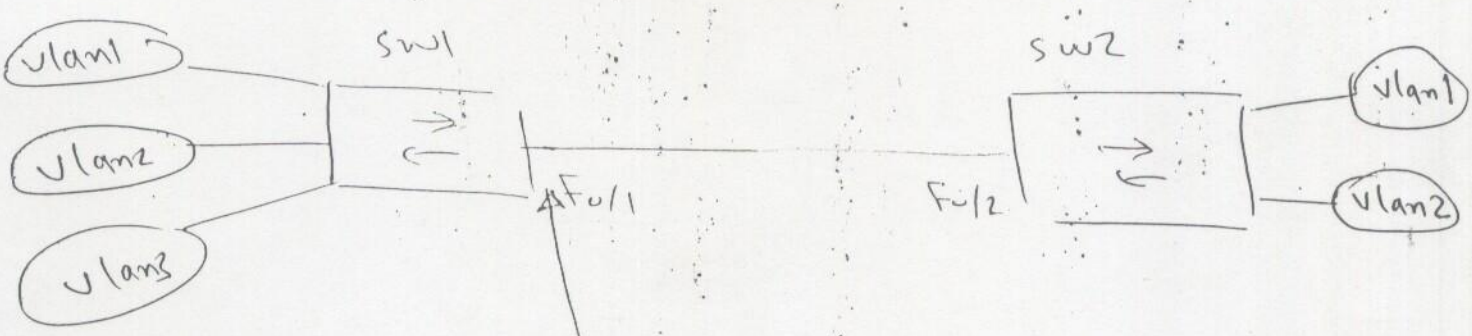
solution: pruning process

switches ~~witch~~ which connected with each other by trunk link should share their vlans

↳ **hint:** The switch he can do pruning he is in server mode

- يوجد طريقة أخرى تؤدي عمل ال Pruning

ألا وهي trunk allowed



(config)# int Fo/1

if) # switch port mode trunk

if) # switch port trunk allowed vlan 1,2

وبالتالي لم يسمح إلا بمرور 1,2 أما vlan3 فلم تمر

ولم يحدث tagging

* The Facts about spanning tree *

- Original stp (802.1d) was created to prevent Loops
- switches send BPDU [Bridge Protocol data unit] to discover loops
- The BPDU also help elect the core switch of the network, called the "Root Bridge"
- The simplistic view of stp: all switches Find the best way to reach the Root Bridge Then Block all redundant links

* understanding the BPDU & election

→ First every switch consider itself a root & send "BPDU" every 2sec × | priority | MAC address | to other sw's on multicast MAC

→ every switch will take a copy of BPDU & resend it to other switches

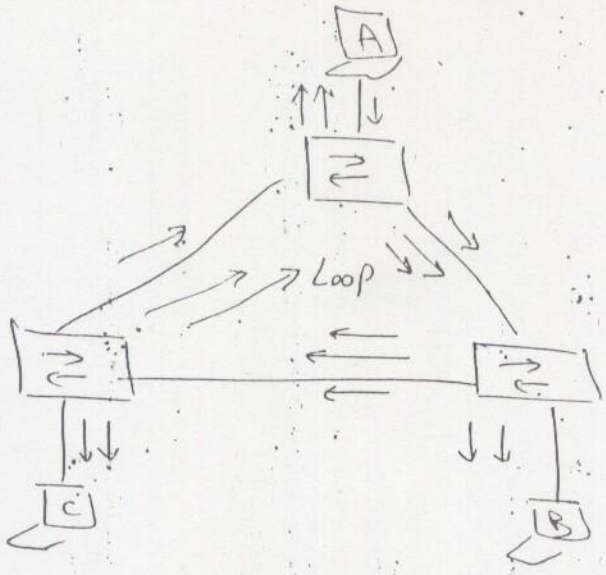
→ each switch will form BPDU data base

(hint) priority is value between 0 → 61440 [default 32768] & lower is better

BridgeID → | priority | mac-address |

Spanning tree protocol

- switches remove L2 loop using <u>stp</u>



يحدث Loop بتيجة
لوجود أكثر من مسار

→ switches Forward <u>B.C</u> packets out all Ports by design

→ redundant connections are <u>necessary</u> in business networks

→ so we will use stp to make a <u>logical Block</u> For one path & when The used Path Fails; <u>stp</u> will open The Blocked one

→ The Place of spanning tree: Drop trees on redundant link's. (until They are needed)

election

1 electing The root bridge [RB]

- is The switch with lowest Bridge ID
  - → ① priority
  - → ② mac-address

→ after electing The Root, The root Bridge only send BPDU's every 2sec

→ other non root switches stop sending BPDU's.

2 electing The Root Port [RP]

RP → best port in each non root sw to reach The root

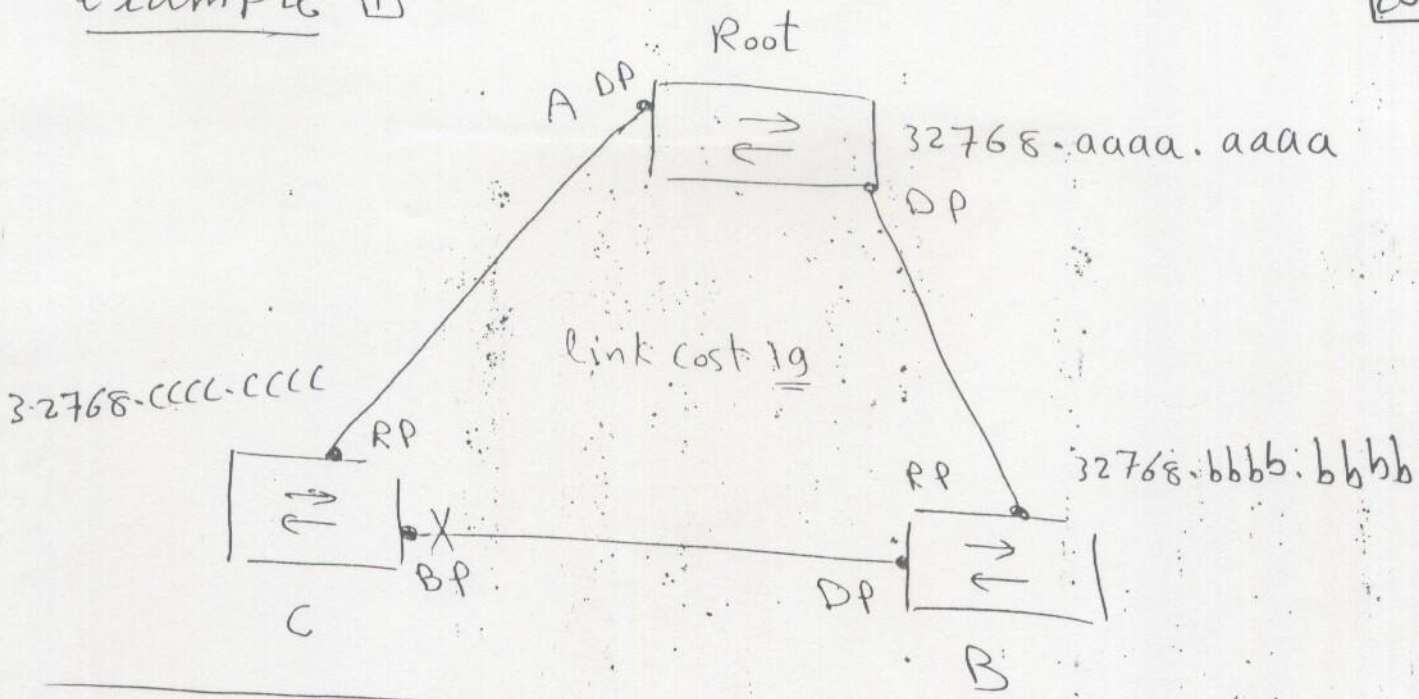
3 electing The designated port [DP]

- each 2sw's on a segment must elect The best Port to deliver data to root

4 Blocked Port [BP]

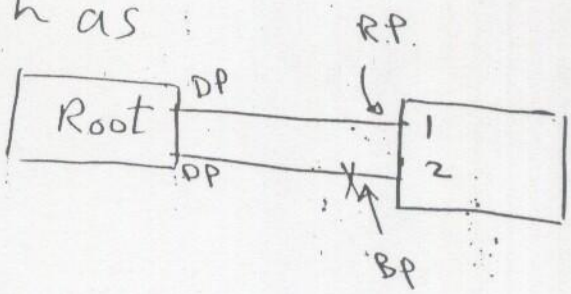
neither RP nor DP is The BP [Blocked port]

example 1



notes

- if 2 Ports on same switch as shown, The Root Port [RP] will be The Port with least Port ID



- one Root ~~Port~~ Bridge / network
- one root Port per non root switches
- one designated Port per segment
- neither RP nor DP is BP

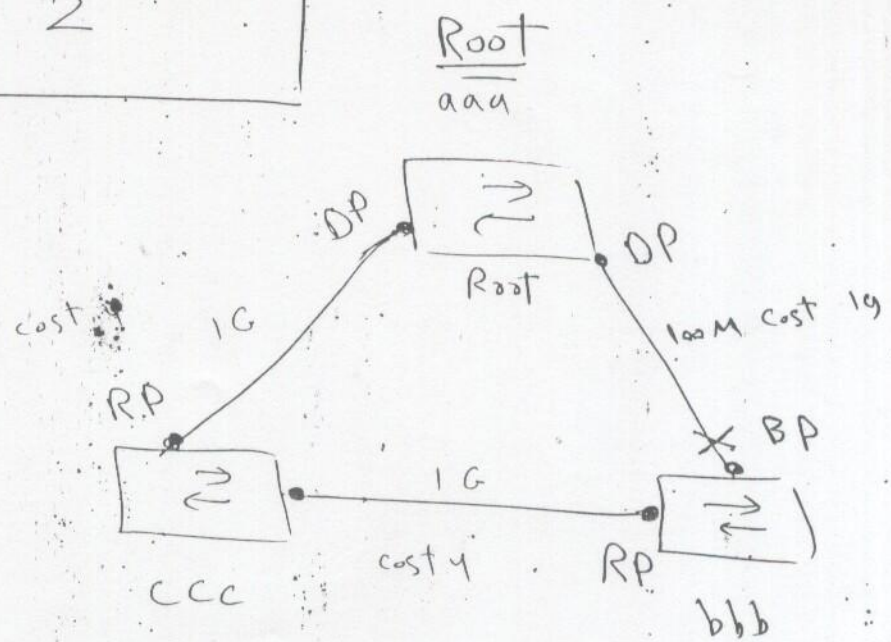
* how stp find the best path

① elect the root

② switches find lowest cost path to Root

Link Bw	stp cost
4Mbps	250
10Mbps	100
16Mbps	62
45 Mbps	39
100Mbps	19
155 Mbps	14
622Mps	6
1Gbps	4
10Gbps	2

example



STP operation states

① **Listening state:**

Process only BPDU's to elect root sw, RP, DP

→ forward delay time = 15 sec

② **learning state:**

Process BPDU + learn MAC's "Populate MAC table"

→ forward delay time = 15 sec

③ **Forwarding state:**

Process BPDU + learn MAC + Forward data

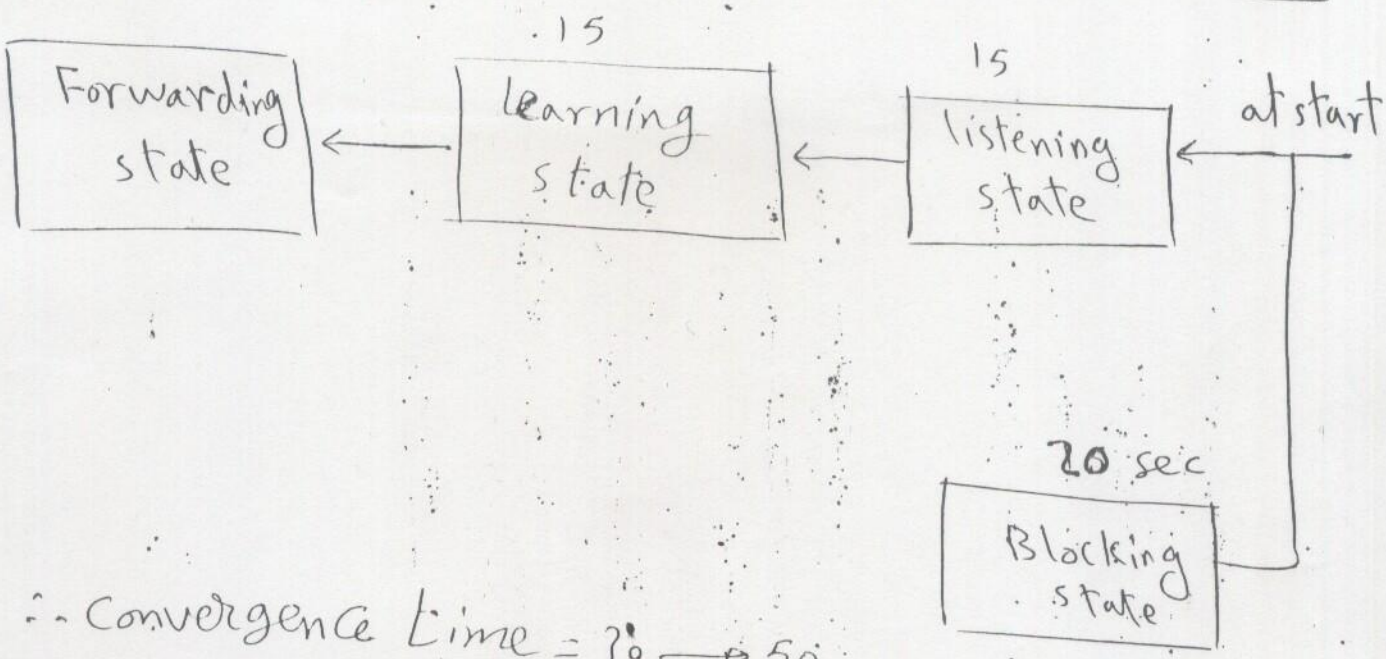
④ **Blocking state**

only listen to BPDU's & drop any data

max time = 20 sec [10 BPDU's]

⑤ **disable state**

Physical Blocking → disconnected cable
→ Port shutdown

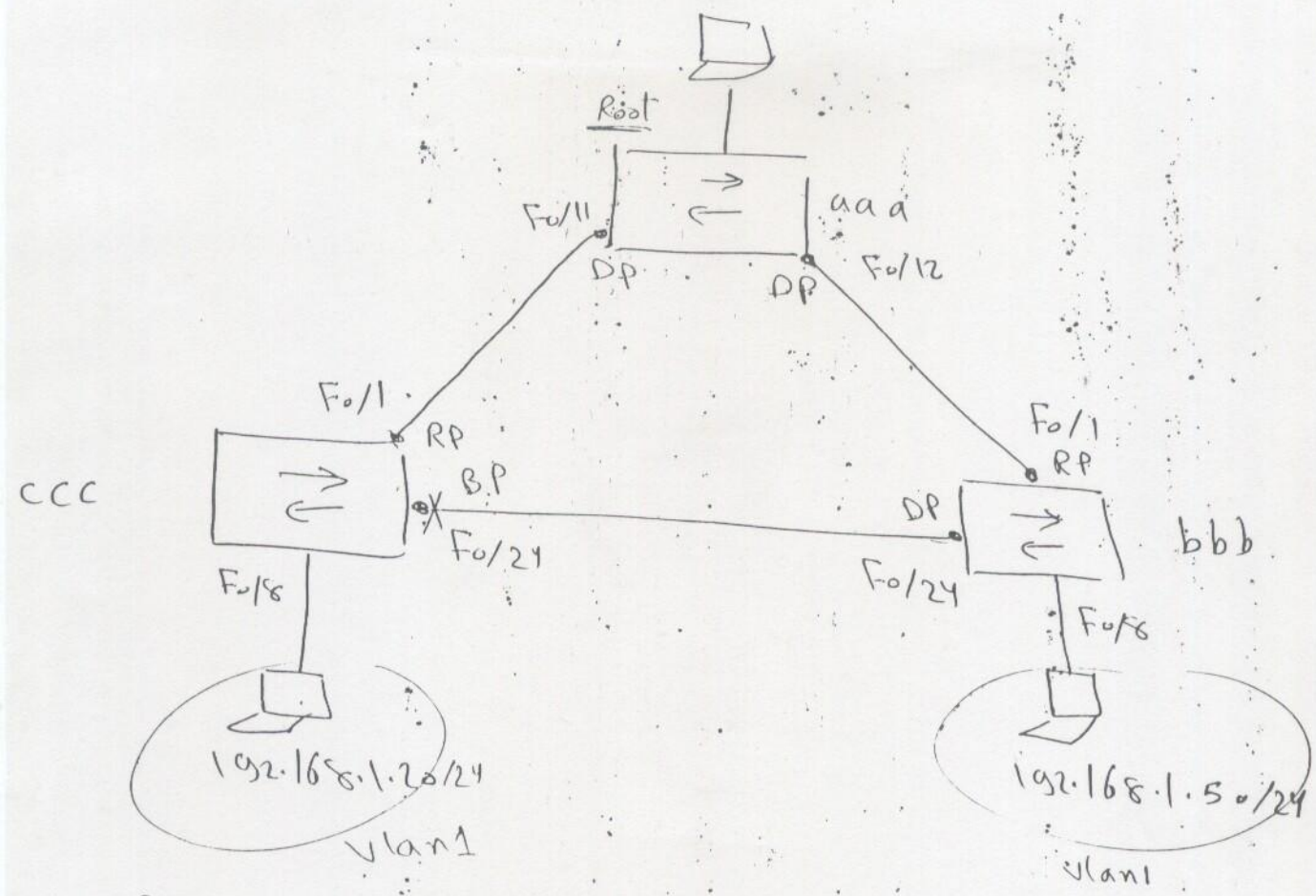


∴ Convergence time = 30 → 50

RSTP : "Rapid spanning tree protocol"

- RSTP speed the recalculations of ~~spaning~~ stp whe network topology change
- For stp convergence time = 30 → 50 sec so it enhance the convergence time to 2 sec
- RSTP elects a backup port for each RP & DP.

LAB



→ if you need switch B to be the Root

B(config)# spanning-tree vlan 1 root primary

ولو أردت أنه تمنع ال priority أقل ليكون هو Root

B(config)#spanning-tree vlan 1 priority ---- قيمة

لو عندك vlan 10, 20, 30 وأردت أنه يكون switch B هو ال Root

لكل منهم

B(config)#spanning-tree vlan 10, 20, 30 root primary

- كما تعلم عندما يتحول الـ port من (Blocking state) إلى (Forwarding state)

فإنه يأخذ من 30 ← 50 ثانية لذلك

وجب عليك تشغيل RSTP حتى لا يأخذ معك

وقت أكثر من ثانيتين

1 قف على كل SW وأعطيه الأمر التالي

(config) # spanning-tree mode rapid-pvst

2 قف على كل access port وأعطيه الأمر التالي

التي تتصل بها pc's

int F0/8

(config-if) # spanning-tree portfast

---

trouble shooting

show spanning-tree

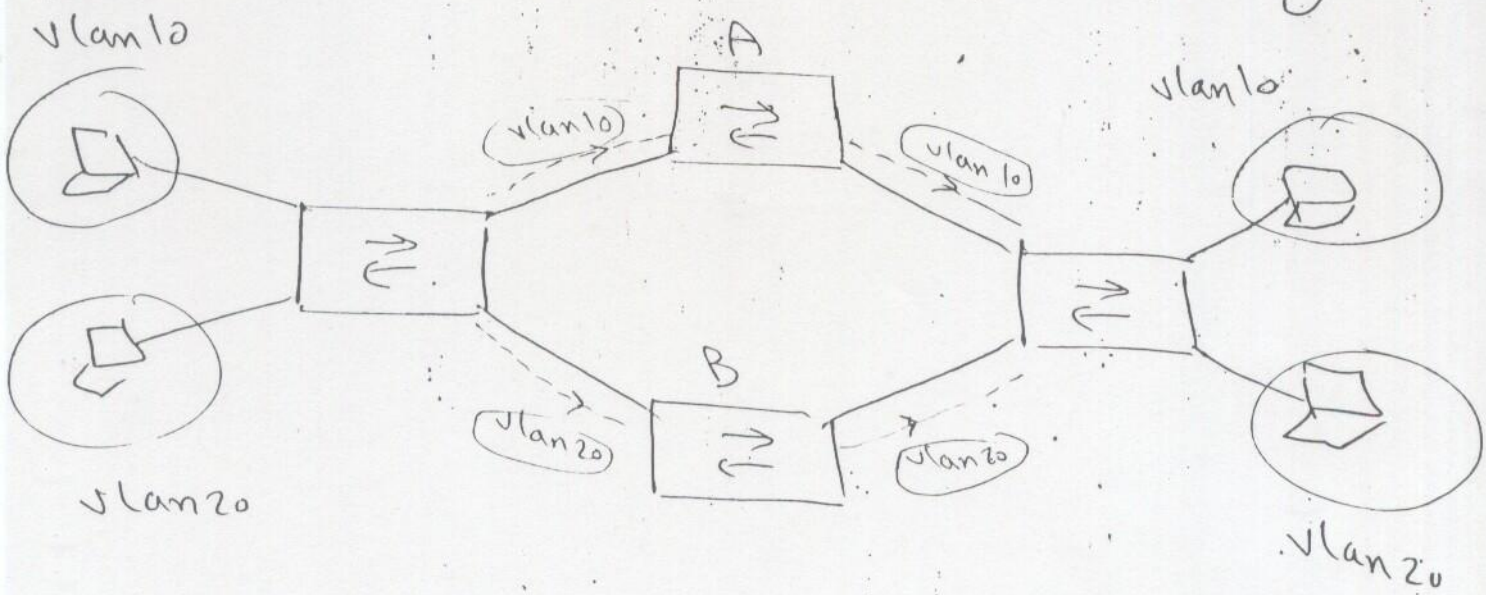
Per VLAN spanning tree [PVST]

- all modern cisco switches Run PVST

32768 → | Priority | Vlan | Mac-address |

- one Root bridge elected For each vlan
- helps load-balance more effectively

ex



- we need switch A to be The Root for Vlan 10 and switch B The Root of Vlan 20 to made load balance in 2 paths

The commands you need

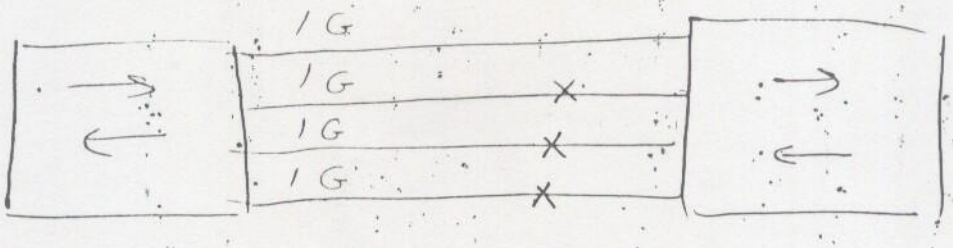
A(config) # spanning tree vlan 10 root primary ~~root~~

B(config) # spanning tree vlan 20 root primary

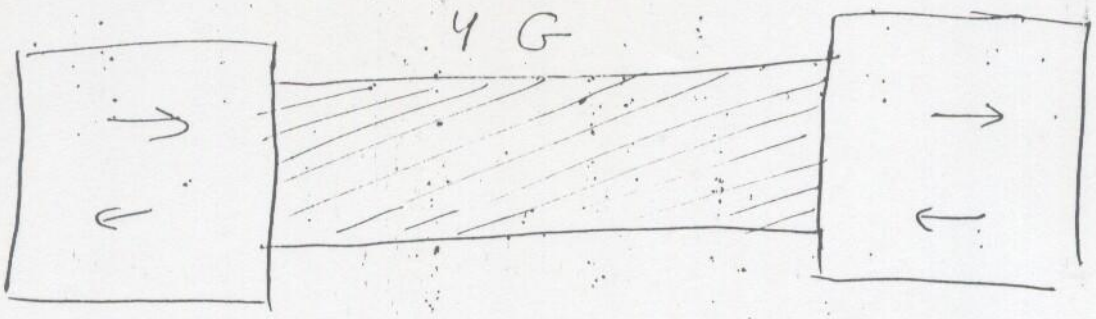
ether channel

what is Ether channel ?

it is away to take This ....



and make it look like This --



→ We have 2 negotiation protocol help you to make eTherchannel

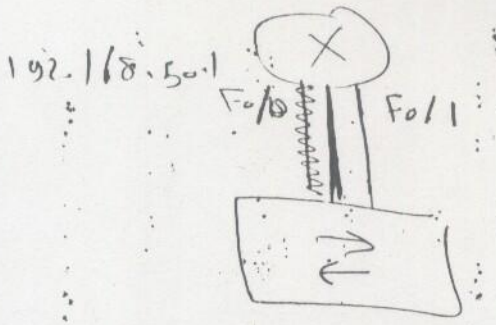
1 Port aggregation protocol [PAGP]

- cisco proprietary
- Port modes: auto, desirable, on

2 link aggregation protocol [LACP]

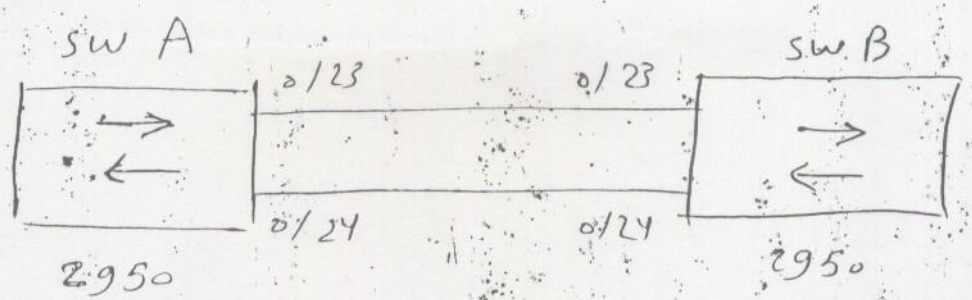
- industry standared [802.3AD]
- Port mode: Passive, active, on

ether channel bet. sw & Router




```
(config)# int port-channel 1
  if) # IP address 192.168.50.1 255.255.255.0
      int Fo/0
  if) # channel-group 1
      int Fo/1
  if) # channel group 1
```

configuration of L2 etherchannel



sw A

A (config) # int range F0/23 -24

A (config-if) # switchport mode trunk

A (config-if) # channel-protocol LACP ← optional

A (config-if) # channel-group 1 mode active

↑ أي رقم

sw B

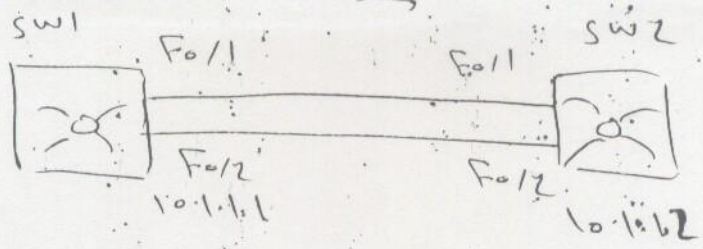
B (config) # int range F0/23 -24

B (config-if-range) # switchport mode trunk

B (config-if-range) # channel-protocol LACP

B (config-if-range) # channel-group 1 mode active

L3 : ether channel



sw1 (config)# int portchannel 1

if)# no switchport

IP address 10.1.1.1 255.255.255.0

int range F0/1 2-2

if-range)# channelgroup 1 mode desirable

لم يقبل

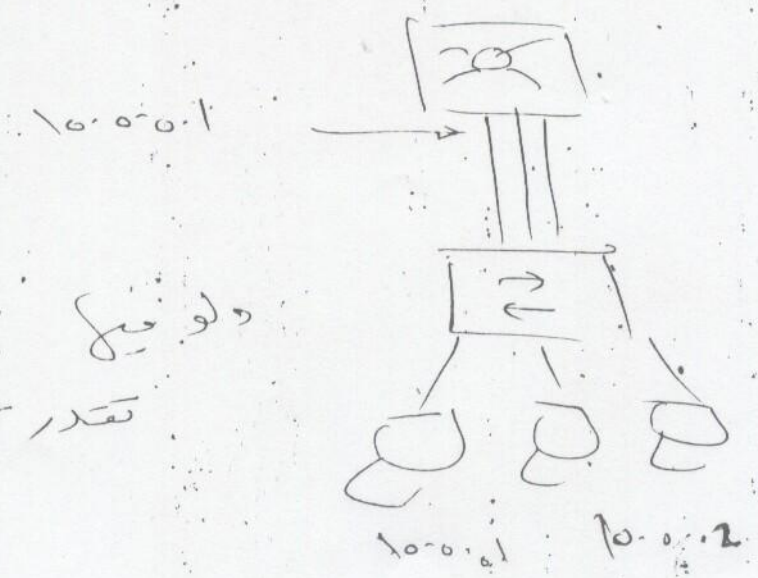
)# no switchport

يقبل هذه المرة

وكذلك

sw2

اشكال الصحيح الصحيح والتصميم



ولو فيه vlan

تقدر تلعب برضه

ether channel troubleshooting

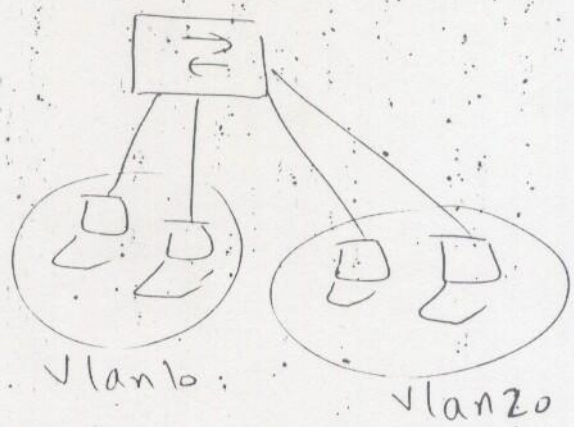
```
# sh int port-channel 1
# sh ether channel
# sh ether channel summary
# sh ether channel port-channel
```

best pratice :

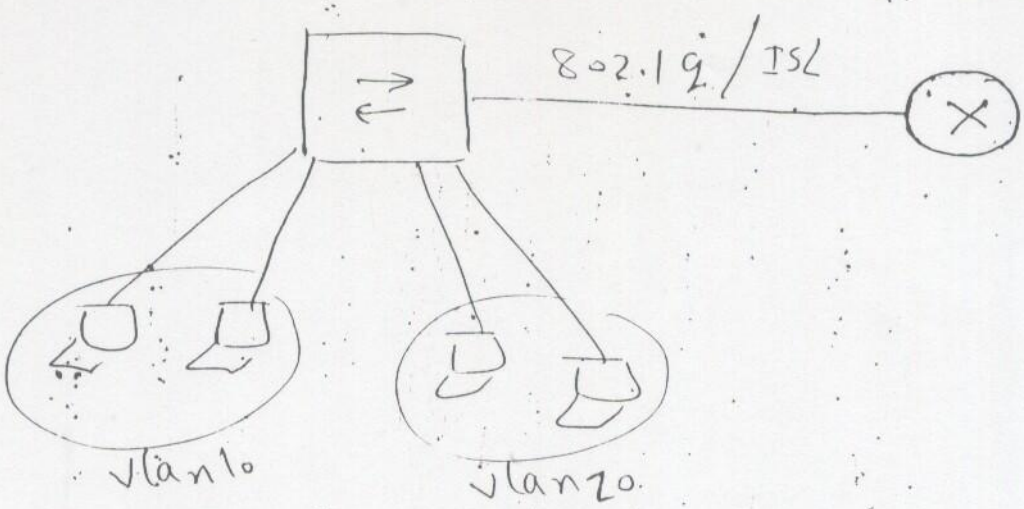
- all ports must use same speed & duplex
- interfaces in Bundle (حزمة) are redundant
- no interfaces in Bundle can be a span ports
- interfaces in a bundle must be in same vlan / trunk
- any changes to port channel affects all Bundled ports
- any changes to individual ports affects only That ports

L3 switching

* The problem: clients need Routing between vlans

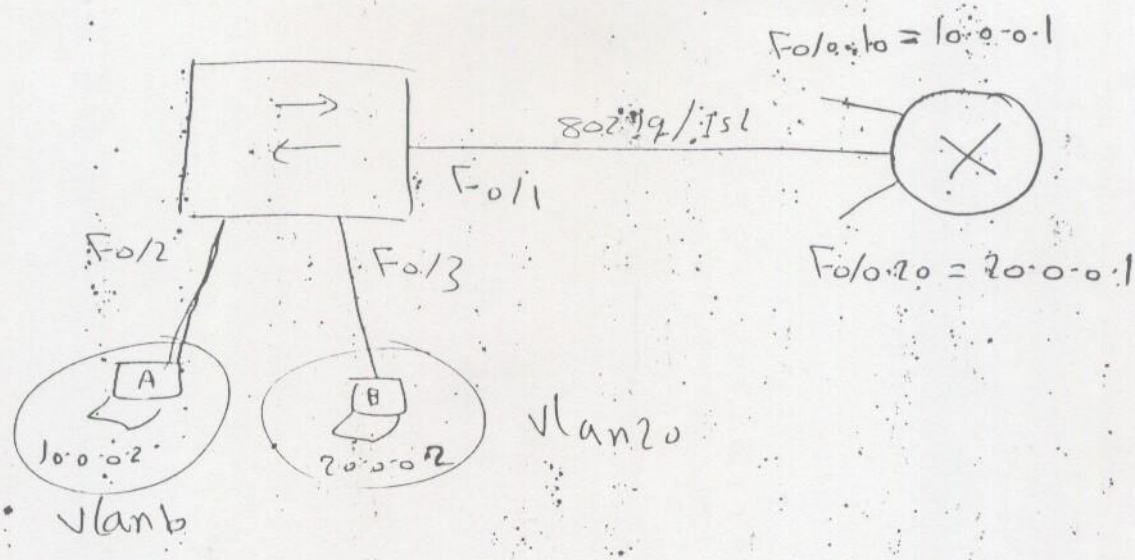


Solution # 1: [Router on a stick]



advantages:	disadvantages:
- simple to setup	- congestion on link
- lower cost	- single point of failure
	- delay of Routing

Configuring Router on stick



1 switch

switch(config)# int F0/2

- if)# switchport mode access
- if)# switchport access vlan 10

int F0/3

if)# switchport mode access

if)# switch port access vlan 20

int F0/1

if)# switchport mode trunk

if)# switch port trunk encapsulation dot1q

2 Router

```
Router(Config)# int Fo/0
    if)# no shutdown
    if)# int Fo/0.10
-subif)# encapsulation dot1q 10
-subif)# IP address 100.0.1 255.0.0.0
subif)# int Fo/0.20
subif)# encapsulation dot1q 20
subif)# IP address 20.0.0.1 255.0.0.0
```

VlanID

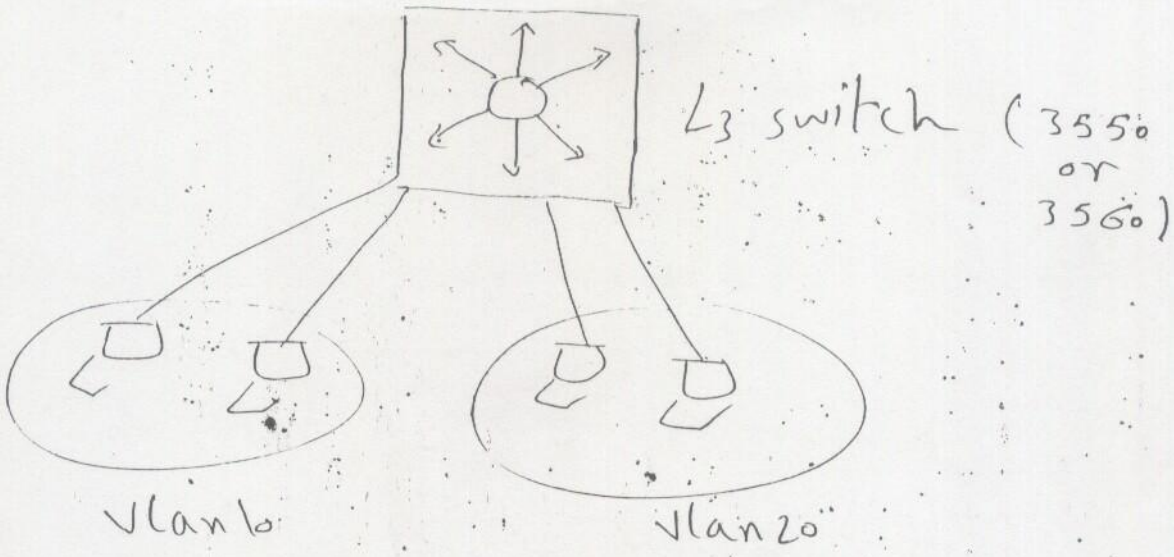
بعد ذلك :

قف على PC A وقم بعمل Ping 20.0.0.2

10.0.0.2

سوف تجد رد عليك

solution #2: multilayer switching



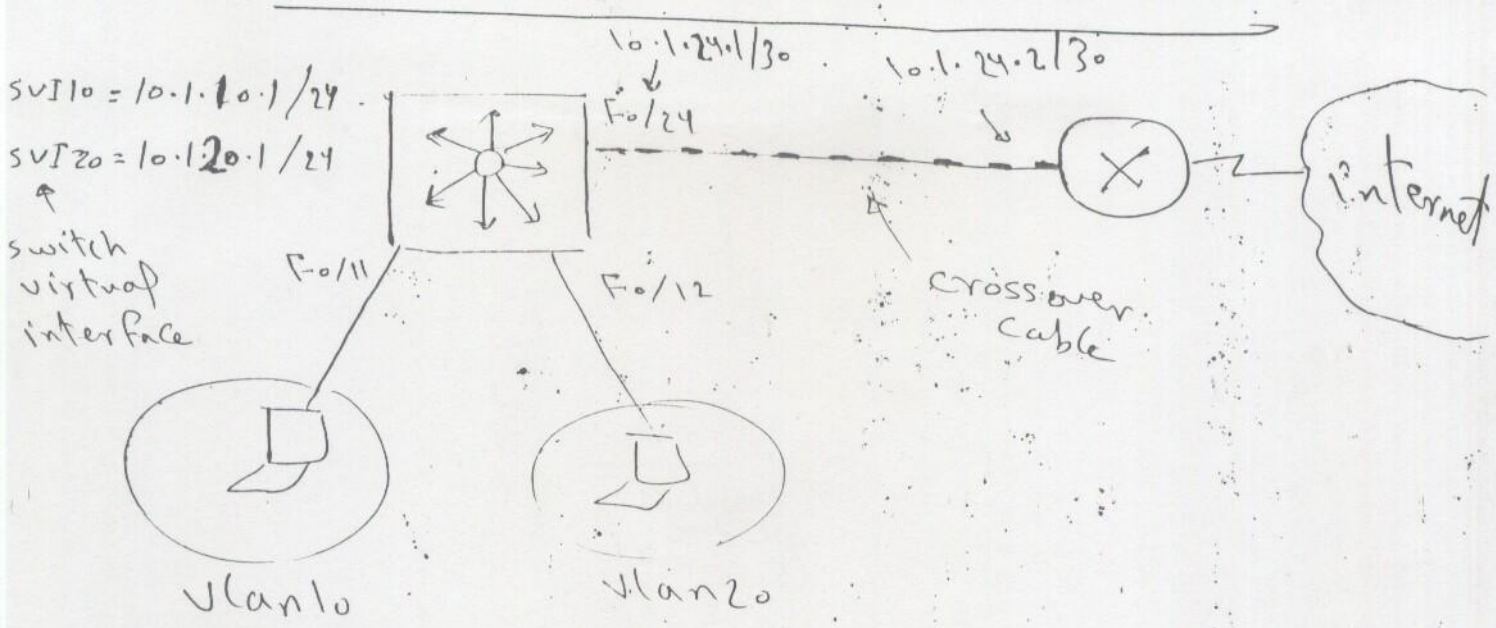
* advantages

- Routing at wire speed
- back plane BW
- Redundancy-enabled

* disadvantages

- Cost

multi-layer switch Configuration



① switch

```
(config) # int F0/11
    if) # switchport mode access
    if) # switchport access vlan 10
        int F0/12
    if) # switchport mode access
    if) # switchport access vlan 20
        int vlan10
    if) # IP address 10.1.10.1 255.255.255.0
        int vlan 20
    if) # IP address 10.1.20.1 255.255.255.0
(config) # IP routing →
```

لا يتم عمل Routing

int vlan20 & int vlan10 بين

```
int Fo/24
(config-if) # no switch port
    if ) # IP address 10.1.24.1 255.255.255.252
```

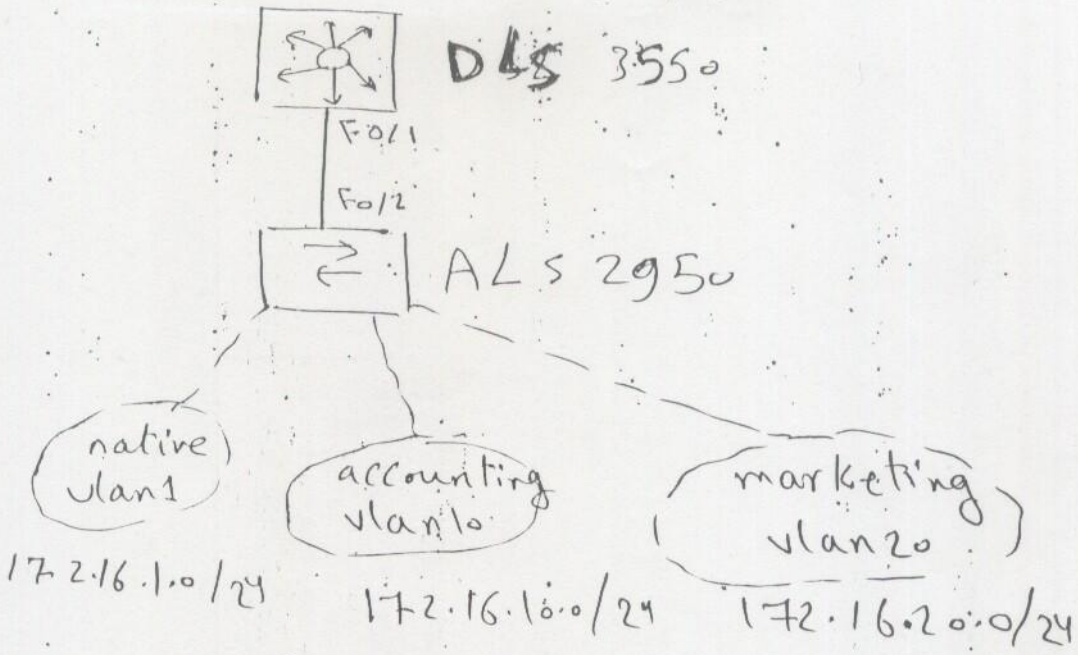
Router & L3 switch ثم Routing ثم تفعيل

```
(config) # router eigrp 1
    router) # no auto-summary
    router ) # network 10.0.0.0
        exit
(config) # IP route 0.0.0.0 0.0.0.0 10.1.24.2
```

Trable shooting

```
# sh IP int brief
# sh IP route
```

ex configure This LAB



DLS 3550

```
(config) # int vlan 1
    if) # no shut down
    if) # ip address 172.16.1.1 255.255.255.0
        int vlan 10
    if) # no shut down
    if) # ip address 172.16.10.1 255.255.255.0
        int vlan 20
    if) # no shutdown
    if) # ip address 172.16.20.1 255.255.255.0
        int F0/1
    if) # switch port mode trunk
        exit
(config) # IP routing
```

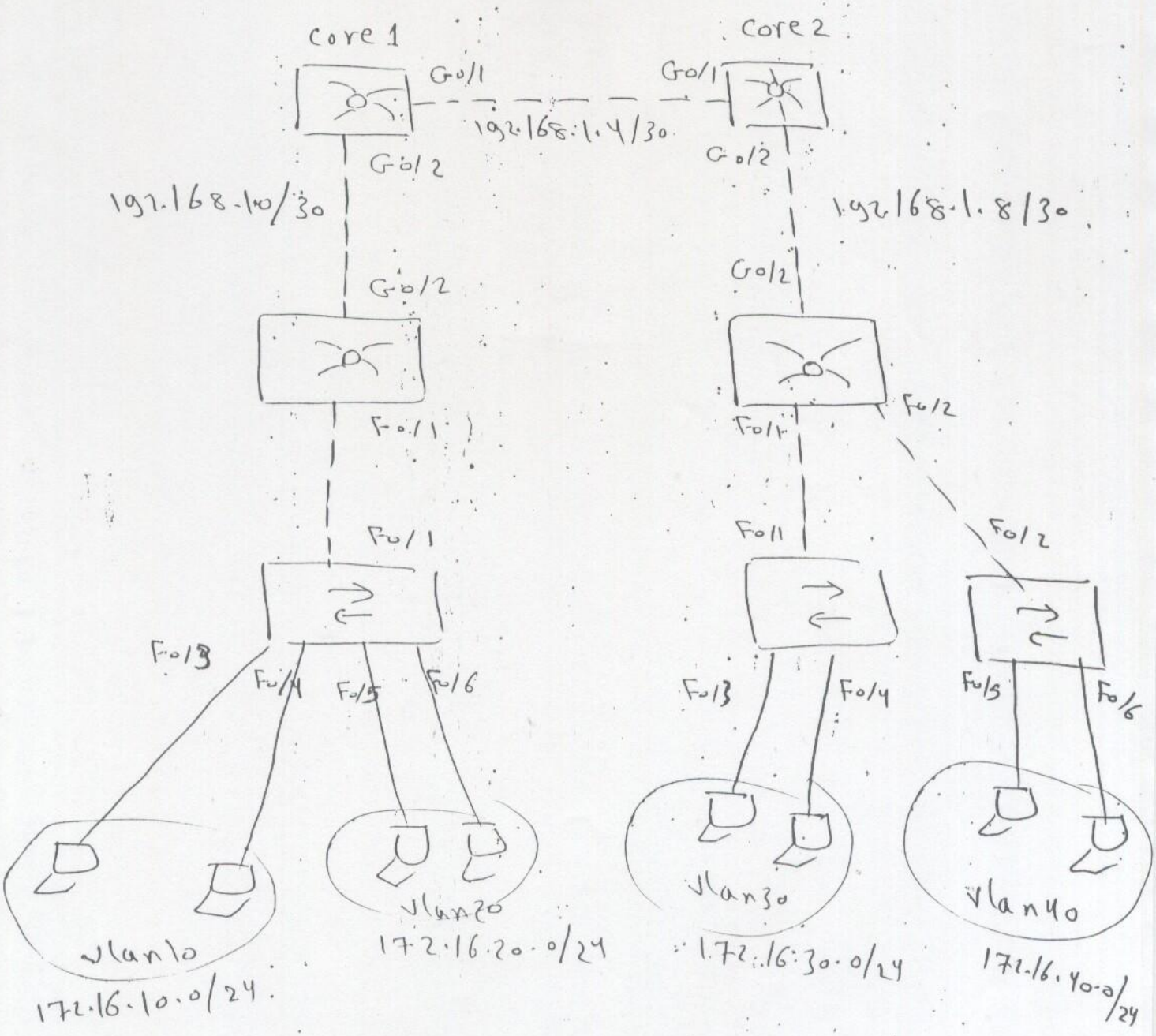
(ALS 2950)

int Fo/2
if) # switch port mode trunk

وبعد ذلك ضع كل port في ال vlan الخاصة به

---

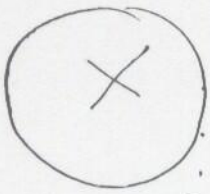
home work : design & configure This



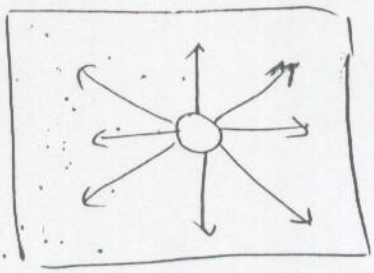
understanding CEF optimization

* L3 Routing Vs L3 switching

- Router & L3 switch Both have IOS software Routing
- software Routing is relatively slow compared to ASICs [application system IC's]
- L3 switch can play a little software-hardware trick

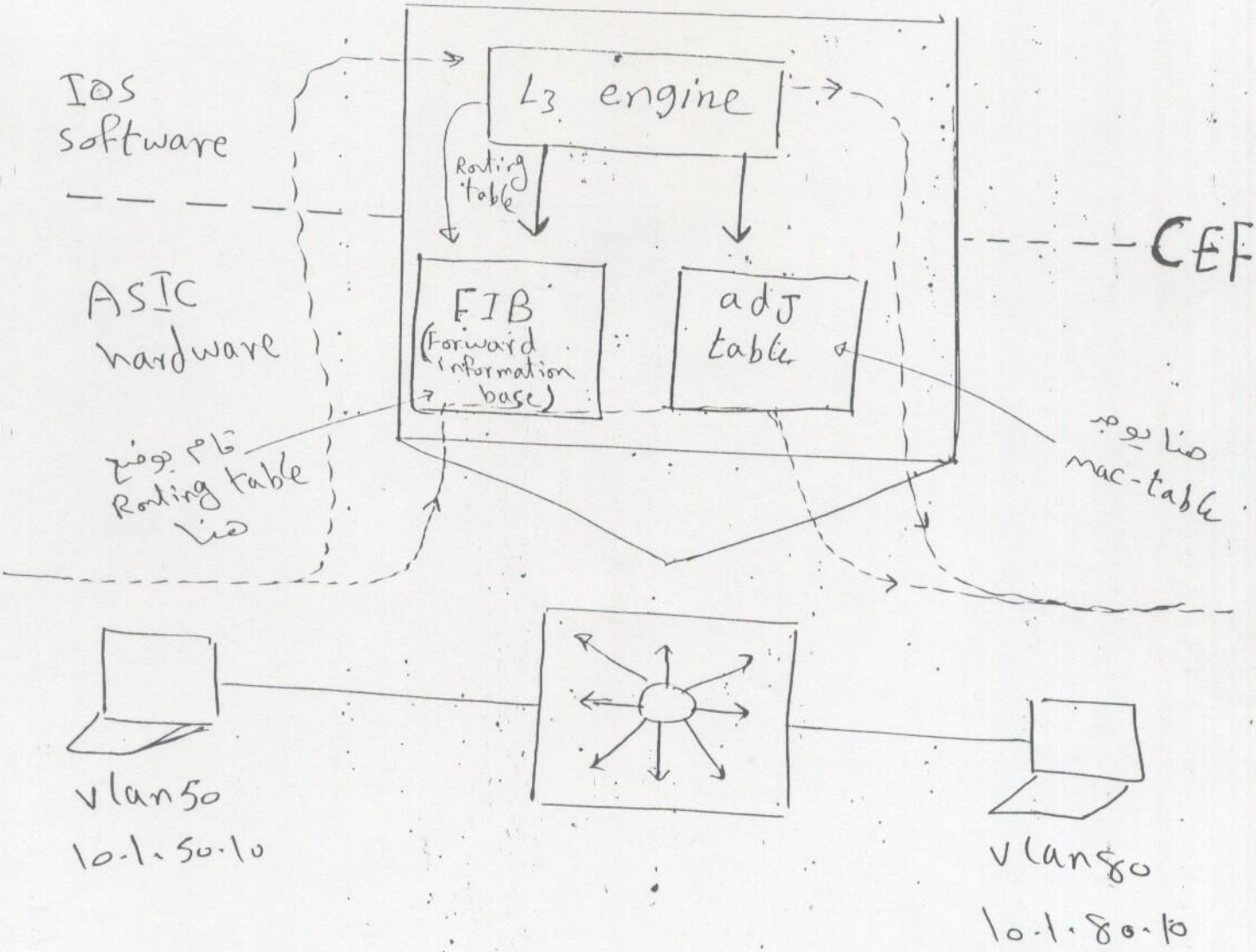


L3 Router



L3 switch

How cisco switches use CEF



- CEF is a technology on L3 switch to speed up Routing Process By making a cash memory called FIB [Forward information Base] and putting The Routing table in it

CEF configuration

- By default CEF is enabled on L_3 switches or you can enable it by command

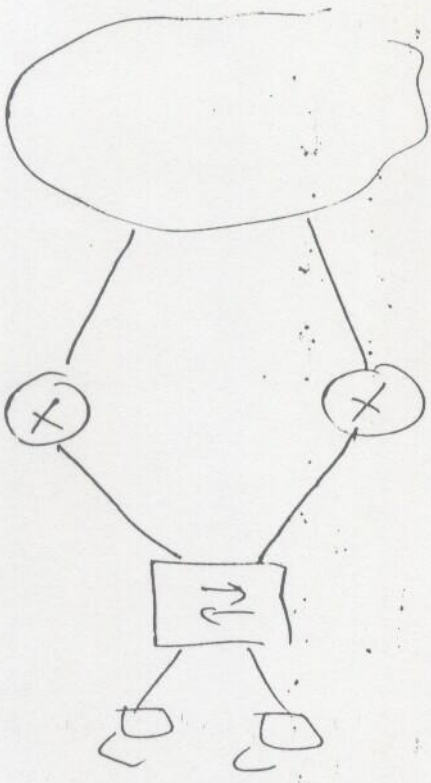
(config)# IP cef or (config)# IP routing

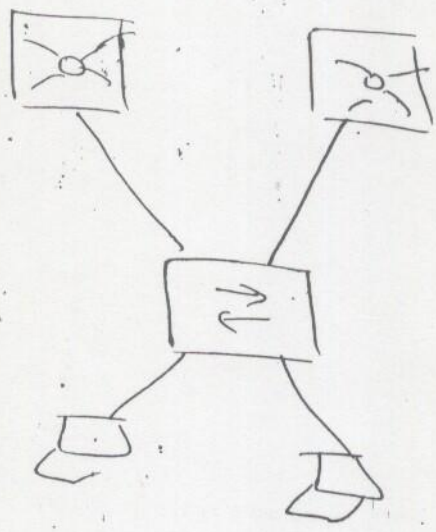
CEF trouble shoot

sh IP CEF summary

sh IP CEF vlan 200 → will show you The hosts IP in vlan 200

Redundancy





- redundancy is good
- if we have a gate way in our LAN & if This gateway is down how we make The backup gate way worked automatically ?
- we have 3 protocol help you to made This redundancy

① HSRP ② VRRP ③ GLBP

1 cisco Hot-standby Router protocol [HSRP]

- created by cisco for cisco in 1994
- uses default hello timer of 3 sec with a hold down timer 10 sec.

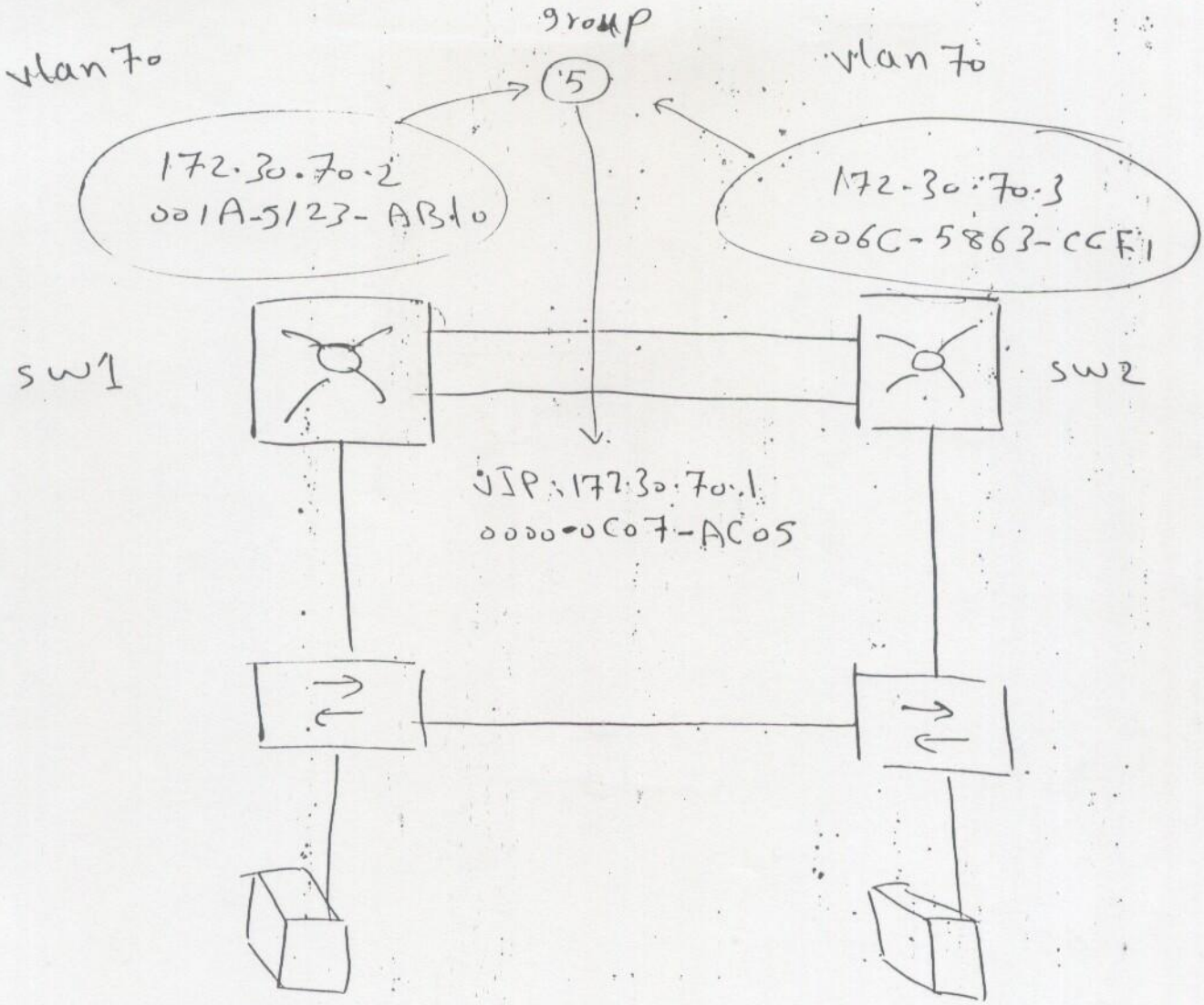
2 virtual Router redundancy protocol [VRRP]

- created by the ietf in 1999
- works between multiple vendors
- has faster timers than HSRP by default
  hello = 1 sec & holddown timer = 3 sec

3 Gateway load balancing protocol [GLBP]

- created by cisco for cisco in 2005
- identical features to HSRP but allow an active-active connection that adds load balancing

explain HSRP



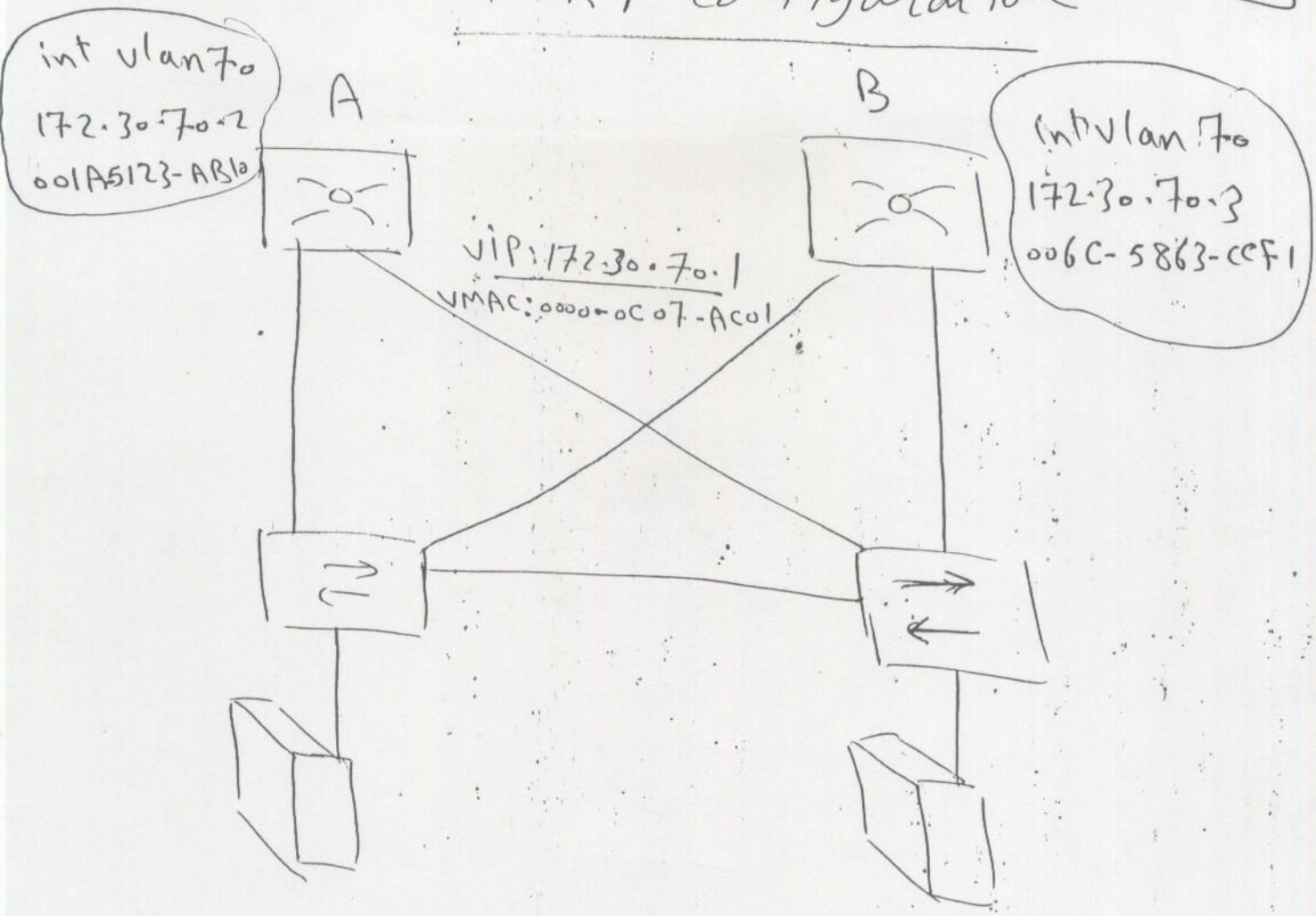
- gateway organized into standby groups
- one gateway active, other is standby state
- phantom [virtual] Router IP and mac-address generated
- hello msg sent once every 3sec & dead after 10sec

→ mac-address structure

0000-0C 07-AC xx

- 0000-0C → cisco vendor ID
- 07-AC → HSRP ID
- xx → standby group Number (05)

HSRP configuration



step① : create standby group

step② : reassign IP address

step③ : verify

step④ : optimize & tune

phantom IP

A(config)# int vlan 70

if)# standby 1 IP 172.30.70.1

group No.

if)# standby 1 priority 150

hint : by default priority = 100 (higher is better)

∴ أقوى من ذلك خلي A sw يكون ال primary GW

ولو وقع يكون C sw هو secondary GW

---

switch C

C (config)# int vlan 70

if)# standby 1 IP 172.30.70.1

ثم بعمل telnet 172.30.70.1 سوف تدخل

على sw A

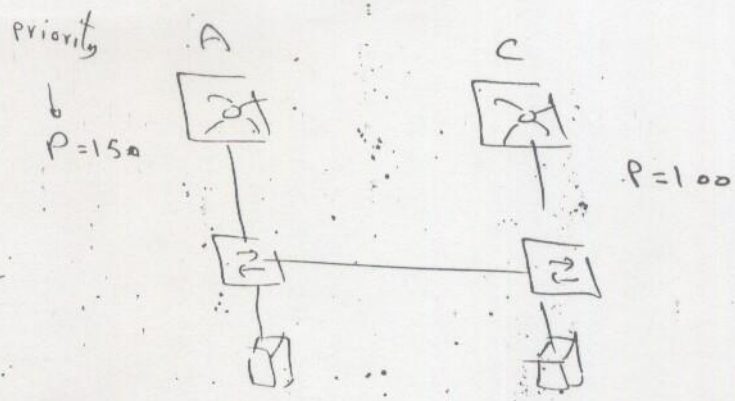
---

troubleshoot

sh standby

tuning & optimizing HSRP

① preemption :



→ if A down
C will be active switch
and if A up again
C still The active sw

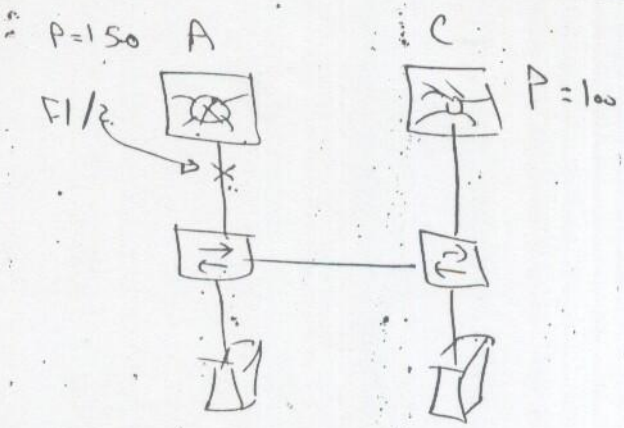
→ to made A The active switch you must use preemption

A(config) # int vlan 70
if) # standby 1 preempt

وكذلك على sw C :

c (config) # int vlan 70
if) # standby 1 preempt

② tracking



→ if F1/2 ~~goes~~ go's down
decrease The priority of
switch A by 60

A(config) # int vlan 70
if) # standby track F1/2 60

③ timers

C (config)# int vlan 70

if)# standby 1 preempt delay reload 180

يعني يا سويتش: لما تعمل reload لا تشغل preempt إلا لما

يعدي عليك 180sec

---

if) # standby 1 timers 1 3

hello time

dead interval

لا تتكلم في ال deadinterval & hellotime

② VRRP terminology shift

- active / standby becomes master / backup
- standby group becomes VRRP group
- master Router can share virtual IP
- one sec hello timer, 3 times hello = down timer

VRRP Configuration

```
(config)# int vlan 70
    if)# VRRP 20 ip 172.30.70.1
    if)# VRRP 20 preempt
```

group No.

→ if you wan to change hello & hold down timers

```
if)# VRRP 20 timers advertise msec 100
```

∴ holddown timer = 3 × 100 msec = 300 msec

hello time

Troubleshooting

```
# sh VRRP
```

→ to change priority

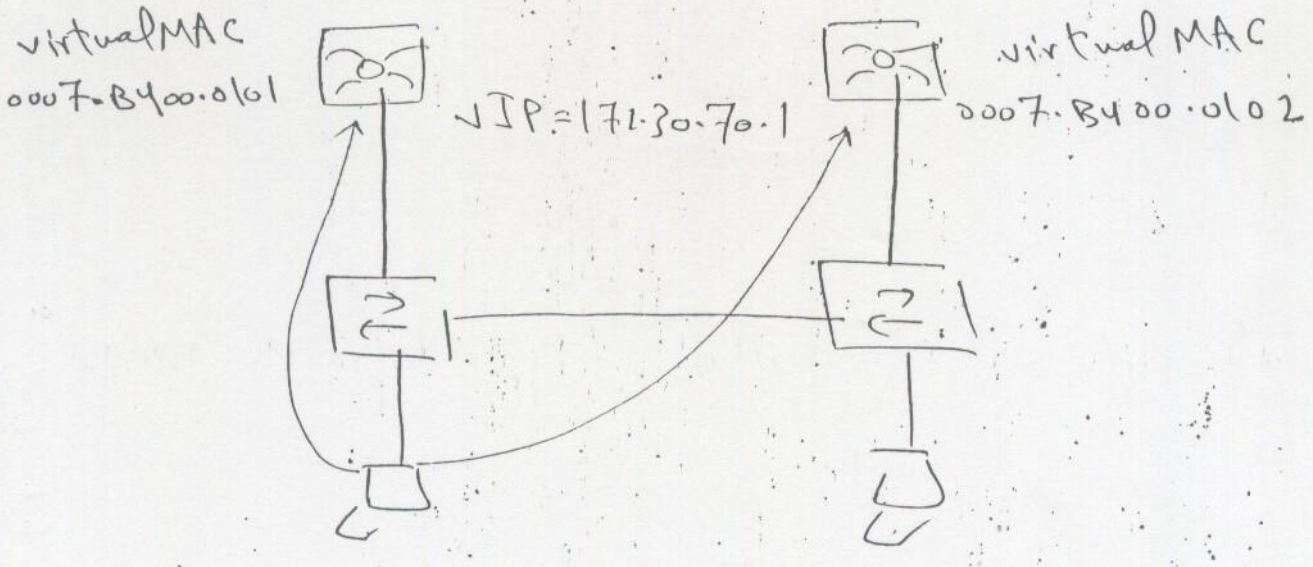
```
if)# vrrp priority 200
```

hint default = 100

③ GLBP

- you have the ability to make load balance between 2 gateways
- single virtual IP with multiple MAC's
- active virtual Gateway [AVG] acts as the "Point MAN"
- other Routers acts as active virtual Forwarder [AVF]

GLBP configuration




```
int vlan70
if) # glbp 1 ip 172.30.4.70
if) # glbp1 priority 150
if) # glbp 1 load-balancing round-robin
```

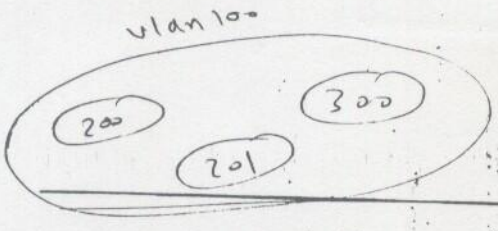
by default 125

Troubleshooting

```
# sh glbp
```

(config) # vlan 100

vlan) # private-vlan association 200,201,300



vlan 100 داخل 200,201,300 ① يضم كل من

~~(config)~~ : configuring port association

(config) # int range Fo/1 0 - 5

if-range) # switch port mode private-vlan promiscuous

vlan 100 هنا أي تقدر تصل إلى والى محتوى ال كل من 300,200,201) # switchport private-vlan mapping 100 200,201,300

هنا البورتات موصلة على أجهزة كمبيوتر

(config) # int range Fo/10 0 - 12

if) # switchport mode private-vlan host

if) # switchport private-vlan host-association 100 200

primary secondary

(config) # int range Fo/20 0 - 25

if-range) # switch port mode private-vlan host

) # switch port private-vlan host-association 100 201

(config) # int range Fo/15 0 - 18

range) # switchport mode private-vlan host

) # switchport private-vlan host association 100 300

Trouble shooting

sh vlan private-vlan

Campus security

Port security

1- Prevent many L2 attack

2- Can use secure mac-addresses

- Dynamic
- static
- sticky

3- limits The Number of mac-addresses Per Port

configuration

① if)# switchport mode access

② if)# switchport port-security

③ if)# switchport port-security maximum 1

④ if)# switchport port-security mac-address H.H.H

⑤ if)#switchport port-security violation
- → shutdown
- → restrict → drop & count
- → protect → drop only

if)# switchport port-security mac-address sticky

لو عندك ١٠ أجهزة مثلاً فبوصلهم على البورت المراد عمل port security عليه

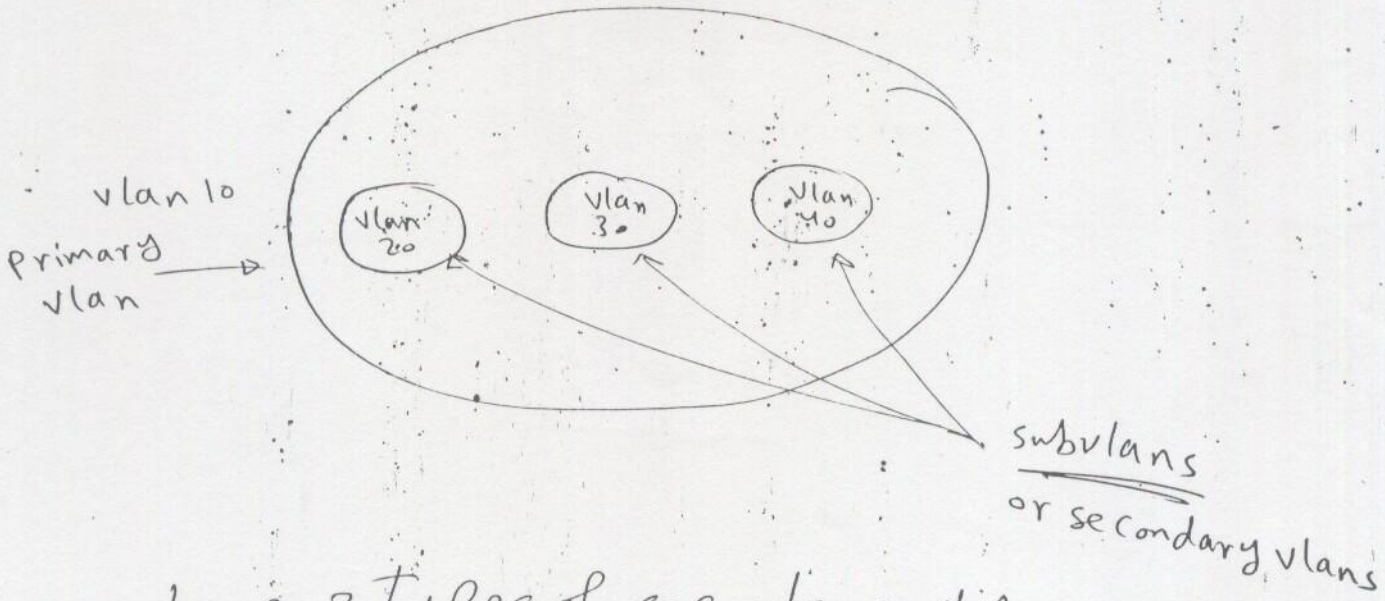
بدلاً ما تحفظهم واحد وراء الآخر استخدم هذا الأمر

Troubleshooting

sh int fo/1 switchport
sh interfaces status

Private VLAN

- Create VLANs within VLANs



→ we have 2 types of secondary VLANs

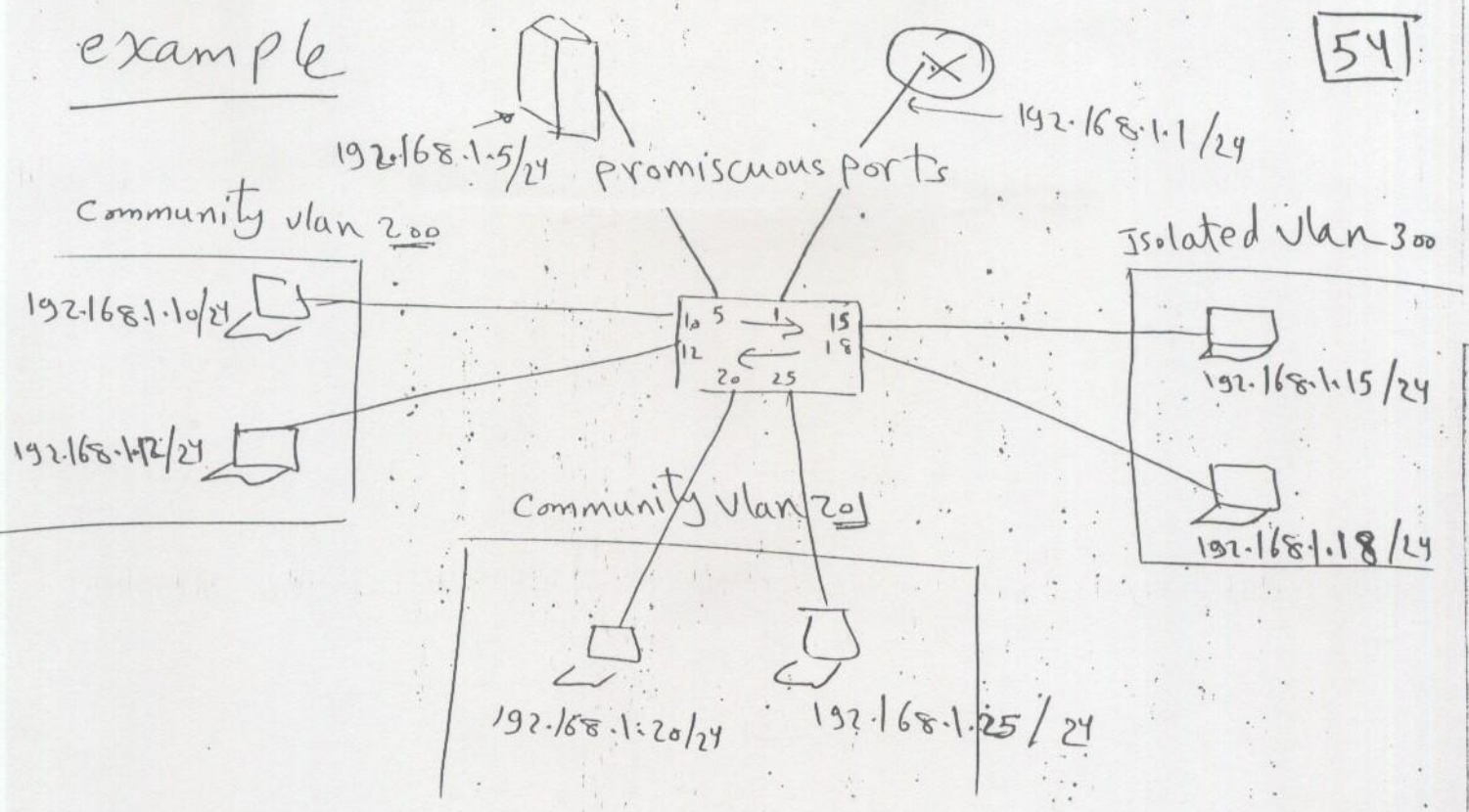
① Community VLANS

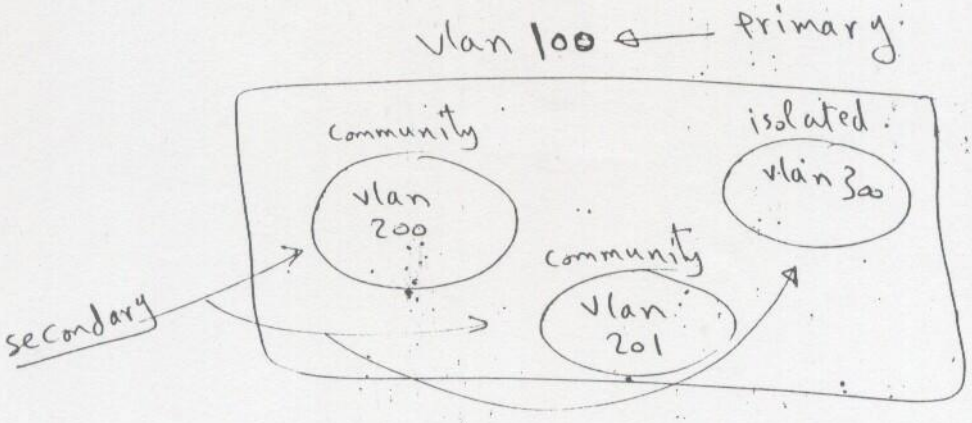
- Ports in This vlan communicate with other ports in The same community & promiscuous ports

② Isolated vlans

- These ports can only communicate with promiscuous ports.

example

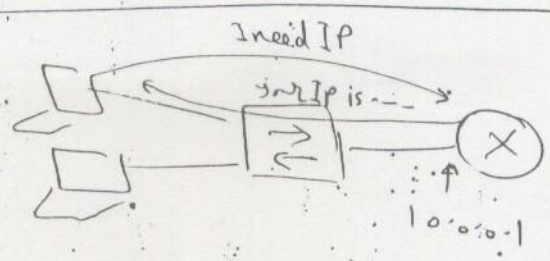





```
switch(config)# vtp mode transparent
(config)# vlan 100
    vlan)# private-vlan primary
(config)# vlan 200
    -vlan)# private-vlan community
(config)# vlan 201
    vlan)# private-vlan community
(config)# vlan 300
    vlan)# private-vlan isolated
```

لابد أن نكون
في هذا الـ mode
لا نستخدم في Private
Vlan

how to enable dHCP server on Router



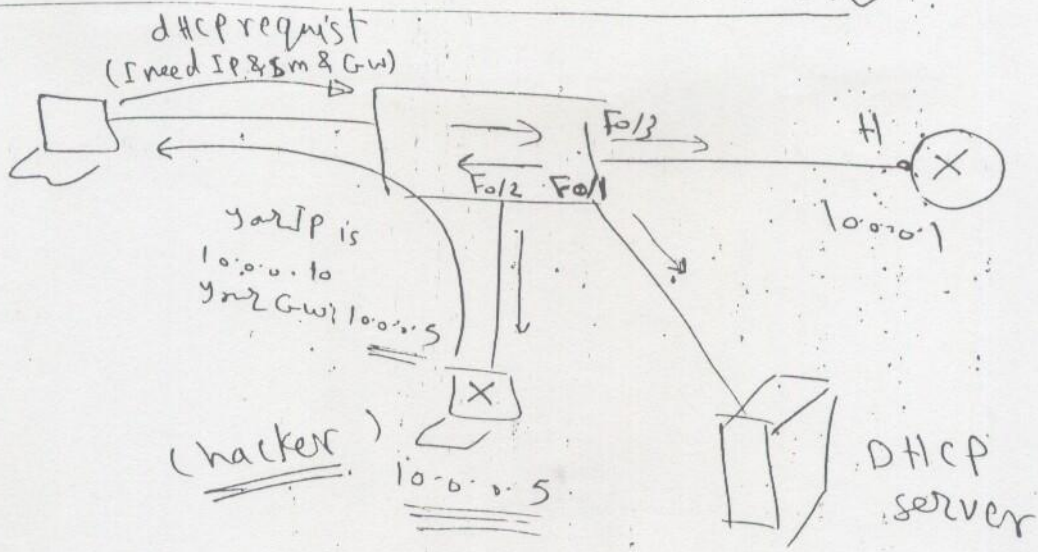

```
(config) # IP dhcp pool aa
    dhcp) # network 10.0.0.0 255.0.0.0
    dhcp) # default-router 10.0.0.1
    dhcp) # dns-server 8.8.8.8
          ) # exit
(config) # IP dHCP excluded address 10.0.0.1
```

هذا ال IP هو gateway IP وهو مستبعد من IP's التي

يوصل الروتر للأجهزة لأنه لا يصح أن يأخذ أحد ال IP

الخاص بالروتر

* MAN in The middle attack



→ to over come man in The middle attack, cisco provides (dHCP snooping).

→ dHCP snooping allows responses to only come from specific ports

(config) # IP dHCP snooping

(config) # int Fo/1

هذا البورت هو فقط لما حقه يرد على DHCP requist

(config-if) # IP dHCP snooping trust

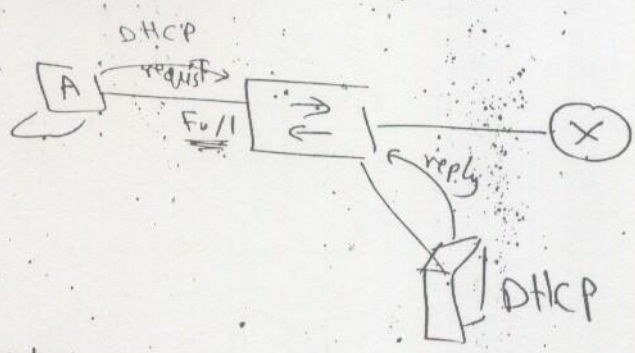
Trouble shooting

sh IP dHCP snooping binding

يظهر لك ال mac IP للأجهزة التي طلبت dHCP requist

* IP source guard

→ after your PC take an IP By dHCP



→ IP source guard make a thing like access-list in interface Fo/1 to Prevent any another MAC & IP address From Putting in interface Fo/1

```
(config) # int Fo/1
    if) # IP verify source vlan dHCP-snooping
```

→ Port-security

disadvantages of IP source guard

- in Large networks with alot of clients will made a large slowdown. يطرح الأداء العام

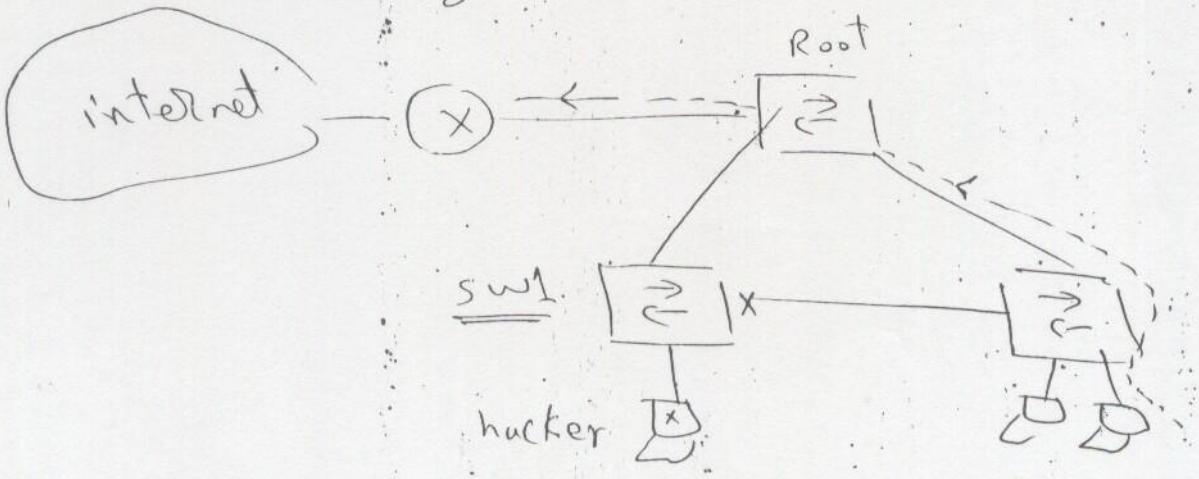
Spanning tree security

① Root guard

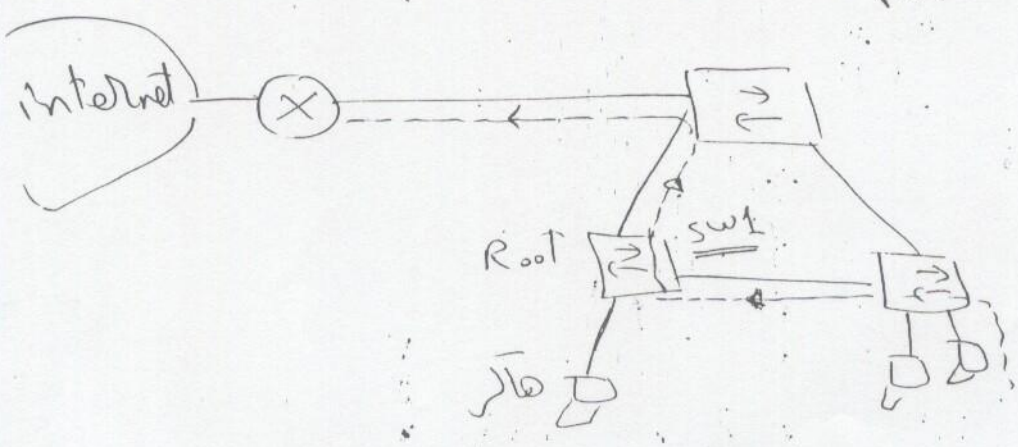
② BPDU guard

① Root guard

→ intruders can attempt to sabotage (يدمر) The Root bridge



← هكر الآن يقدر يخترق sw1 ويخليه هو ال Root عن طريق تقليل ال priority



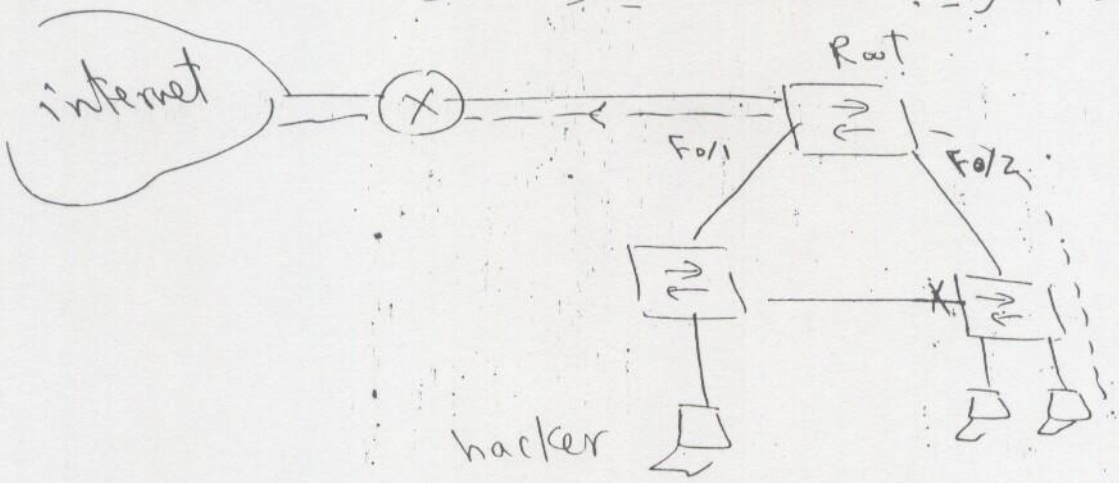
← وبالتالي سوف يمر كل ال traffic على (Root sw) وهو sw1

أى أن الهاكر جعل الـ traffic يمر بالـ switch القريب منه

وعندها يمكنه عمل sniff لهذا الـ traffic

- لذلك نستخدم الـ Root guard لمنع هذا الهاكر من جعل

الـ switch القريب منه أن يكون هو Root



Root (config)# int F0/1

if)# spanning-tree guard Root

لأقل إنا الـ Root مهما تميزت او priority في السويتشات الأخرى

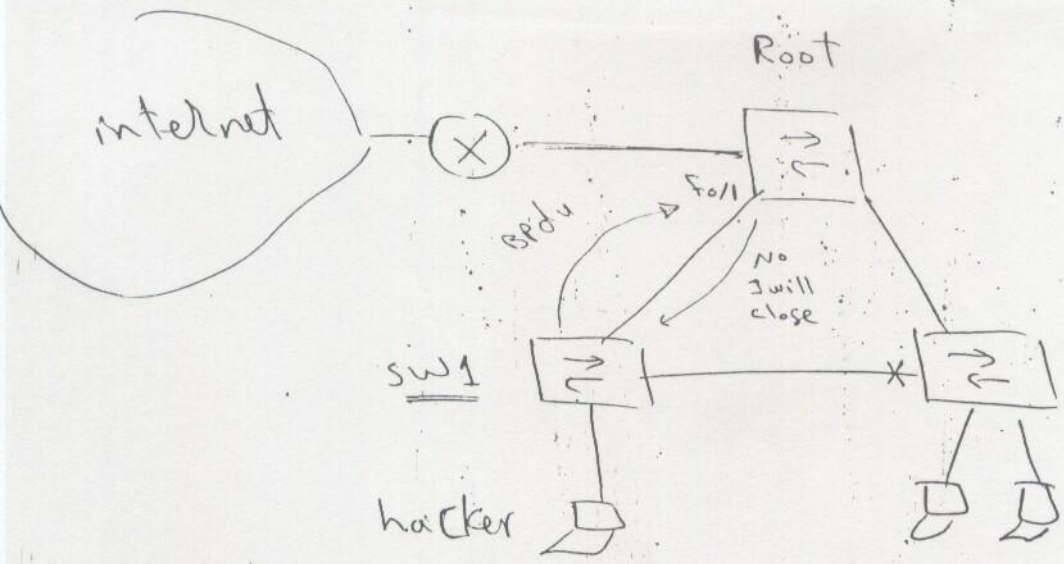
int F0/2

if)# spanning-tree guard Root

→ uplink fast must be disabled because it can't be used with root guard

(config) # no spanning-tree uplinkfast

② BPDu guard



لو كان لديك شك أن الهاكر يوجد على السي المتصل
بال Root switch على الفتحة Fo/1 كان لزاماً عليك
أن تقوم بعمل BPDu guard على Fo/1 على Root switch

```
int Fo/1
if) #spanning-tree BPDu guard enable
if) #spanning-tree port fast
```

لو شغلت (BPDu guard) على إحدى الفتحات لا بد أن تشغل معها portfast

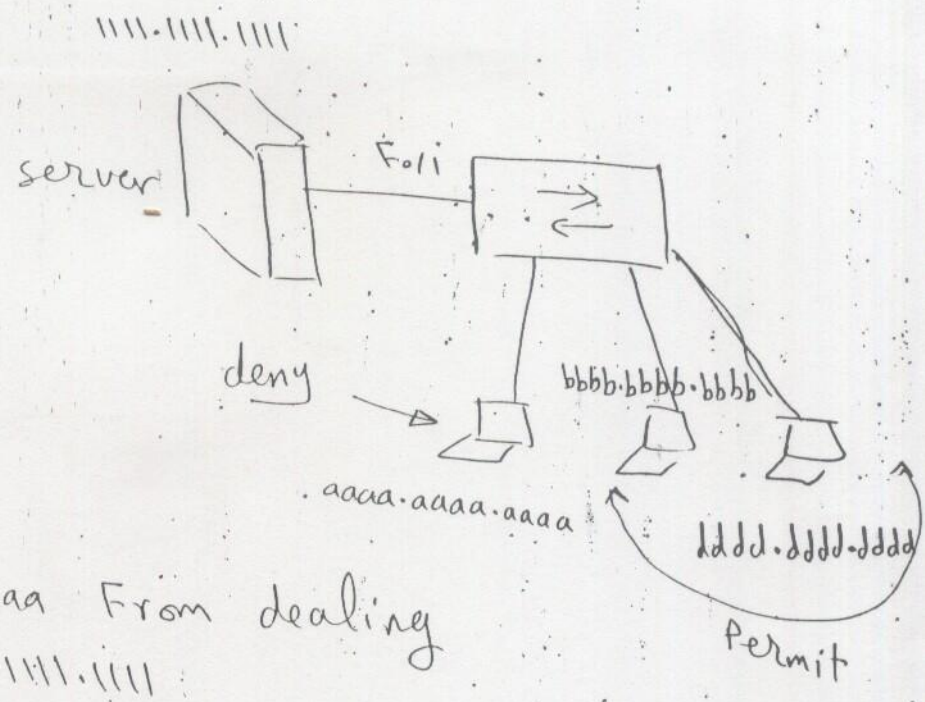
---

hint (config)#spanning-tree portfast bpdu guard default

يعني لو شغلت الـ (BPDu guard) على أحد البورتات سوف يعمل
الـ portfast بشكل تلقائي على ذلك البورت

mac access-list

example



→ deny aaaa.aaaa.aaaa From dealing with server 1111.1111.1111

solution

(config) # mac access-list extended aa

(config-ext-macl) # deny host aaaa.aaaa.aaaa host 1111.1111.1111

(config-ext-macl) # Permit any host 1111.1111.1111

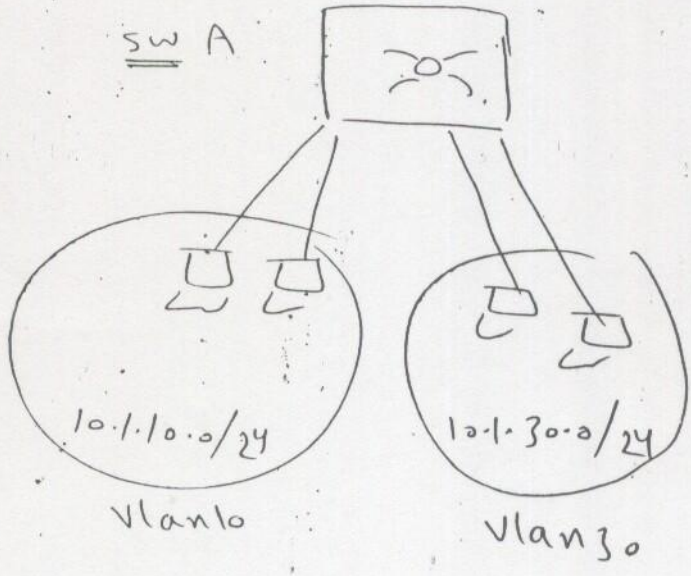
int F0/1

if) # mac access-group aa out

* VLAN Access-list [VACL]

- VACL allow you to Filter all traffic on a VLAN
- supported on multi-layer switch only
- typically Found in larger environments

example 1



- switch A has two vlans 10 & 30
- clients on vlan 10 should be restricted to 10.1.10.0/24 subnets

  يعني أي pc في vlan 10 لازم يكون
  الـ IP يتبع في subnet 10.1.10.0

- clients on vlan 30 should be restricted to 10.1.30.0 subnets

solution

```
(config) # access-list 1 permit 10.1.10.0 0.0.0.255
(config) # access-list 2 permit 10.1.30.0 0.0.0.255
```

(config) # vlan access-map zizo 10 ← sequence Number

(config-access-map) # match IP address 1 ← رقم الـ ACL

(config-access-map) # action Forward

(config) # vlan access-map zizo 20

access-map) # action drop ← deny any أي

vlan access-map لتفعيل هذه الـ ←

(config) # vlan Filter zizo vlan-list 10

أي طبق هذا الـ Filter على الناس اللي في vlan 10

ونفس الكلام للناس اللي في vlan 30

(config) # vlan access-map mido 10

access-map) # match IP address 2

access-map) # action Forward.

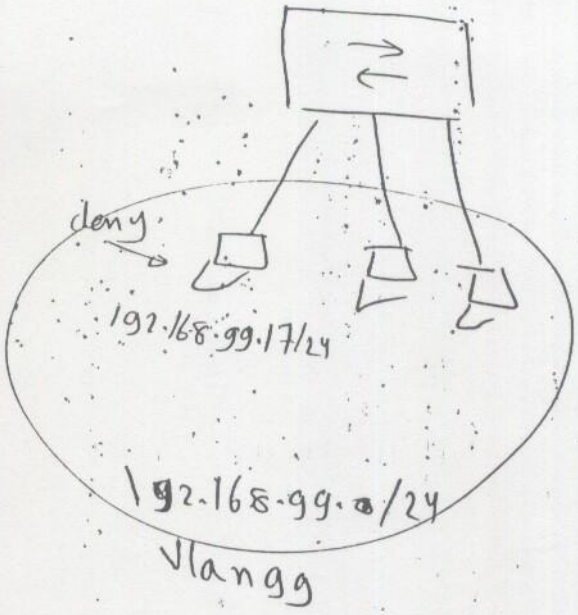
(config) # vlan access-map mido 20

access-map) # action drop

(config) # vlan Filter mido vlan-list 30

example 2

→ we need host 192.168.99.17/24 is not allowed to connect to any other host on its local subnet



نريد أن نمنع ذلك الجهاز من أن يتعامل مع باقي الأجهزة الموجودة في نفس الشبكة

```
(config) # access-list 100 permit IP host
```

→ 192.168.99.17 192.168.99.0 0.0.0.255

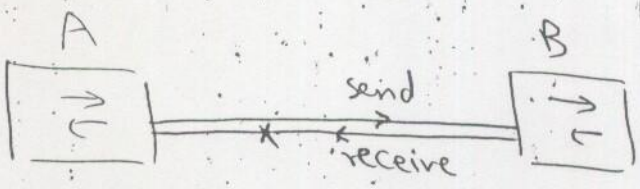
```
(config) # vlan access-map block 10
access-map) # match IP address 100 ← ACL رقم
map) # action drop
(config) # vlan access-map block 20
access-map) # action Forward
) # exit

(config) # vlan filter block vlan-list 99
```

1 Loop Guard

يوجد أسلوب بالـ
لحماية stp من أن يحدث
loop ولا

65

what is The mean of unidirectional link Failure?

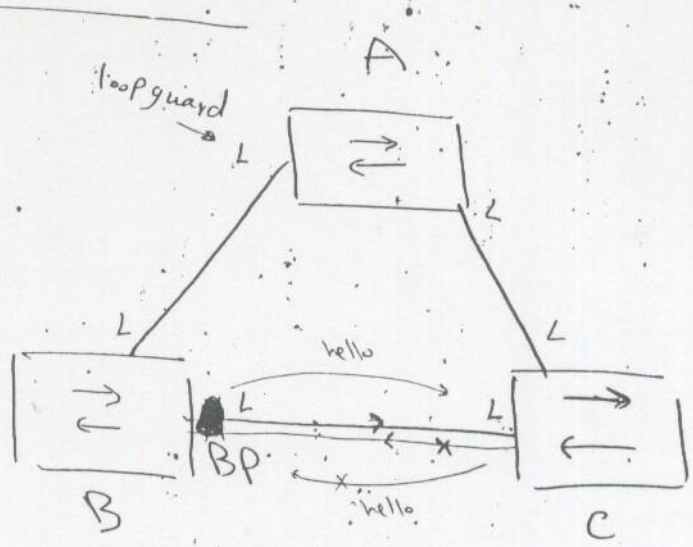


a hardware Failure happen in cable made switch A can send to switch B but can't receive or vise versa
العكس

وعادة ما تحدث هذه المشكلة في كابلات الفايبر

- loop guard stops loops caused by unidirectional link Failures

example



- A is Root bridge
- link between B & C is Blocked at (B)
- link between B & C goes unidirectional
- B releases The Block, one-way loop occures
- loop guard should be enabled (per port) on all switches uplinks

Loop guard configuration

(config) # int F0/1

(cf) # spanning-tree guard loop ← على كل الـ ints وعلى كل الـ switches

أو تستطيع إعطاء هذا الأمر

(cofig) # spanning-tree loopguard default

أي عندما يصير أي switch بـ unidirectional Failure

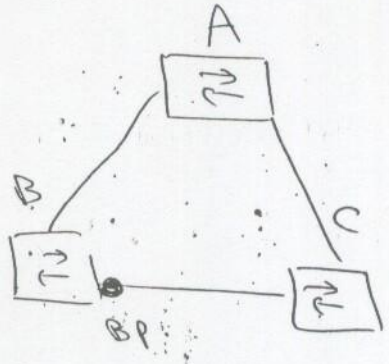
على أي بورت من بورتاته فإنه سوف يغلقه حتى لا يحدث Loop

وسوف يجعل البورت error disable

---

[2] unidirectional link detection [UDLD]

- different from loop guard, But same goal
- designed specifically For fiber
- sw A send a "L2 Ping" between neighbors
- configuration



(cnfig) # udld enable

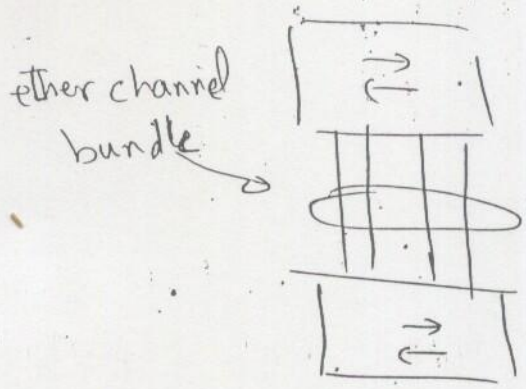
(cnfig) # int F1/2

(cofig-if) # udld port

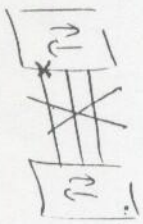
ملحوظة : من الفروقات الجوهرية بين UDLD & loop guard

1 UDLD ← صنع خصيصاً من أجل fiber cables

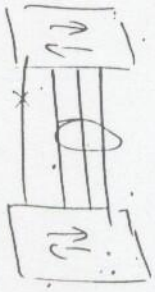
C



- if loop guard works on switches and a unidirectional failure happen on one cable of bundle, The etherchannel stops completely



- if UDLD works on switches and a unidirectional Failure happen on one cable of bundles The ether channel still working with other cables

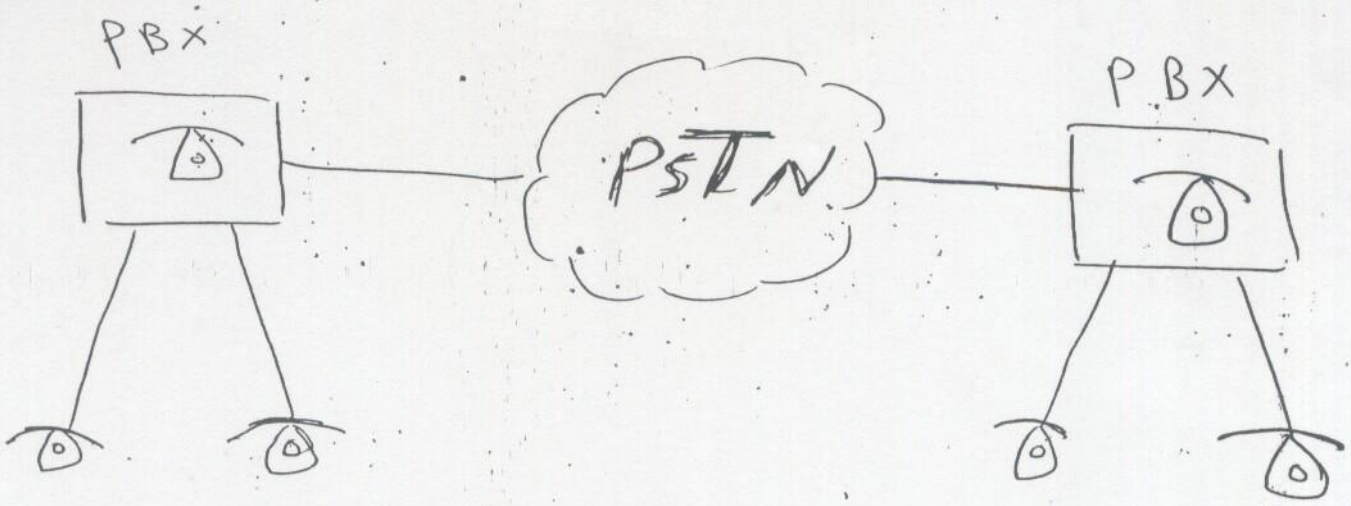


VoIP and QOS

→ why organization would use IP telephony?

- cost saving
- bandwidth & equipment efficiency
- moves, adds & changs
- lower cost of voice transmission
- new application & devices [always updated]

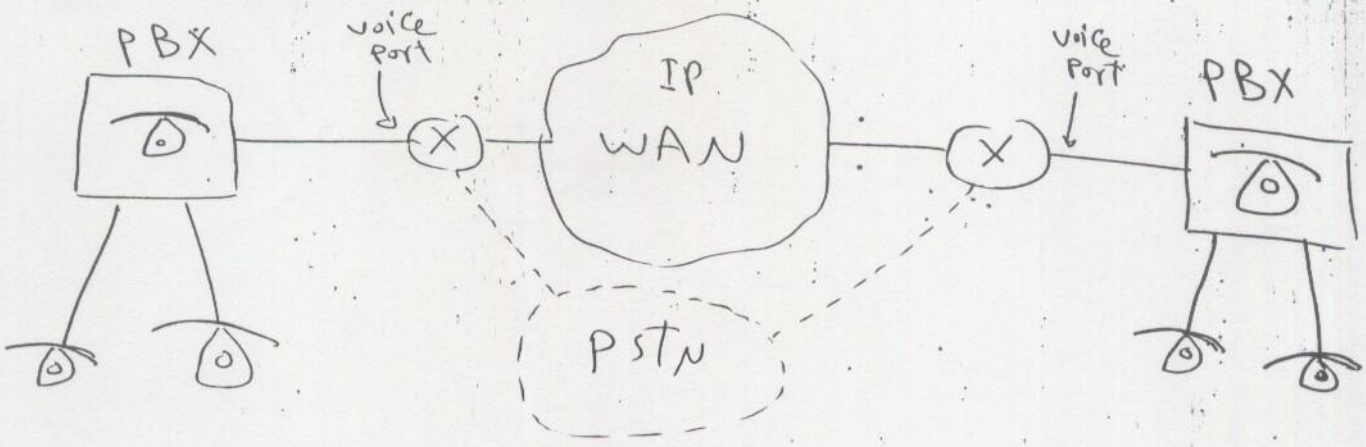
A VoIP



"example of analog phone network"

→ we have 2 ways for migration from analog voice to digital voice [voip]

I Phase 1. IP telephony



- keep PBX system & analog phones
- calles Routed over WAN Rather Than PSTN

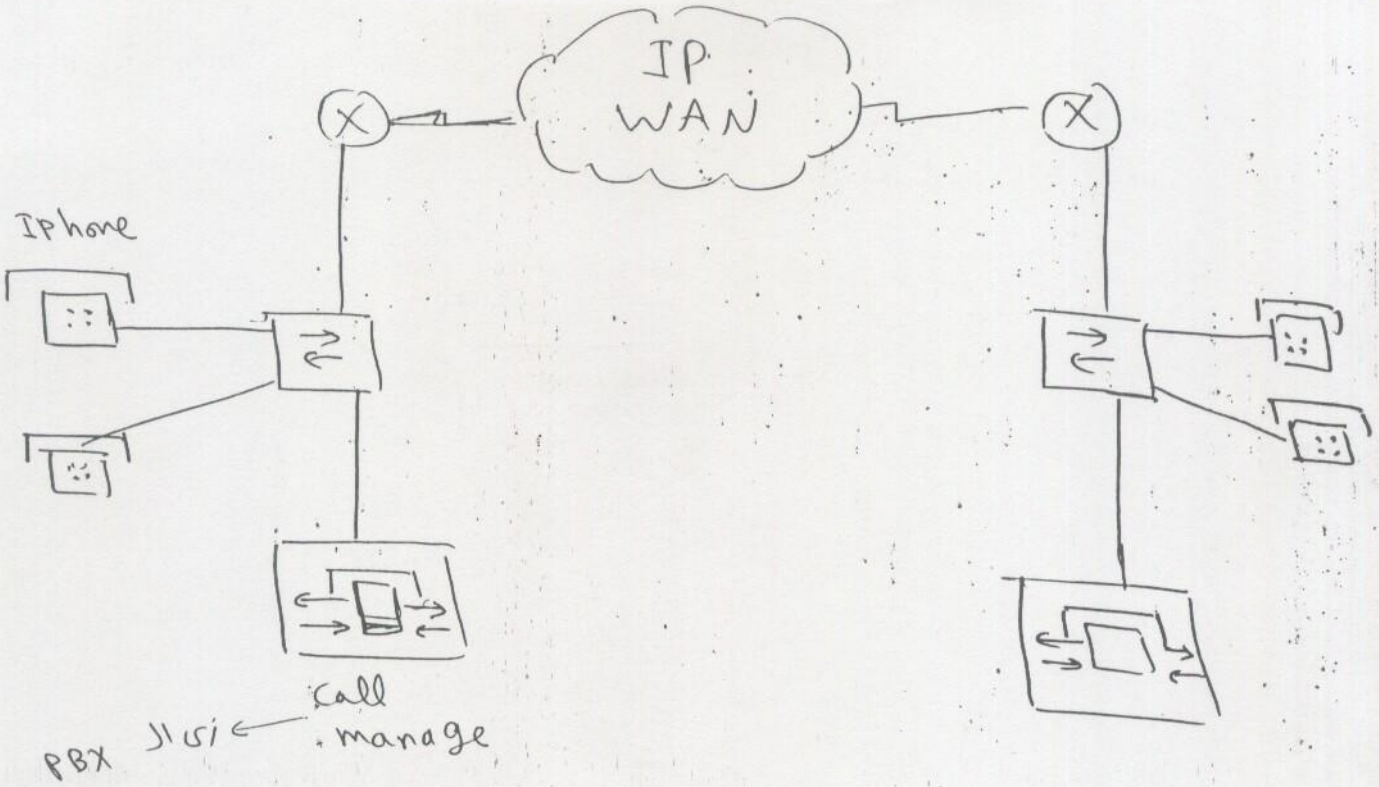
→ major benefit : free long distance

المكالمة مجاناً ولأي مكان بين الأفرع بتاعتك

→ major requirement : quality of service [QOS]

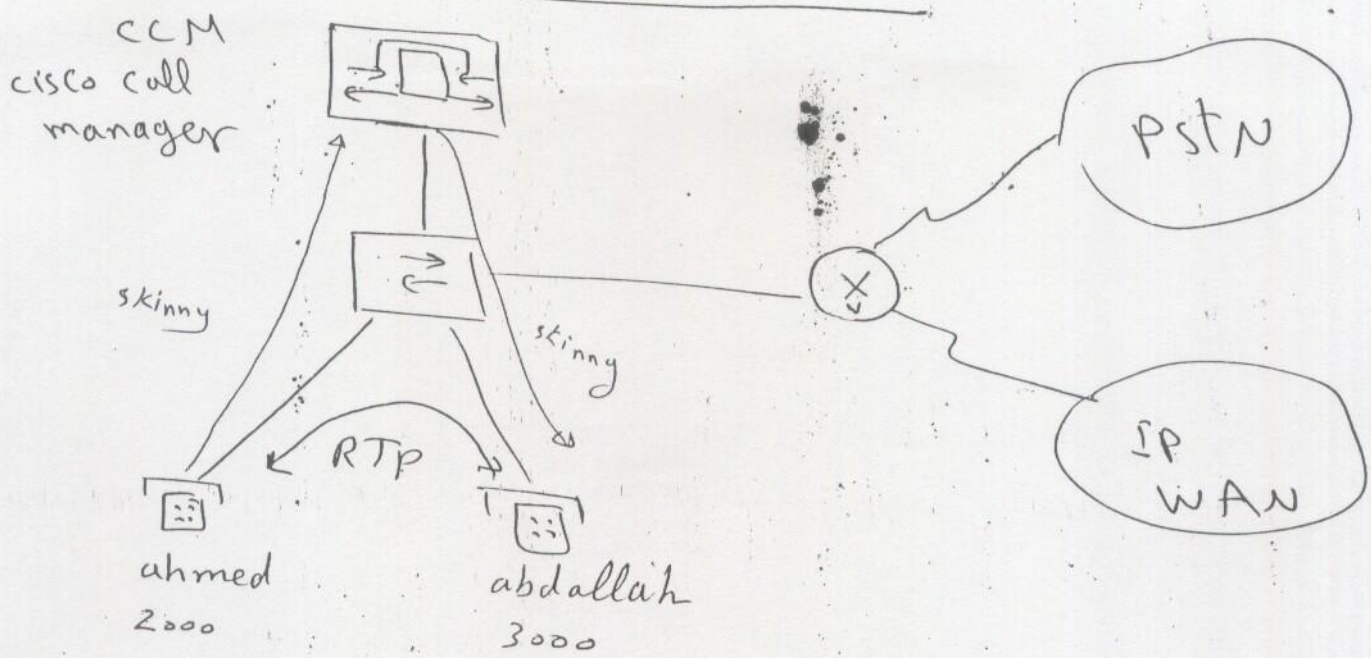
نحتاج إن نقل الصوت بجودة عالية

2 Phase 2 IP telephony



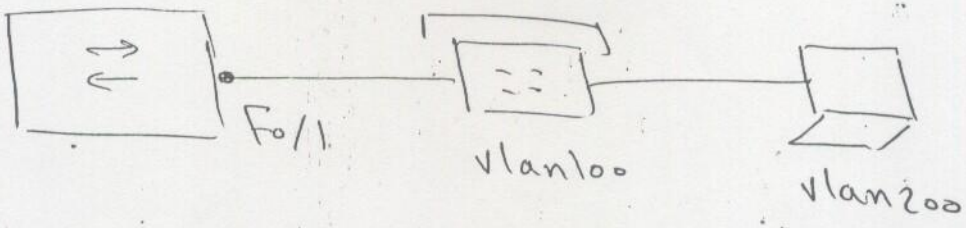
- voice & data network have become one
- PBX & digital phones for sale on EBAY
- true integration between voice & data
- typically new structures start here

How cisco voice works



- when ahmed wants to speak abdallah he will pick up his phone and call "3000"
- when he pick up the phone there was a skinny msg goes from ahmed's phone to call manager (CCM)
- The skinny msg say's that "ahmed pick up the hand of his phone" and dial the number "3000"
- The call manager (CCM) send ~~ast~~ a skinny msg to abdallah "3000" and say to him "Ring))))" there was a call to you come from "2000"
- when abdallah pick up the hand of his phone the call manager open a call between 2000 & 3000 by using RTP [real transmission protocol]

Dual VLAN



يوجد طريقتان لنقل ال data & voice على نفس البورت

1 int F0/1

if) # switch port mode trunk

if) # switch port trunk native vlan 200

وكل هذه الطريقة ليست آمنة لأن في هذه الحالة

البورت F0/1 ← trunk أي هكر يجي عليه hack

ويرسل لل (DTP packets) فيقوم البورت بإرسال البيانات الصوتية إلى ذلك

الأخير معتقداً أنه سويتش

2 int F0/1

if) # switch port mode access

if) # switch port access vlan 200

if) # switch port voice vlan 100

وأنت تعلم أنه عندما يكون ال port access mode لا يستطيع

أحد أن يرسل لل (DTP packets) ويحوله إلى trunk

لذلك هذه هي أفضل طريقة لنقل data&voice على نفس port

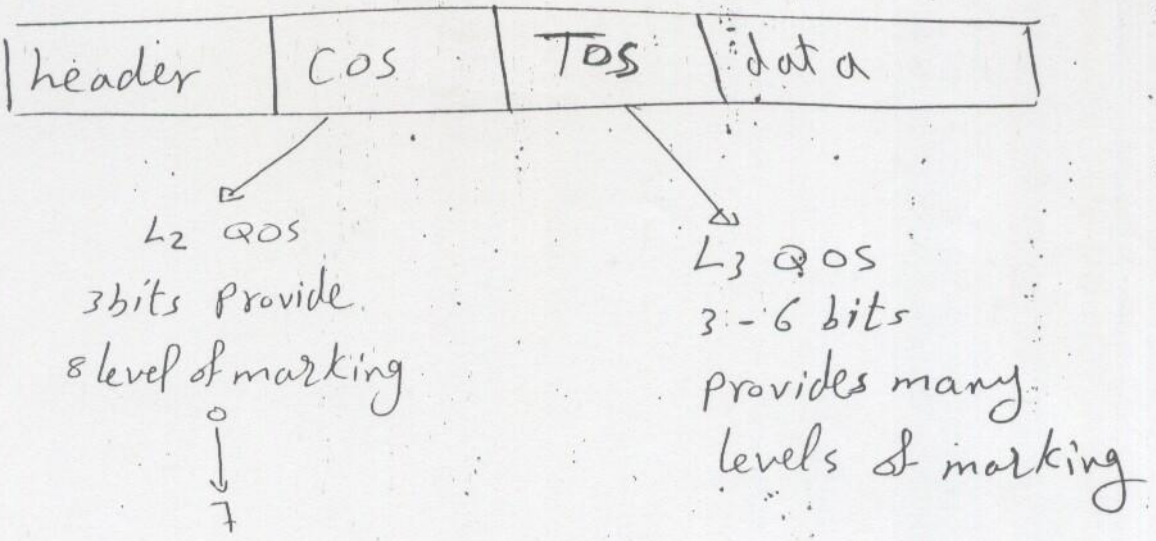
13 QOS quality of service

عندما تأتي ال data إلى ال Router أو switch . أي من هذه البيانات ستمر أولاً أو أي من هذه البيانات لها الأولوية في المرور

هذا ما نعرف باسم quality of service [QOS]

→ we have 2 types of QOS

1. class of service [COS] : layer 2
2. type of service [TOS] : layer 3



ex : you can mark SQL data as a level 4
and voice data as a level 5
∴ voice لها الأولوية في المرور

Configuration

1

int Fo/1

if) # mls QOS trust cos

multi layer switch

means: I will trust The COS on This port

وسوف يكون لـ الأولوية في النقل

---

2 if) # mls. QOS trust device cisco-phone

means: I will trust The quality of service QOS if There was a cisco-phone

---

3 if) # auto QOS voip trust

means: if There was any voice traffic transfer I will trust QOS

وسوف أعطيه الأولوية في النقل

وهذا الأمر أفضل من 1 و 2

Trouble shoot

sh Run

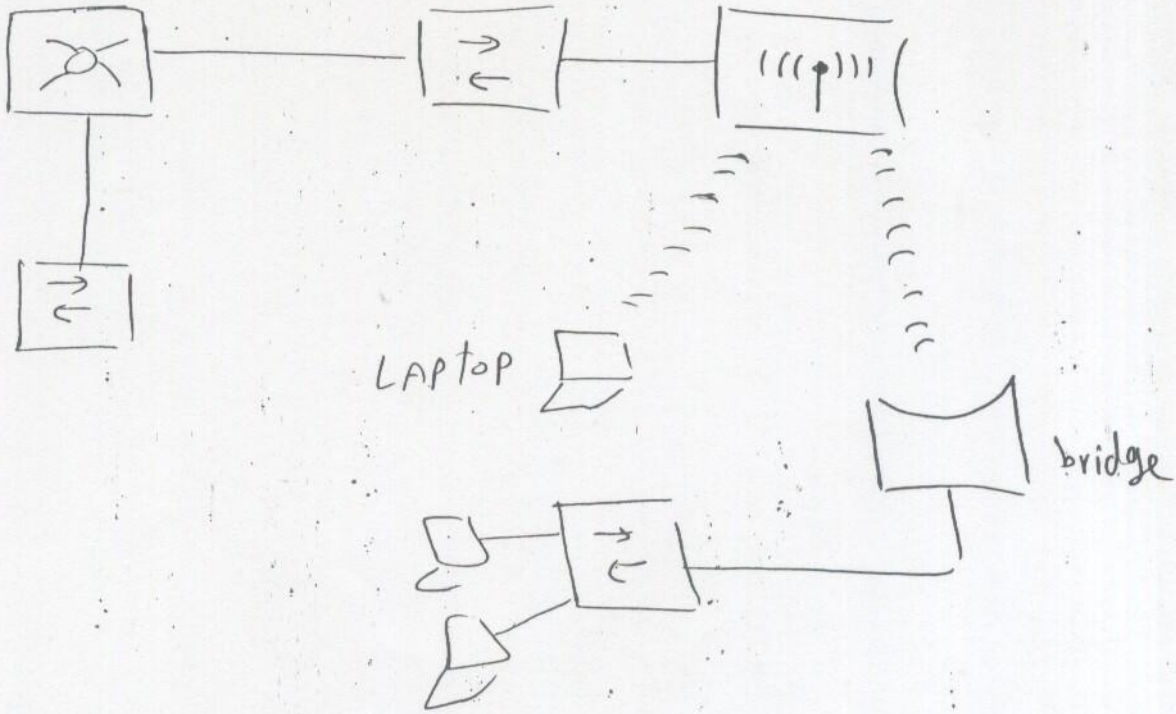
wireless

* wireless LAN Facts

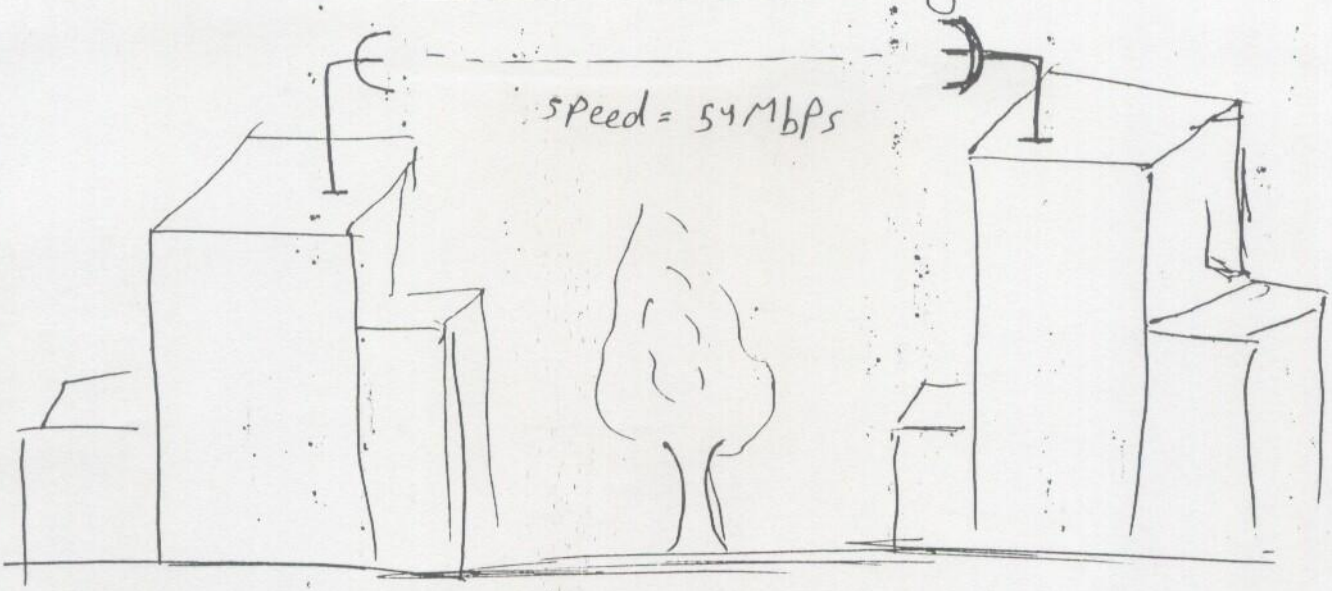
- wireless access point [WAP] communicate like HUB
- uses unlicenced bands of radio frequency
- wireless is a physical & data link standared
- faces connectivity issues because of interference

* where wireless Fits *

① in The same LAN.



② connect between Far buildings



* understand SSID

- The service set identifier (SSID) uniquely identifies & separates wireless networks

→ when a wireless client is enabled

① client issues a Probe

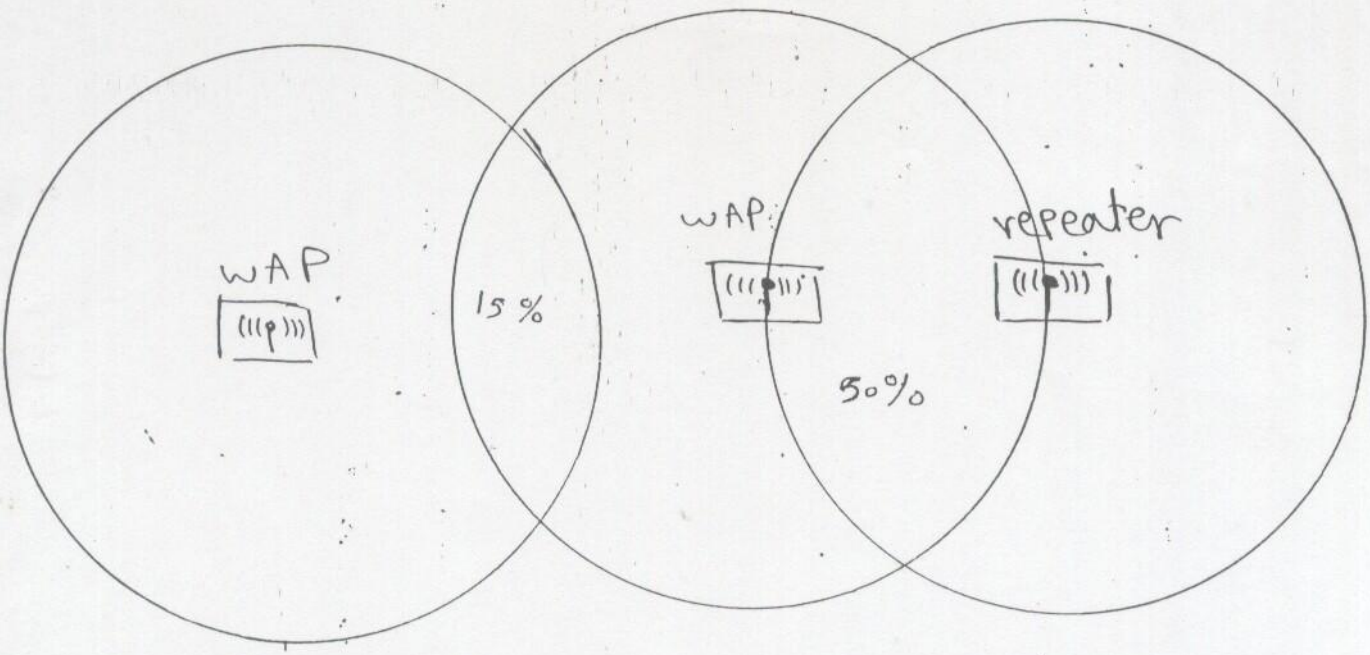
② access point(s) respond with a beacon

③ client associates with chosen SSID

④ access point adds client MAC to association table.

Correct design of wireless LAN

- RF service areas should have 10-15% overlap
- repeaters should have 50% overlap
- Bordering access points should use different channels

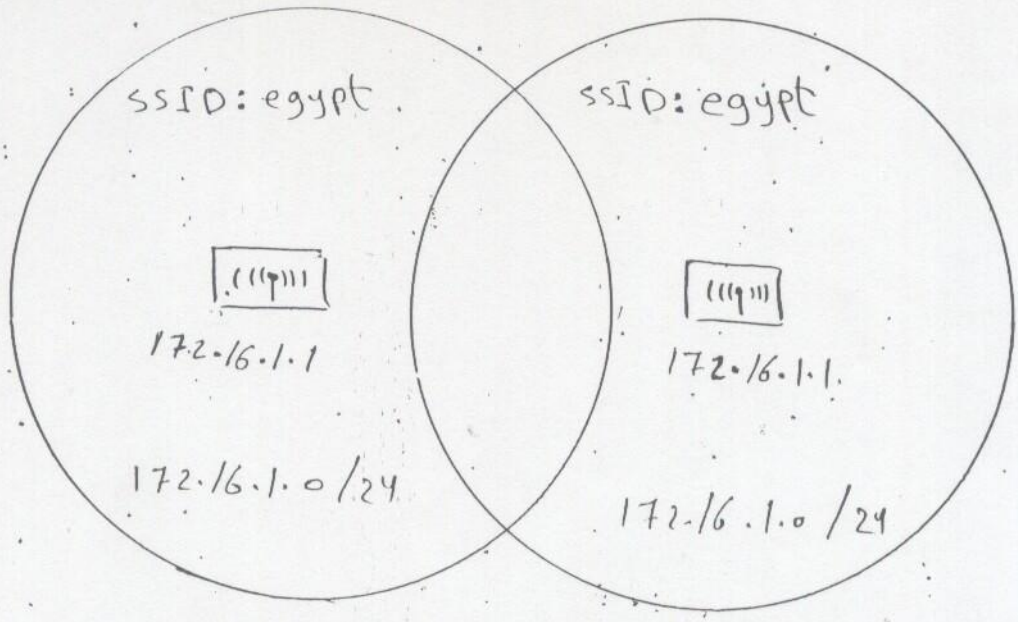


Client Roaming

- as more mobile devices are released, client Roaming becomes a big deal
- true Roaming allows seamless movement between access points

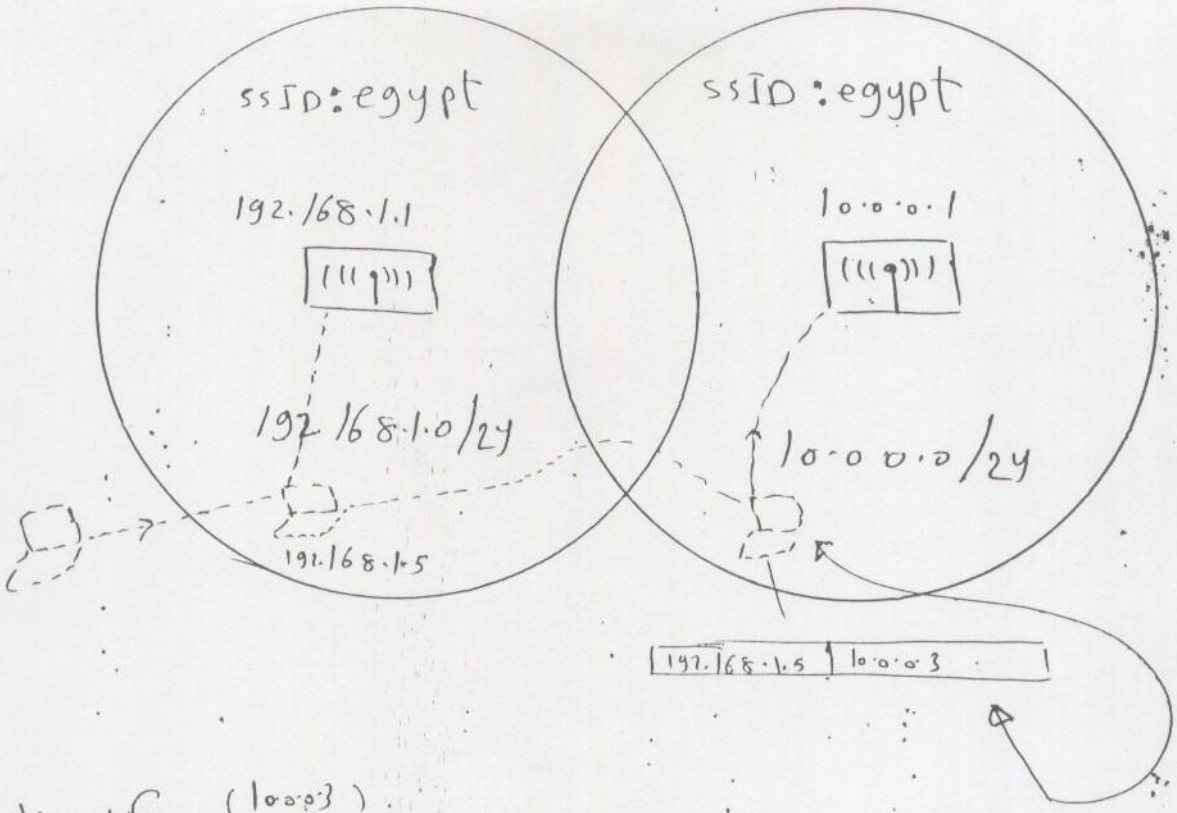
- ~~Pro~~ * we have 2 flavor of Roaming

1 L2 Roaming



→ requirement: same SSID, same VLAN, same subnet

2 L3 Roaming [mobile IP]



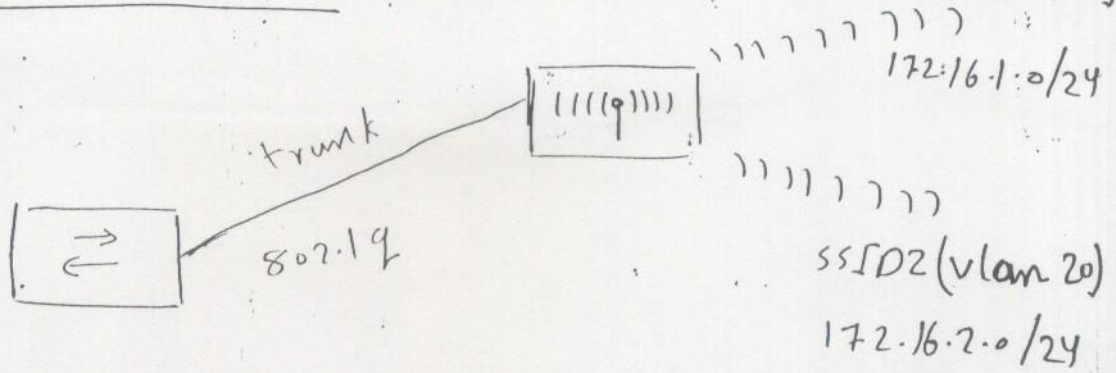
بمجرد دخول Laptop هنا فإنه يحصل على IP جديد (10.0.0.3) ، ولكنه يظل محتفظاً

بال IP القديم لحين العودة إلى الشبكة 192.168.1.0/24

→ Requirement: same SSID

ملحوظة: L2 Roaming أسهل استخداماً وأكثر انتشاراً

wireless VLAN support



→ multiple VLANs provide support for:

- multiple security levels
- multiple subnets
- multiple access-list

unlicensed frequencies

- 900 MHZ range: 902 - 928
- 2.4 GHZ range: 2.400 - 2.483
- 5 GHZ range: 5.150 - 5.350

* understanding RF

- RF waves are absorbed [Passing through walls] or ~~reflect~~ reflected [by metal]
- higher data rates have shorter ranges
- higher frequencies of RF have higher data rates
- higher frequencies of RF have shorter ranges

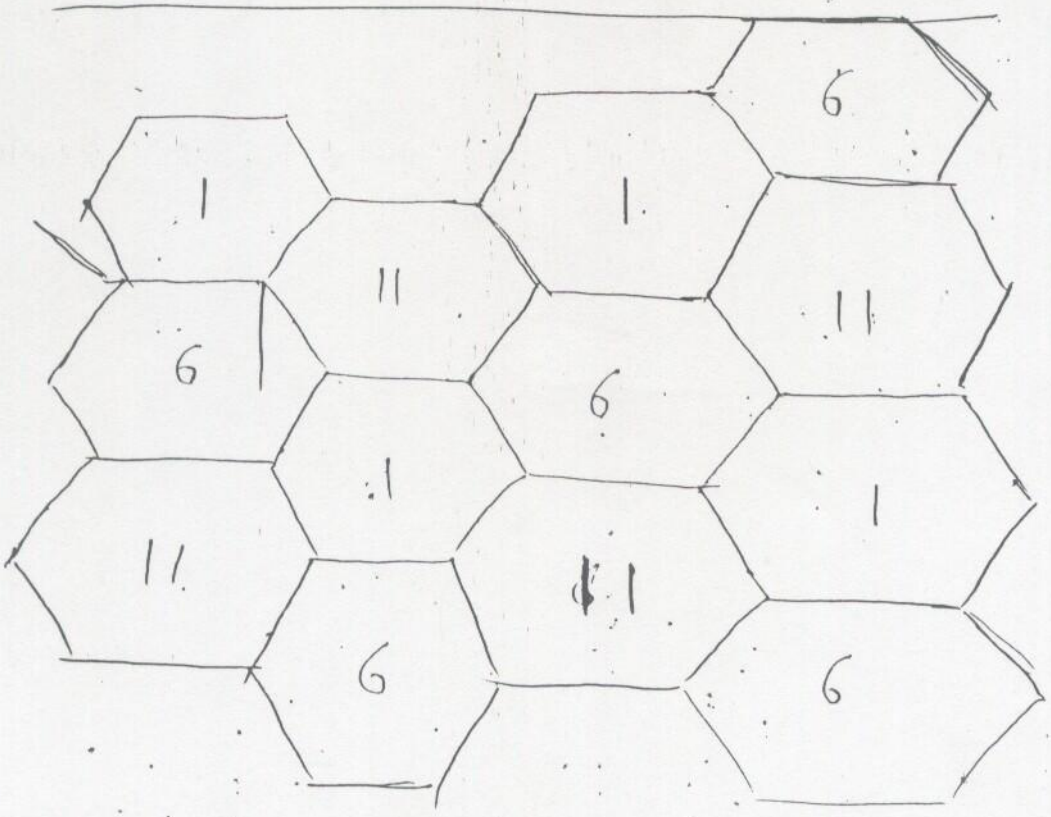
The 802.11 lineup

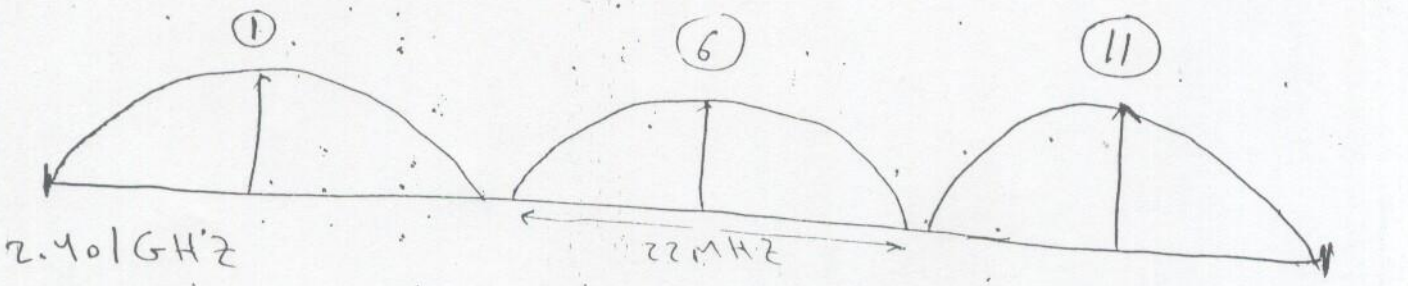
- 802.11b
  - official as of september 1999
  - up to 11 Mbps
  - most popular standard
  - Three clean channels
- 802.11g
  - official as of June 2003.
  - back wards compatible with 802.11b
  - up to 54 Mbps
  - Three clean channels

• 802.11a

- official as of september 1999
- up to 54 Mbps
- not cross compatible with 802.11 b/g
- 12 to 23 clean channels

Designing your wireless coverage





802.11 b/g channels

يتم البث على ٣ قنوات مختلفة حتى لا يحدث تداخل

wireless range

- The further you go, the lower your speed

example: 802.11 G does 54 Mbps
↳ if you are 40 ft from the AP

example: 802.11 a does 54 Mbps
↳ if you are 20 ft from the AP

example: 802.11 b does 11 Mbps
↳ if you are 110 ft from the AP

wireless LAN security

- wireless has added a whole new Paradigm to security
- The wireless security evolution:

1997 → wired equivalent Privacy [WEP]
↖ very weak

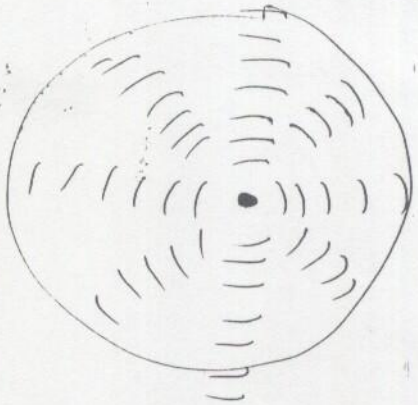
2001 → 802.1X [EAP]

2003 → wi-fi Protected access [WPA1]
↳ use TKIP key

2004 → IEEE 802.11 I [WPA2]
↳ use AES key
أقوى من TKIP

* Antenna types *

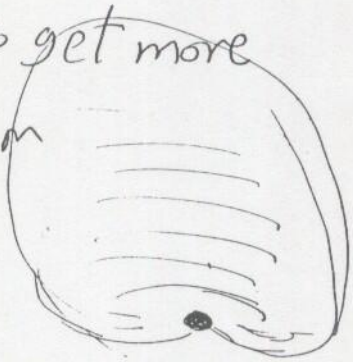
① omni-directional antenna:



- Provides even spread of wireless signal in a radius around The Access Point

② Directional antenna:

- allows you to point antennas to get more radius & range in a specific direction



③ YAGi antenna:

- Provides Dual adjustments of direction & Focus The more streamlined Focus gets intense reach/range

⇓

to see These 3 antennas you can play cisco explorer game