2018

Switching papers

Written by:
Eng.
Amgad M. Mesallam
Edited by:
Eng. Abeer Hosni

"Switching"

Chapter 1:-

"Layer 2 devices"

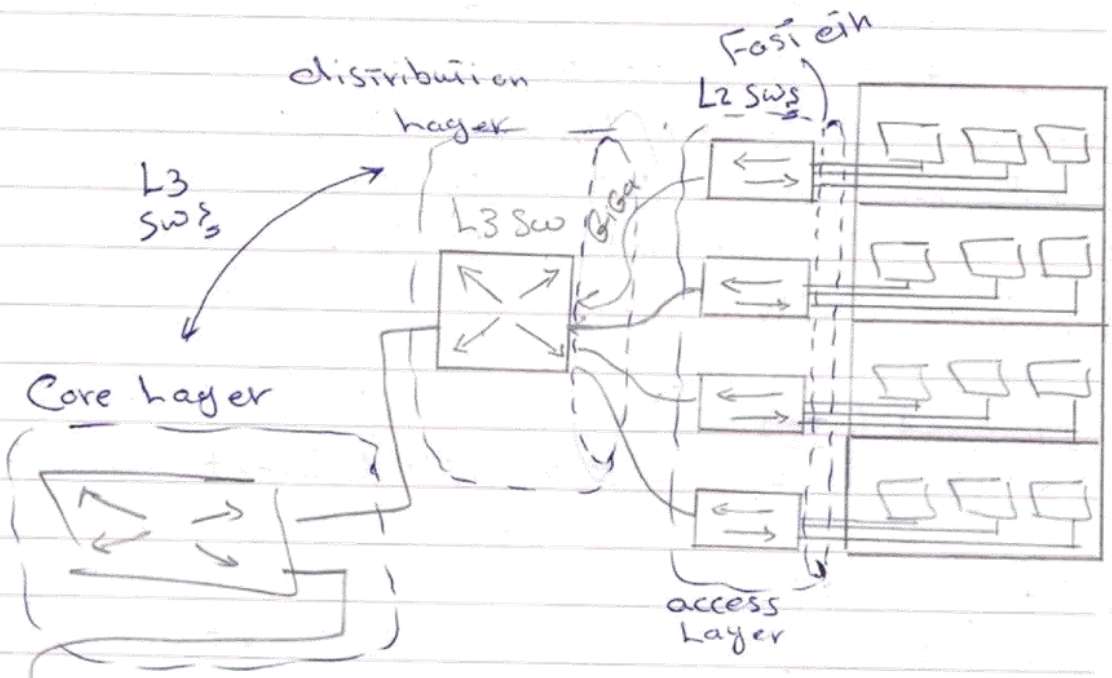
A layer 2 device is a device that understand MAC, for ex:-

* NIC (Network Int. Card)
* Bridge
* Switch: Multi-port ~~bridge~~ bridge up to 256 port

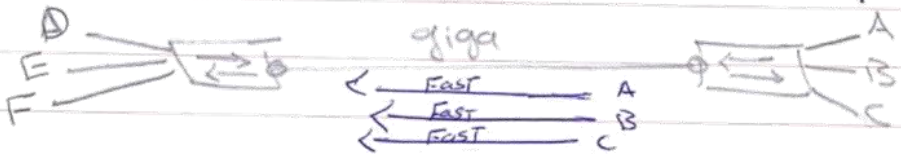
على شان اربط شبكة في نفس الـ Network => switch
باستخدم الـ switch
لو الـ Network مختلف باستخدم الـ Router

- الفرق بين الـ bridge والسويتش أن الـ bridge بتعامل مع الداتا كـ software وبالتالي هو جهاز بطيء وكمان بيقسم الشبكة لـ broadcast domains. بينما السويتش بيستخدم الـ ASIC لنقل الداتا وبالتالي بتعامل معها كـ hardware وبالتالي بيوصل الداتا بسرعة الـ int (أي جهاز سريع) وهو كذلك بيقسم الشبكة لـ broadcast domains.

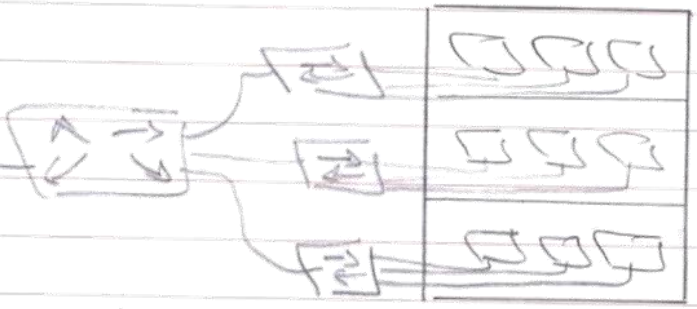
I Hierarchical Network Design



Recommended => Connect 2 switches by giga eth. or 10giga eth



 => 24 Port Fast eth.
2 Port GiGa eth.



وكمان الـ Hierarchical Network design ؟ بشرح كيفية ربط الشبكة بالـ internet . لذلك عادة بعمل model آخر مع cisco enterprise architecture، وهو بيكون من :-

cisco enterprise architecture :-

1. enterprise campus (access + distribution + Core + serverfarm)
2. enterprise edge (the internet connectivity)
3. service provider edge (ISP)
4. Remote (like VPN users).

---

* IN-Band (IB)
  معناها عمل Connect على الراوتر باستخدام tool مثل الـ telnet أو الـ SSH أو الـ HTTP .

* out-of-Band (OOB)
  معناها عمل Connect على الراوتر باستخدام الـ Console أو الـ AUX واستخدام terminal emulator لعمل الـ Connect عليه .

---

* link aggregation :-
تجميع العديد من الـ links في bundle واحدة لزيادة الـ BW.

Cisco ⇐ Recommend ⇐ لو هاعمل Configuration لعدد
لإمكان أكون في الـ Access Layer لو إحنا نقدر نخش
من الـ Distribution لأن أبعد عن الـ Core

* Scalability :- Hierarchical Network
Can be expanded easily

* Redundancy :- at the Core and distribution level ensure path availability.
أكثر من طريق علشان أوصل من الـ source لـ destination
* Network Diameter :-
عدد الـ devices اللي بتعدي عليها الـ Data علشان توصل من الـ source لـ destination.

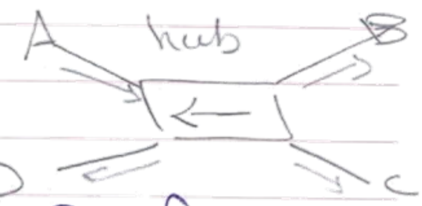
* What is the Converged network

شبكة تحتوي على كل أنواع الـ traffic مثل الداتا والـ VoIP
والـ video وغيرها.

Chapter 2:- (Switching)

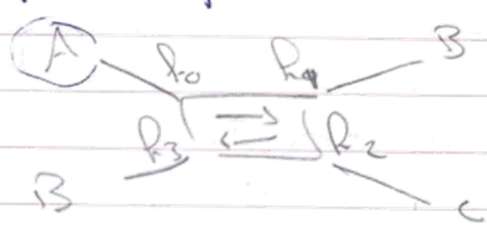
الفرق بين ال hub وال Switch.

(CSMA/CD)



يبعت flood لكل اللي على الشبكة ماعدا اللي جاي منه
ال Data (يقوم بعمل flood على كل الـ ints ماعدا الـ
int الذي استلم منه الداتا).

اول frame بيعمله flood
فقط وبعد كده يبني ال
Mac-address-Table
موجود في RAM



Mac-add-table

int	MAC
f0	A
f2	C

بناخد ال Source،
لان ال Source الموجود.

← aging-time

اي قيمة جوا ال Table تفضل لفترة اسمها aging-time
لفترة By default ⇐ 300 sec.

Communication modes:-

- Single => (Radio)
- half duplex ←☁→ بيقدروا يشتغلوا على نفس
السلكة، ولو حصل Collision بيحلها بـ CSMA/CD

- full duplex ⇄
بايتين كل سلكة واشتغل على سلكة
وبالتالي لا نحتاج الـ CSMA/CD.

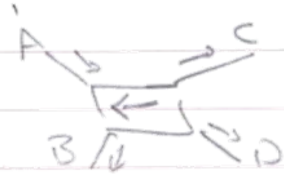
by default auto negotiation <= switch

* لو خليت sw1 full و sw2 auto فيشغل CSMA/CD
half على sw1 =

* Broad Cast domain

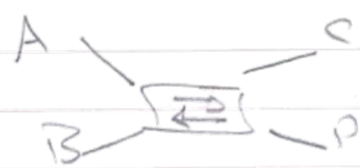
نطاق اللي هيسمع منه الـ Broadcast

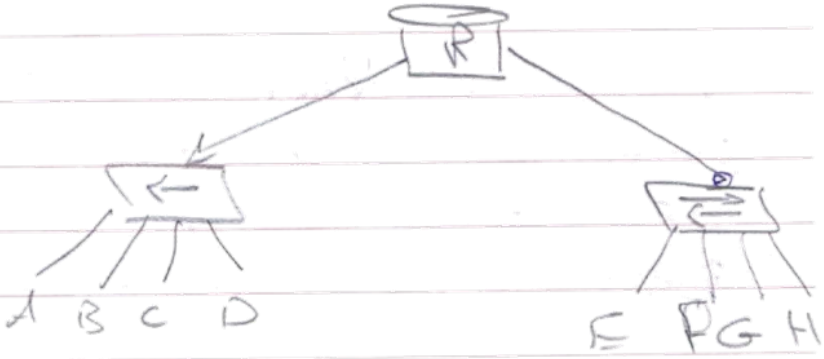
for hub => 1
for sw => 1



* Collision domain

for hub => 1
for sw => No of ints



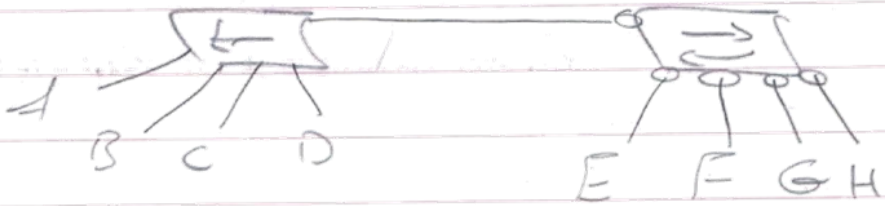


Broad Cast domain (2)

Collision domain

for hub => 1

for sw => 5 ⟹ (6)



Broad Cast domain = (1)

Collission domain = (5)

* Switching Modes:-

*Store and forward
معناها ان الـ Data اول ما بتيجي الـ Switch بتيجي الـ frame
وبعدها بتجمعها لحد ما تكمل جميع الـ frame كاملة
وهي 1500byte وبعدها بتبعتلها الـ Destination.

* مشكلتها انها بطيئة

* Cut-Through
الـ frame (bit) بتحويل بابعتها الـ Destination
على طول

مشكلتها فالـ frame هي الـ checksequence= FCS
موجودة في أول 64byte من الـ frame.
clock sequence: علشان نكون متأكدين انه مفيش

- Fragment offset
الـ Switch بتجمع اول 64b وبعدها بتعمل
علشان تتأكد عنده امكانية لـ FCS وبعد عن طريق
Error Detect

* في الـ Fragment offset فانه السويتش بيتعامل مع أول 64byte
بطريقة الـ store and forward وذلك حتى يكون عنده القدرة على عمل
detect للـ error بطريقة الـ FCS ، وبعد ذلك باقي الـ frame
يتعامل معها بطريقة الـ cut-through .

Switch boot sequance :-

* The boot sequance of Cisco Switch :-

- the switch loads the boot Loader software from NVRAM
- the boot loader :-
  - Performs Low-level CPU initialization
  - performs POST
  - intialize the flash file system
  - loads the o.s image into the RAM

* ملف Switch في flash

① The ios of the switch

② the VLAN data base

③ the Configuration file.

* The Switch uses the NVRAM to store two types of file

① Start-up Config
② The boot Loader.

Lab8- Password recovery
"Switch"

مش بيشتغل على GNS ولا ال packet Tracer

الخطوات : ١) باعمل "Reset" هاشيل كابل ال Power
. واركبه تاني وفي أول 15sec هاضغط على زرار Mode
وهلاقي ⇐

switch: Flash_init ↵
switch : Load_helper ↵ ⇐ بيعمل
initialization لل flash

وال password بيبقى موجودة في ال flash في ملف اسمه Config.Text

ال switch أول ما بيقوم لازم يلاقي الملف Config.Text

switch: Rename ▫ Flash:Config.Text ▫ Flash:
Config.old ↵ أي اسم
: boot

هيبعمل boot مش هيلاقي ال Config.Text
وبالتالي هاقدر ادخل على ال switch وبعد كده هارجع اسم ال Config.old ⇐ لاسمه الأصلي ⇐ Config.Text وبعد كده اقدر اغير ال Password

sw # rename flash: Config.old flash: Config.text
sw # dir flash:
sw # Copy flash: Config.text system: running-Config

Switch> ena ↵
Switch# Config t ↵
sw(Config)# hostname sw
sw(Config)# line Console 0 ↵
(Config-line)# password ——
(Config-line)# login
(Config-line)# do wr
(Config-line)# Exit ↵

sw #show interface status ↵ بيجيبلي حالة ال انترفيس كلها

هلاقي ال Duplex وال speed ⇐ auto

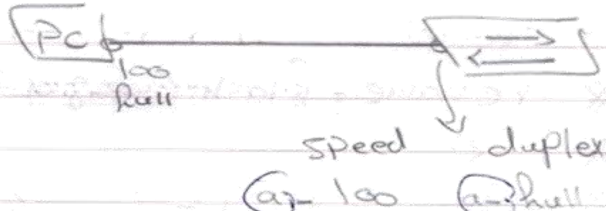
وهلاقي ال Type ⇐ 10/100 يعني بيدعم السرعتين

وال انترفيس لو كان GiGa هلاقيه 10/100/1000 يعني

هيدعم ال ٣ سرعات دا بالنسبة من التوصيل من ال sw.

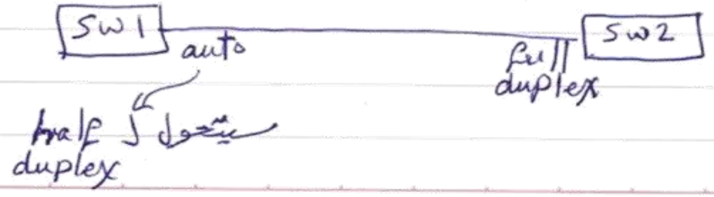
```
Cisco(Config-if)#speed = 100↵
Cisco(Config-if)#duplex = full↵
```

غيرت السرعة بتاعة ال انترفيس من Auto لـ 100 وال duplex من auto لـ full



وهنا هياخد وهياخد القيمة دي عن طريق ال auto.negotiation.

Note) لا يفضل عمل ال hard Code لل duplex على أحد السويتشات وتركه auto negotiation على السويتش الآخر.



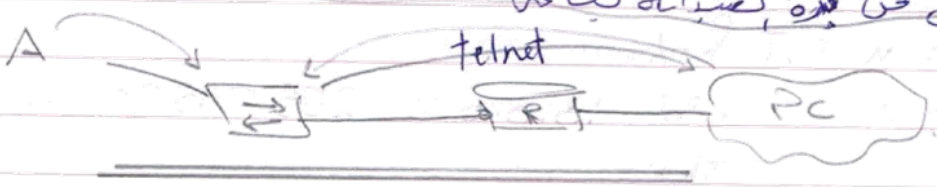
* ليه محتاج اعمل IP على Switch ؟
- علشان اقدر اعمل Connect Remotly
طريقة Telnet او SSH.

Switch(Config)# interface Vlan 1 ↵

sw(Config-if)# IP add 10.10.10.10 255.255.255.0 ↵
sw(Config-if)# No shutdown ↵
sw(Config-if)# exit
sw(Config)# IP default-gateway 10.10.10.1

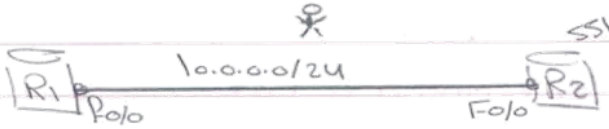
---

* ليه بعمل Gateway على Switch ؟؟
- علشان اقدر اعمل Connect على طريقة Telnet
لان من فكرة الشبكة بتاعتي



Switch# Config t
(Config)# Line Vty 0 4
(Config-line)# Password Cisco
(Config-line)# Login
(Config-line)# end

SSH
Secure Shell (22) Port



Telnet ⇒ Clear text
SSH ⇒ encrypted data
VPN ⇒ Tunneled data

R1

(Config) ✱✱ Int F0/0
R1(Config-if) ✱✱ IP add 10.0.0.1 255.255.255.0 ↵
R1(Config-if) ✱✱ No shutdown

R2

R2(Config) ✱✱ Int f0/0
R2(Config-if) ✱✱ IP add 10.0.0.2 255.255.255.0 ↵
R2(Config-if) ✱✱ No shutdown
R2(Config) ✱✱ line vty 0 4
R2(Config-line) ✱✱ login local
✱✱ exit
R2(Config) ✱✱ username abeer privilege 15 password 123
R2(Config) ✱✱ IP domain-name Cisco.Com ↵

R2.Cisco.Com
R2.Cisco.Com

Hostname Domain name

FQDN

fully qualified domain name

الـ Router بتشتغل الـ Key بين
Fully qualified domain name من Data
(FQDN) بتكون Key (مثال) R2.Cisco.com بتاعه اللي هو

نوع Algorithm ← نوع علم التشفير

(Config) ✻ Crypto key generate rsa ?

(512) : ـــ

لو استخدمت Key كبير الـ Security بتعلى
بس الـ Router بتاخد Performance بتقل

SSHV1 ⇒ Security أقل

SSHV2 ⇒ ~~768~~ 768 bit حجم الـ Key اللازم لا يقل عن
وبتختار حجم الـ Key مثلاً 1024 .

r2✻ show crypto key mypubkey rsa↵

↵ لو عايز استرجع الـ Key اللي اتمسحت بـ Data

r1✻ ssh -l Abeer 10.0.0.2↵

To Connect to R2 ↵

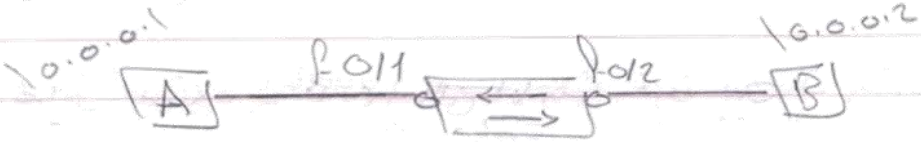
r2 # show ip int br ↵

r2 # Config t
line vty 0 15 ↵
Transport input SSH ↵

↳ معناها ان كل شي يعمل على الـ Router
SSH الا عن طريق الـ Remotly

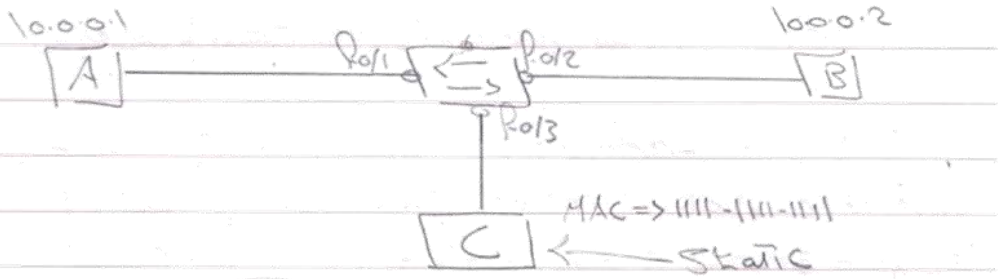
r2(Config) # IP SSH version 2

MAC address table



Switch> ena ↵
show mac-address-table ↵
OR # show mac address-table ↵

A => Ping 10.0.0.2 ↵
نعمل generate الـ traffic حتى يتم بناء الـ MAC add table
SW # Show mac-address-table ↵



(Config)## Mac-address-table ▫ Static ?

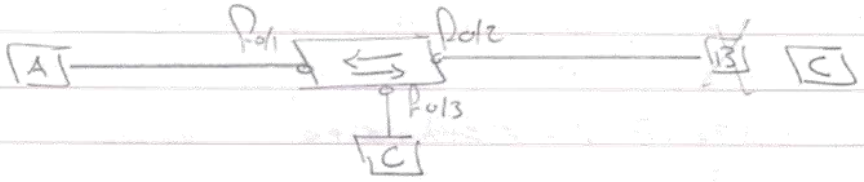
Mac-address-table ▫ Static ▫ 1111.1111.1111 Vlan 1 ↵
▫ Fa0/3 ↵

↵ لو عاوز اضيف Mac بطريقة Static

Show mac-address-table ↵

Table ↵ 300sec ميعتش اى حاجة فى خلال Source لو ↵ بيمسح.

(aging time is 300 sec by default)



لو وصلت كمبيوتر C فان B كدة ↵ 300 عنده معلومة غلط وفى هذه الحالة قدامى حل من اتنين

① استنى عشرة ↵ 300 sec لحد ما ↵ Table يمسح

② امسح ↵ Table بايدى.

Clear ▫ mac-address-table ▫ ?

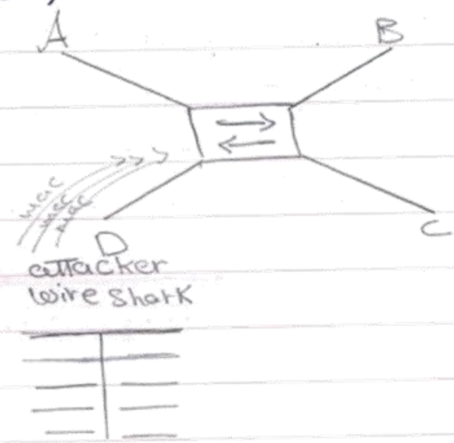
* ازاى اغير القيمة ال default بتاعة ال 300 sec ؟؟

sw(config)# Mac-address-table aging-time 300 ↵
لو كتبنا 0 بدل 300 معناها انى باعمل Disable
لل Aging Time وهيفضل القيمة موجودة دايما فى ال Table

sw# show Mac-address-table aging-time ↵

LAN Security attack

1 MAC address flooding:-
(MAC add table overflow)



قبل ما يعمل setup لل wireshark
هيعمل حاجة اسمها Mack add flooding
وهيفضل يبعت Mac كتيييير لحد
ما ال Table يتملى وتخلص ال Ram
ساعتها ال sw هيهنج وبعد ما يهنج
ال sw هيشتغل كأنه hub
وفى هذه الحالة هيعمل setup لل wireshark
وهيبقى Man in the middle

* وعلشان احمى نفسى :-

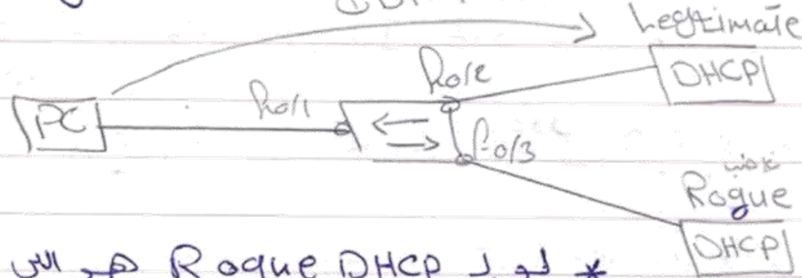
Mitigation :- Port Security.

اخر صفحة فى ال sec 1

* ويتم عمل ذلك النوع من ال attacks عن طريق العديد من ال tools مثل macof. وهى tool موجودة فى ال back tracks.

② Spoofing attack:-

④ DHCP ACK
③ DHCP Requist
② DHCP offer
① DHCP Discover



* لو ال Rogue DHCP هو اللى وزع ال IP عشان يكون الشبكة بتاعته مش فى نفس ال Range بالتالى الشبكة وقعت.

* لو وزع IP فى نفس ال Range بس قال للاجهزة ان ال Gatway هو نفس ال IP بتاعه ساعتها اى حد هيحاول يبعت Data هتروحله هو وبالتالى بقى Man in the middle.

الحل :-

sw(Config)#IP dHCP snooping

← هيوقف اى حد انه ياخد IP من ال DHCP فى الشبكة.

sw(Config)#int f0/2 ↵

sw(Config-if)IP dhcp snooping Trust ↵

وبالتالى ال DHCP المربوط على f0/2 فقط هو الذى يستطيع ارسال ال IPs.

→ شغال على كل ال VLans

* لو عايز اشغله على Vlan معينة

sw(Config)#IP dHCP snooping Vlan 1

* لو عندي ال pc هو ال Attacker و بيعت Mac كتيرة و عايز فضادها IP لحد مايخلص ال Pool بتاعة ال DHCP (:

هاجي عند ال Int بتاعه وهاحدد ال x عدد ال IP الي هاخدها

sw(Config)# Int fa0/1
sw(Config-if)# IP dHCP snooping limit rate 2

③ CDP => Cisco Discovery Protocol

لو فيه 웃 ولقط ال CDP هيقدر يعرف معلومات كتيرة

عشان اعمله Disable على مستوى ال Router

او على مستوى ال Int

(Config)# No CDP run ← Router
(Config-if)# No CDP enable ← Int

④ Telnet attack

بلاش ال Telnet ونشتغل SSH (:

Port Security

أنا عندي مشكلة إن جهاز A مثلاً من ممكن يبعت Mac كتير ويوقع الشبكة.

ال Port Security يعني تحت ال Int بتاعه وساعتها لو جهاز A بعت Data من ال Mac بتاعه هاقبلها ولو جاله Date ب Mac مختلف مش هيقبل.

أي مستخدم ال MAC لجهاز ال A لأنه بيكون شرط لإرسال الداتا.

* لو جيتلي Data و Mac مختلف

Violations:-

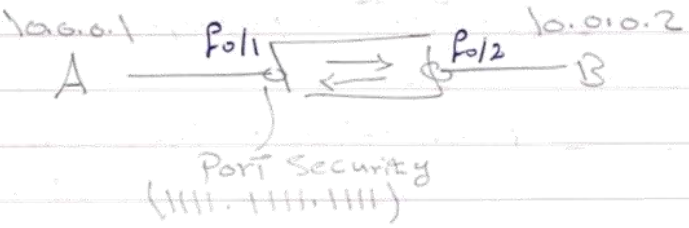
- Protect يعني مش هيعمل Data وخلاص.

- Restrict
① مش هيعمل Data إسقاط
② هيزود الـ Counter بـ 1
③ هيظهر Syslog على الـ SW ويقول Mac إللي بيعمل Attack

- Shut down (default)
① مش هيعمل Data
② هيزود الـ Counter بـ 1
③ هيظهر Syslog على الـ SW
④ هيوقع الـ Port وهيحطه في حالة اسمها err-disabled. وعلشان اشغله لازم ادخل على الـ Port وعمل shut down وبعدها No shut down.

أو يكسر عمل Timer لحالة الـ err disabled التي وقع في الـ int.

« Port security »
lab



lab => packet Tracer => sw => 2960-24TT

PC 1 => 10.0.0.1
sub => 255.255.255.0
PC2 => —— 10.0.0.2/24
sw => int Fo/1 ↵
sw (Config-if)# switchport port-security ↵
error
sw (Config-if)# switchport mode access ↵
Enable لازم نكتب => switchport port-security ↵
portsecurity لـ (to enable port security)
sw (Config-if) # switch port port-security ▫ mac-add ?
H.H.H
sticky

H.H.H => # switch port ▫ port-security ▫ mac-add
1111.1111.1111 ↵ portsecurity لـ Enable لازم نكتب الأول
mac => 111.111.111 وبعدين اي Data الـ جاية

Sticky ✱ switchport port-security mac-address ↵
sticky ↵

هيبقى اول frame هيتبعت من ال PC وهياخد منه ال Mac
وهيطبق عليه ال port security

sw(config-if)✱ switchport port-security maximum ↵

يعني ال Switch بيقبل mac واحد by default
وممكن اعدلها من (1-132) bit

(config-if) ✱ switchport port-security violation protect ↵

PC1 => ping 10.0.0.2
Request time out
" " "

sw # show port-security int fo/1 ↵

معلومات عن ال port-sec. اللي شغالة على ال int

PC1 => IP config /all ↵

علشان اعرف ال Mac add.

✱ no switchport port-security violation protect ↵
✱ switchport port-security violation restrict ↵
✱ do show port-security int fo/1 ↵

* No switchport port-security violation restrict ↵

* switchport port-security violation shutdown ↵
هلاقي إن الشبكة وقعت

** show int f0/1 ↵
"err-disabled"

1) اول خطوة باشيل الـ PC الغلط واركب الـ صح
2) باعمل shutdown للـ Int وبعدها no shutdown

الـ led بتاع الـ switch

- اخضر — لو لونه اخضر
  - اخضر ثابت => شغال لكن مفيش Data بتعدي
  - اخضر flash => شغال وفي Data بتعدي
- "amber"
  - يعني الـ Int بايظ أو أسباب أخرى

---

sw(Config)# errdisable recovery cause security-violation
sw(Config)# errdisable recovery interval 300 sec

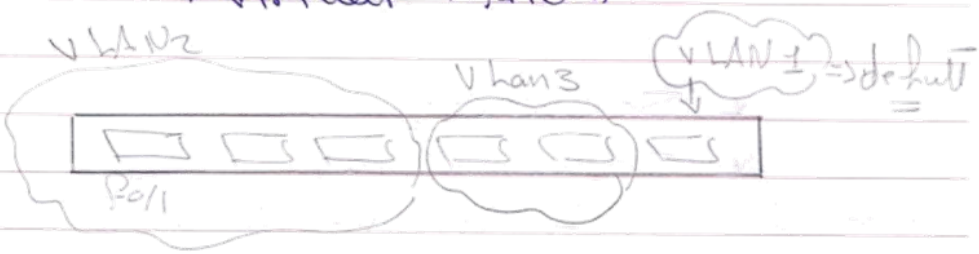
or

sw(Config-if)# switchport port-security aging time 300 min
sw(Config-if)# switchport port-security aging type (absolute | inactivity)

sw# show errdisabled recovery

« V Lan »

« Virtual LAN »



داخل مجموعة من الأجهزة عندى فى VLAN معينة، وكل مجموعة من الأجهزة تتبع VLAN معينة ← تطبع الوصول لبعض.

لو جيت على Vlan3 وعملتها Delete هتلاقى لـ آسف بقت « amber » homeless وكل الأجهزة هتش هيتشتر على Connectivity

ولو عايز ارجع لـ Connectivity قدامى طريقة من اتنين :-

① ارجع لـ VLan3 تانى وهترجع بال آسف اللى كان عليها

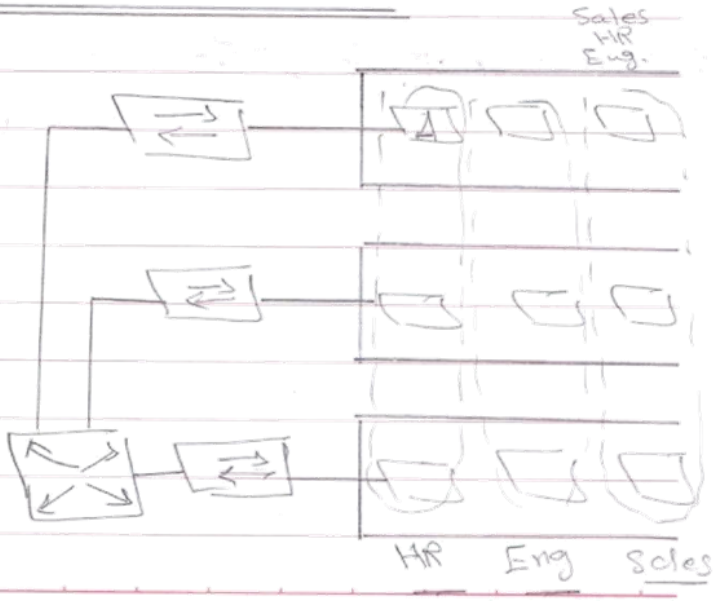
② اضغط لـ آسف اللى كانت فى VLAN3 فى VLAN 1 تانية.

---

① اما افصل كل دور لوحدة بشبكة لوحده (غير عملى).

② او اضغط كليك يمين فى (Wei. II) Non Security دى تختلف دى

③ اضغط كليك يمين فى VLAN ودى Recommended



بعد ما قسمت الشبكة لـ VLAN + Broadcast
هيوصل فقط للأجهزة من الـ VLAN بتاعته.

* Security
* Segmentation,

يعني قسمت الشبكة بناءً على Vlan شايفة تقسيم فقط على ضمان الـ security

* managability

علشان Vlan تستطيع الوصول لـ Vlan تانية لازم يتم Routing
يعني هيشوفوا بعض كـ Unicast مش Broadcast

(Broadcast is not evil) أنا باقلل فقط الـ Broadcast domain

* Managability:- هاقدر manage الشبكة بتاعتي بأسلوب أسهل.

* الهدف الرئيسي من تقسيم الشبكة لـ VLANs هو تقسيم الشبكة لأكثر من broadcast domain.

« VLAN Characteristics »

* VLAN ID :-

لـ VLAN باعطاها Create لـ رقم و لرقم ده
ممكن يكون صاحبة من اتنين

Normal
- VLAN 1 « default »
- VLAN 2 → 1001
- VLAN 1002 → 1005

Extended
- VLAN 1006 → 4094

* لـ VLAN 2 → 1001 دول اللي انا اقدر admin
اطبقها عادي على لـ Switch

* لـ VLAN 1002 → 1005 اتقدموا خلاص وكان بيستخدم
في لـ FDDI و لـ Token Ring

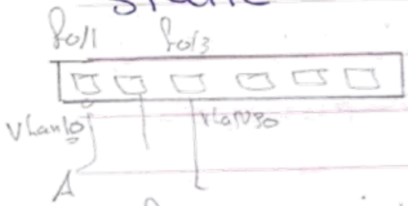
* Extended ⇐ بيستخدم في شركات لـ ISP على transparent sw

كل VLAN ليها رقم و اسم و اي VLAN باعطاها
عن طريق امر create

مثلاً VLAN 2 ⇒ HR
اذا لم أحدد لها إسم { VLAN 3 ⇒ VLAN 0003
VLAN 20 ⇒ VLAN 0020

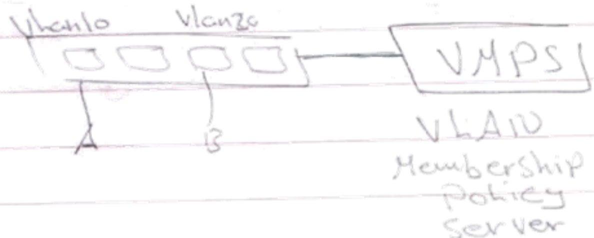
« Types of VLANs »

static



لو غيرت A لـ fa0/3
هروح أدخل على تاني وأغير الـ VLAN

dinamic



MAC	VLAN
A	10
B	20

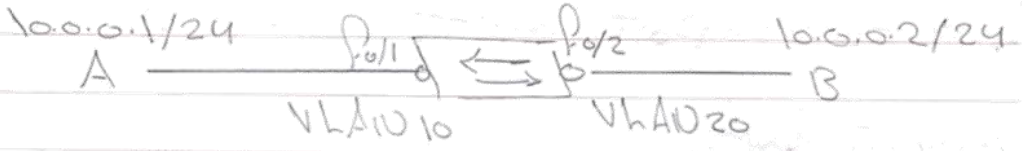
بـ create الـ Table عليه
الـ Database فيها الـ PC والـ VLAN
بتاعته ولو غيرت مكان الـ PC لو هو
هيعمل الـ تاني لـ VLAN بتاعته.

« Voice VLAN »

IP Telephony

أبسط إني أسيب الـ Telephone والـ PC في نفس الـ VLAN
علشان ما برنامج بيشغلها setup على الـ PC مش بيضغط على الـ Tele
وتسمع أي مكالمات.

"VLAN Config"



Packet Tracer:

Switch> ena↵
switch ✻ show VLAN ↵ (لكل المعلومات عن الـ VLAN)
✻ show VLAN brief ↵ (معلومات مختصرة)

على شان اعمل VLAN Configuration فيه طريقين

Vlan database

فيه وهي مش بيستخدم
Not Recomended.

Switch ✻ Vlan database
sw(Vlan) ✻ Vlan 2
sw(Vlan) ✻ Vlan 3 name HR
Vlan 3 added
Name: HR

لازم اقول Exit عشان تضاف في الـ Vlan database او اقول Apply وبعدها هيخرج لـ Vlan وهيبين في نفس الوقت "لو استخدمت Control-Z مش هتضاف"

Config mode

✻ Config t
✻ Vlan 10
✻ exit
✻ Vlan 20
✻ Name SALES

لو عايز Create في VLAN اكتر من واحد في سطر واحد ↓

✻ Vlan 10,20,30-40

واحد واحد ← من 30 لـ 40

(Config)# int fo/1 ↵

(Config-if)# switchport mode access ↵ باعطيله أسامي كل

(Config-if)# switchport access vlan 10 ↵ بـ Vlan

(Config)# int fo/2 ↵

(Config-if)# switchport mode access ↵

(Config-if)# switchport access vlan 20 ↵

لو عايز أضع 100 port في كذا vlan معينة

For ex:- ① fo/3 : fo/6 => Vlan 2

② fo/8, fo/10, g1/1 => Vlan 4

⇓

① switch (Config)# int range fo/3 - 6 ↵

switch(Config-int-range)# switchport access mode

sw (Config-int-range)# switch port access vlan 2 ↵

② switch (Config)# int range fo/8 , fo/10 , g1/1 ↵

sw (Config-int-range)# switchport mode access ↵

sw(Config-int-range)# switchport access vlan 4 ↵

Switch (Config)# no VLAN 4 ↵

بعمل Delete لـ Vlan4 دول أسامي

Homeless. أصبحوا

الـ Vlan يجرى ما باعمل Create بتحـط
فى الـ Flash:Vlan.dat

شىء تاني أي فى الـ Vlan موجودة فى
NVRAM: Startup-Config.

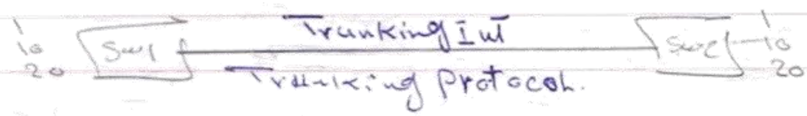
* علشان ادخل الـ Switch على الـ default
اواعمل الـ Reset للـ Switch
لازم ٢ خطوات:-

Enable mode*

1. erase startup-config ↵
2. Delete Flash:Vlan.dat ↵
3. Reload ↵

(Trunking)

Vlan 1



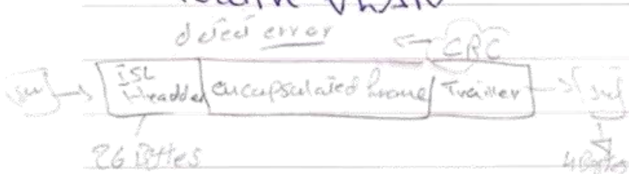
بس ازاي الـ sw يعرف ان الـ Data تبع VLAN معينة
بيحصل عن طريق Trunking Protocol

* Trunking protocol وظيفته إنه بيمسك كل frame من sw لـ sw التاني و يحط عليه الـ Sticker بتاع الـ Vlan اللي المفروض توصله.

* بيوجد نوعين من الـ Trunking protocol

ISL

- Cisco properiary
- encapsulate frame
- Doesn't support Native VLAN



dot1q = 802.1Q

- IEEE Standard.
- tags frame
- support Native VLAN «كل الـ sw شغالة بيه»

(ISL) inter switch link

حجم الـ packet ⇐ By default ⇐ 1500 byte

MTU ⇒ Maximum Transfer unit

الـ sw بيقدر يتعامل مع الـ frame أقصاها 1518 byte

Gaint

وأقلها 64 byte

Runt

drop

لو وصلتي frame أكبر من 1518 بيعملها

ولو أقل من 64 بيعملها Drop.

* الراوتر بتقوم بعمل fragmentation لل packet إذا تعدى حجم الـ MTU بتاعي تكون لو جيا الـ ethernet لا يستطيع

(802.1Q)

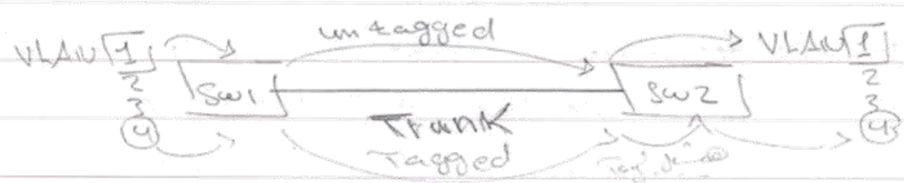
بيزود حاجة اسمها Tag في الـ sw ويبقى منه الـ VLAN ID

ويزود FCS علشان يعمل error detect على الـ Data الجديدة

بعد قبل الـ Tag كان.

Native VLAN :-

By default Native VLAN = Vlan 1

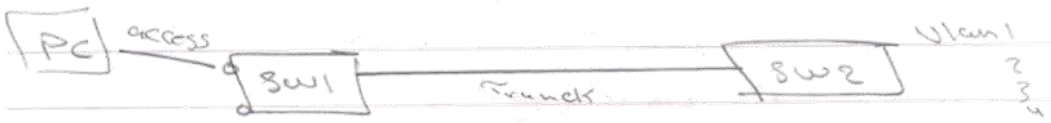


الـ Native Vlan لازم يبقى واحدة على الـ Switches

Cisco ⇐ Recommend ان الـ Voice يختلف عن الـ Native Vlan

علشان الـ Voice أصلاً تتقل

* عن طريق الـ native VLAN يمكن ان تحدث attack على السويتش اسمه double tagging لذلك لا يفضل استخدام الـ native VLAN أصلاً أو عمل tagging لها.



access int: belongs to only one Vlan
Trunk int: belongs to all Vlans.

DTP

((Dynamic Trunking Protocol))

Int ⇒ ① access
② Trunk

default ⇐ Dynamic → auto
↳ desirable

3550 → dynamic desirable 3560, 2960 → dynamic auto

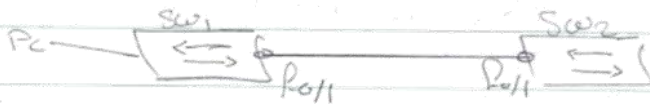
بيعتوا لبعض كل 30sec بيبدأو ايعض هيشتغلوا ازاى
عشان استعداد تشتغل Trunking ولا لا

auto ⇒ negotiation كل 30sec مستنى لتان يبدأ له

desirable ⇒ انا اللى هبدأ ابعت.

لو جيت الاقى Int Trunk Recomanded اللى اوقف ال DTP له

Lab:-



لو عاوز اعرف ال int شغال على Trunk ولا لأ

* Show int Trunk ↵

لو عاوز اعرف ال int شغال Trunk ولا access ولا Dynamic auto ولا Dynamic desirable

* Show int fo/1 trunk ↵

كل المعلومات عن ال int شغال ايه.

* Show int switchport ↵

او * Show int fo/1 switch port ↵

administrative mode: dinamic auto
operational mode: access

Sw1* int fo/1 ↵
(Config-if)* switchport mode ?

H.W

* show int Trunk ↵

على شان اوقف ال DTP Protocol لازم الأول Hard Code
اشغل ال int ⇐ Trunk ولـعزلة اوقفه بالأمر
(Config-if) * Switchport nonegotiate ↵
sw #show dtp ← to know general info about DTP

VLAN Hopping

- Double tagging using native VLAN
- switch spoofing using DTP

إذاي اغير الـ Native VLAN ؟؟

sw1 # int f-0/1 ↵

sw1(config-if)# switchport trunk ?

allowed

native

switchport trunk native vlan 2 ↵

sw2 ⇐ نفس الكلام.

لازم اغير الـ Native Vlan في الاتنين.

---

show int Trunk ↵

الـ Trunk بيشيل كل الـ Vlan لكن بإيدي

أمنع امرر الـ Vlan الي عايزها

(config)# int f0/1

(config-if)# switchport trunk allowed vlan2 ↵

(config-if)# switchport Trunk allowed ?

(word) add all none remove except

- all VLANs are allowed through the trunk int by default
- but we can specify specific VLANs

« Inter VLAN Routing »

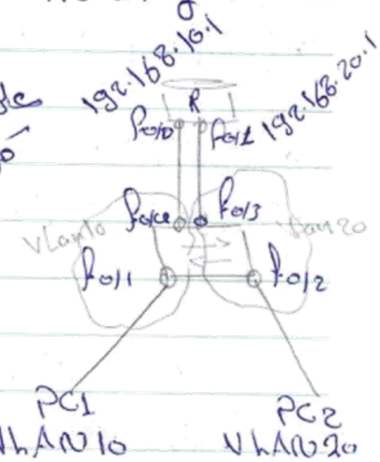
بأعمل Routing بين ال VLAN على شان كل VLAN
تشوف التانية بعض ك unicast مش Broadcast.

* inter VLAN routing is done using a L3 device, router or a L3 switch.

① Router

* Traditional inter-VLAN Routing

على شان اعمل Routing لل VLAN لازم
كل VLAN تكون في Network ID مختلف



مشكلتها في ال VLAN الكتيرة

اذا كان يوجد عدد كبير من ال VLAN سنحتاج
int على الراوتر لكل VLAN.

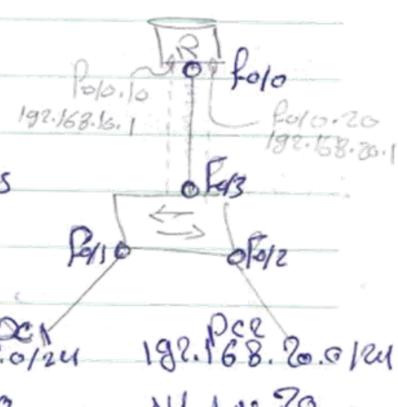
192.168.10.0/24 192.168.20.0/24

* Router-on-a-stick

هادي على ال Router وهاعمل ال Int Fa0/0
واعمله no shut وهادي على ال Router واعمل
subinterfaces ⇐ وهديه واعطيه IP

Fa0/0.10 => 192.168.10.1
Fa0/0.20 => 192.168.20.1

معرفة ان ال آتي بين ال R وال sw
هيبقى Trunk



على شان ال Router-on-stick يشتغل صح لازم يكونوا متوصلين بـ feth او Geth ولكن عيبه انه ممكن يسبب Congestion في الشبكات الكبيرة

```
Labs- sw# int f0/1 ↲
sw(Config-if)# switch mode access ↲
sw(Config-if)# switchport access vlan 10 ↲

sw(Config)# int f0/2
sw(Config-if)# switchport mode access ↲
sw(Config-if)# switchport access vlan 20 ↲

sw(Config)# int f0/3
sw(Config-if)# switchport mode trunk ↲

Router# int f0/0
(Config-if)# no shutdown
Router(Config)# int f0/0.10 ↲
R(Config-subif)# encapsulation dot1 10
R(Config-subif)# IP add 192.168.10.1 255.255.255.0 ↲

R(Config)# int f0/0.20 ↲
R(Config-subif)# encapsulation dot1 20
R(Config-subif)# IP add 192.168.20.1 255.255.255.0 ↲
```

PC ⇒ IP ⇒ subnets ⇒ Gateway

PC1 ⇒ 192.168.10.100/24
gateway → 192.168.10.1

PC2 ⇒ 192.168.20.100/24
gateway → 192.168.20.1

from PC1

Test => Tracert 192.168.20.100

or Ping 192.168.20.100

---

② L3 sw افضل Senario لل Routing هو ال L3 sw

* لما باجي اعط IP على ال sw بإعطيه على Int وهمي

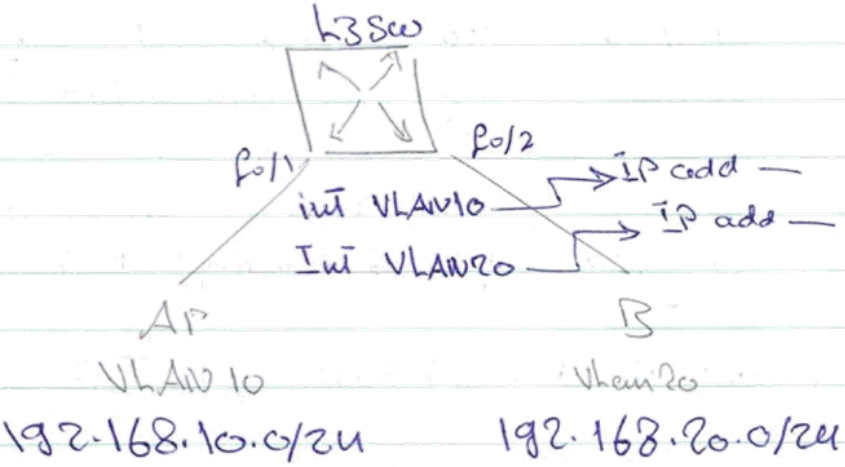
اسمه SVI

Switched Virtual Interface.


```
sw(Config)## int Vlan 1
sw(Config-if)## IP add 10.0.0.1 255.255.255.0
sw(Config-if)## No shut
```

معنى كدة VLAN هي ال mangement بعض الناس
VLAN

بتاعة VLAN1 هي اللي هتقدر Telnet على ال sw



int's configuration ↓ is ip routing ↵

** Sw(Config)** ip routing ↵

⇒ Routing ↓ Enable ↓

lab

```
Sw(Config)# int Vlan 10
Sw(Config-if)# ip add 192.168.10.1 255.255.255.0
Sw(Config)# int Vlan 20
Sw(Config-if)# ip add 192.168.20.1 255.255.255.0
Sw(Config)# Vlan 10,20
Sw(Config)# ip routing
Sw(Config)# int Fo/1
Sw(Config-if)# switchport mode access
Sw(Config-if)# switchport access Vlan 10
Sw(Config)# int Fo/2
Sw(Config-if)# switchport mode access
Sw(Config-if)# switchport access Vlan 20
```

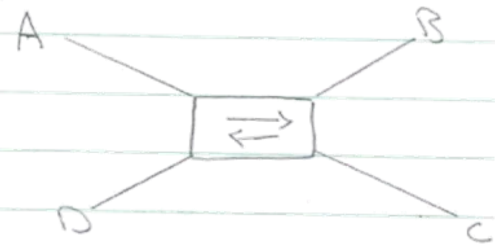
*Routing is enabled on router but disabled on L3 sw by default

« Switching »
Revision

Switch Tops:-

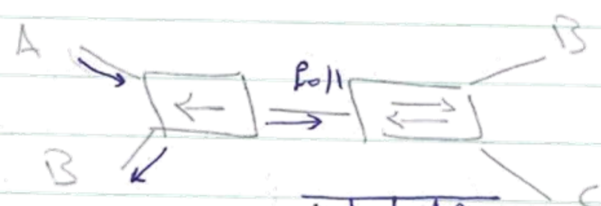
① MAC Address learning:-

اول Frame بيعملها Flood ماعدا
ال int اللي جالي منه ال Data
وبعد كده بـ Build ال Mac.add.table



② Forward decision:-

ال sw لو لقي ال Source
وال Destination ← Connected
على نفس ال int ــــ فلتر
هيعمل Block لل int
لحد ما ال Frame تثبت وتفتح
ال int تاني

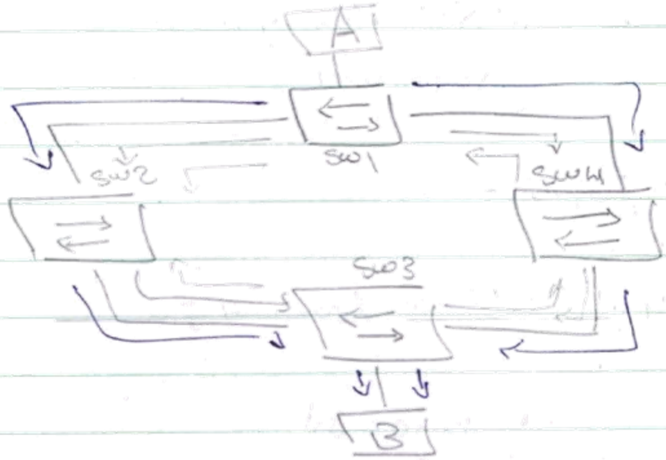


int	MAC
f0/1	A
f0/1	B

③ prevent switching loops Caused by redundancy.

لو حصل switching loop ملهاش حل إلا إني اعمل Reset

لكل ال sw اللي على الشبكة



* في حالة ال (Redundant Topology) هيبقى عندي عرضه إنه يحصل عندي switching loop . لو ال PCA بعت Broadcast ساعتها هيحصل عندي Broadcast Storm

مشاكل ال Reduntant Topology :

① Broud Cast Storm :-

② multiple frame Copies :-

في حالة ال unicast ال frame هيوصل مرتين لل Destination

③ Mac address table instability:-

مابيفضلش جهاز
sw هيوصل على 2 int. من ال
ساعتها ال Mac Add Tabe <= instable

SW3

Int.	Mac
~~Fa0/1~~	~~A~~
Fa0/2	A

لحل ال sw عليه Protocol اسمه ال STP
وهو اللي هيوقف ال Switching Loop.

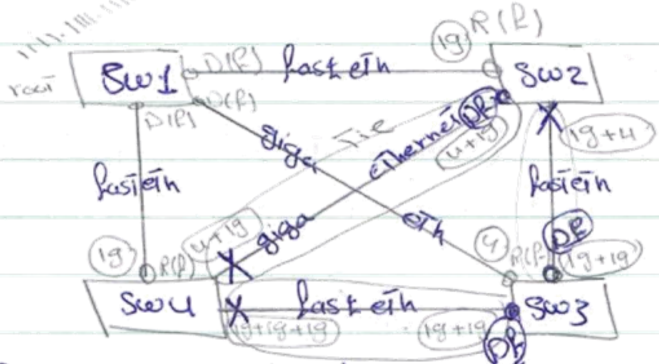
* هيخلي ال frame تمشي في طريق واحد بس ولو الطريق
ده وقع => تلقائي ال sw هو او ال STP هيشغل الطريق التاني

STP

Spanning tree protocol

(* at Startup)

① one root bridge per Network
«bridge => switch»



② one rootport Per non-root bridge.
③ one designated port Per Segment
④ block all other.

---

1. يعني sw واحد بس هو اللي هيبقى root switch
كل sw يعني عليه قيمة اسمها BPDU
BPDU «bridge protocol data unit»

2 byte	6 byte
Priority	Mac add.

By default=32768

اول ما الـ sw هتقوم مع بعضها هـ كل sw هيقول انا الـ ROOT ساعتها هيحصل tie اللي هيحصل الـ Tie الـ Priority عن طريق اقل قيمة بين المشتركة انه الـ sw كلها قيمة By default = 32768 ساعتها اللي هيحلها هو الـ Mac add والـ ROOT هيبقى الـ sw صاحب اقل Macadd.

---

* لو الشبكة كلها شغالة و stable ودخلت sw جديد في الشبكة وعليه اقل MAC ساعتها الـ sw الجديد هو اللي هيبقى الـ root.
* الـ sw root اول ما بقى root كل الـ Int اللي عليه ساعتها هتبقى في حالة اسمها Designated forward "DF"

وكل الـ Data هتعدي من عليه.

© كل الـ sw التانية هتبقى (non-root switch) وساعتها كلها هيبقى عليه Int واحد اسمه root port.

Link speed	COST "IEEE"
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

هيبدأ احسب أقل سوتش قيمت الـ cost على شان يوصل للـ root
الـ Int اللي هيبقى عن طريقه الـ cost اقل سواتش الـ
Int ده هيبقى هو الـ root int وهيبقى في حالة
اسمها Root forword (RF) ويفتح (هيسمح) للـ Data تعدي
من عليه

---

③ كل سلكة هيبقى عليها D.Port
هيبص على الـ سلوك اللي مش عليها D.Port وهيقارن عن طريق
الـ cost تبع الـ sw على شان يوصل بالـ root وهيختار
الأقل.
لو حصل Tie هيتحل عن طريق الـ Int اللي مربوط بـ sw
ليه Mac اقل.

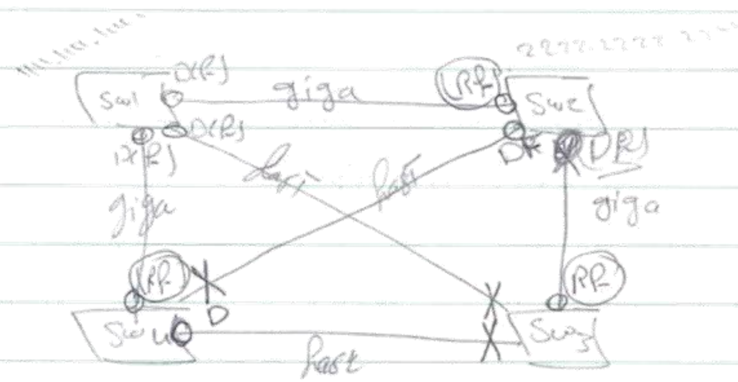
---

④ اي Int متطبقش عليه الـ Rules هيتعمله Block ④

Logically down.

وهيبقى فى حالة اسمها Logically down.

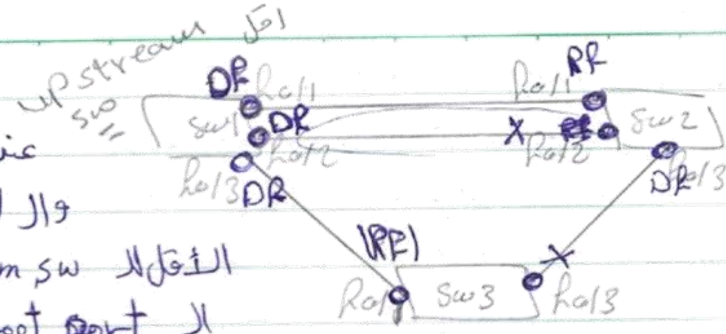
Ex:-



* بعدما بقى sw Root هيبعت كل 2 sec BPDU عن طريق
الـ D(P) اللي للـ sw ويستقبل باقي السويتشات على الـ Root
port ثم تمررها للـ designated port.

Ex

عند حدوث tie في الـ cost
والـ MAC add فبدال port ID
الأقل الـ sw upstream هو الذي سيكون
الـ root port.



x at Convergance

الـ root switch بيبعت hello كل 2 sec.

- STP port states:-

1. Disabled => يعني انا اللي عاملة shutdown بإيدي
2. Blocked
3. listening => بيـ listen للـ BPDU لمدة 15sec وبعد كدة هيتحول لحالة الـ learning
4. learning => يبدأ يتعلم الـ Mac add ويحطها في Table لمدة 15sec وبعد كدة يتحول لـ forward
5. Forward =>

BPDU Timers

* Hello time:- By default 2 sec بتبعت كل

* Forward delay:- الفترة اللي بتقعد فيها الport وهي بتتعدل من Blocked لـ Forward <= 15 sec + 15 sec = 30

* Maximum age:-

= 10 * hello = 2 * 10 = 20 sec.

---

* at change

① If root bridge goes down:-

all other switches go to blocking state for 20 sec then → go for listening state for 15 sec then → to learning Mac for 15 sec ⇒ 15 + 15 + 20 = 50 sec

② If any other change happened

all routers goes directly for listing for 15 sec then ⇒ goes to learning for 15 sec

⇒ 15 + 15 = 30 sec.

heebs:-

* STP is enabled by default on all Cisco SWs.
* Show spanning-tree ↵

على شان افضل 800 مين هو ال root

SW1 # Config t ↵
SW1(Config) # spanning-tree ?
SW1(Config) # spanning-tree vlan 1 ?
SW1(Config) # spanning-tree vlan 1 — لجعل ال Enable ال STP على VLAN 1
SW1(Config) # spanning-tree vlan 1 root ?
SW1(Config) # " " " " primary
SW1 # show spanning-tree ↵

هلاقي انه قلل ال Priority

priority is increments of 4096
* spanning-tree vlan 1 priority 4096

PVST ⇒ Per-VLAN STP (Default on Cisco SWs)
supports ISL only

PVST+ ⇒ supports ISL and dot1q

كل مرة تطبق STP على Vlan لوحدها

extended System ID :-

VLAN1 ⇒ Priority ⇒ = 32768 + 1 = 32769 (default; 1 = VLAN ID)

Vlan 10 ⇒ " ⇒ = 32768 + 10 = 32778

* عند تغيير ال priority عن طريق أمر root primary فإنه shortcut لأمر ال priority.

STP enhancement :- تحسينات

* Port Fast : خاصة بـ Connecting to PC بيتحول
من Block لـ Forward في No time «على طول».
* اذا حدث تغير على السويتش
فانه يرسل TCN لكل السويتشات

ويتطبع تحت بـ Int لعمل flush لل MAC table. ولما حدث تغير على
int مربوط بـ pc لا يوجد داعي لعمل flush على مستوى الشبكة كذلك لا يوجد
مخاطر من جعل ال int يتحول من BLK لـ FWD
مباشره دون الخوف من حدوث switching loop.

* int fa0/1
* No show spanning-tree ↲
* Shut down
* No shutdown ↲
* spanning-tree portfast ↲
* switchport mode access.

واذا استلم السويتش BPDU على ذلك ال int سيجعل ال portfast disable.

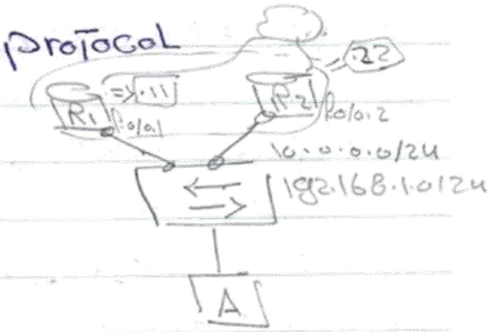
* RSTP ⇒ rapid-STP

- STP ⇒ Blocking ⇒ listing (15sec) ⇒ Learning (15sec) ⇒ Forward
  Max age = 10 * hello = 20 Sec.
- RSTP ⇒ Discarding ⇒ learning (15sec) ⇒ Forward
  max age = 3 * hello = 6 Sec
  كل sec بتبعت ال hello

802.1D ⇒ STP IEEE

802.1w ⇒ RSTP IEEE

Redundancy protocol



لو R1 (down) على طول الأجهزة تبعت
على R2 لوحدها وده عن طريقه
واحد من ال Protocols ⟵

1- HSRP ⇒ Hot standby router protocol
((Cisco Propritary))

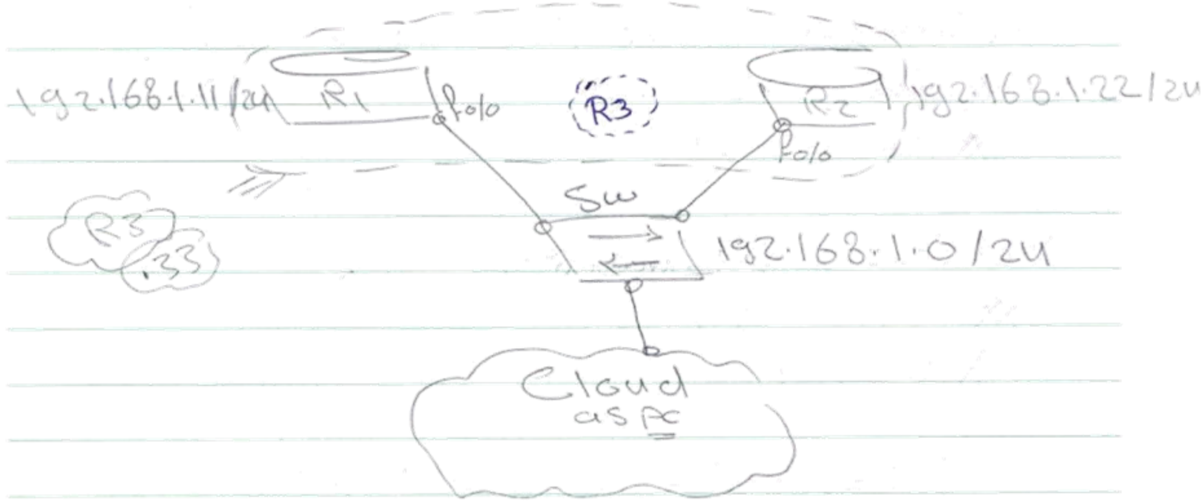
2- VRRP ⇒ Virtual router redundancy protocol
((IEEE standard))

3- GLBP ⇒ Gateway load balance protocol
((Cisco Propritary))

هاجي على R1 و R2 وهاحطهم في Group وهطلع
منهم Router وهمي وهيبقى ليه MAC خاص بيه
(R3) وال أجهزة هتشاور عليه عن طريق ال Gateway.
وفي واقع الأمر R3 هتشاور على R1 لكن الأجهزة متوصلة
على ال Internet عن طريق R1 ولو R1 وقع ساعتها R3
هيشاور على R2.

Lab: نفس الكلام هيطبق على ال R هو اللي هيتطبق على L3sw

GNS ⇒ Run as administrator



r1(Config)# int f0/0 ↵

※ Ip add 192.168.1.11 255.255.255.0 ↵

No shut ↵

r2(Config)# int f0/0 ↵

※ IP add 192.168.1.22 255.255.255.0 ↵

No shut ↵

r1(Config)# f0/0 ↵

※ Stand by 1 ? — باحط أي رقم Group طالما IP

※ Stand by 1 IP 192.168.1.33 ↵ ↵

The IP of the virtual router.

R2(Config)# int f0/0
* standby 1 ip 192.168.1.33 ↵

R1(Config)#line vty 0 4 ↵
* pass 123 ↵
* login ↵

R2(Config)#line vty 0 4 ↵
* pass 123 ↵
* login ↵

PC => Cmd => Telnet 192.168.1.33

Active. على R1 هلاق انه بشاور على شاشة جهاز

Ping 192.168.1.33 -t ↵

* R1(Config-if) #shut down ↵

هلاق Ping واحدة جهاز الى وقت وجهاز نفسه
تلقائي على R2 و R2 صار الى يقول Active.

⇐ أى R هيبقى Active وايهم Standby ؟؟

ال R اللي هيقوم الأول هو اللي هيبقى Active.
ولو قاموا فى نفس الوقت, اللي هيحصل ال Tie هيبقى ال
Priority ⇐ اللي ليه Priority اعلى هو ال Active
بس هيبقى ال Priority ⇐ (100) ⇐ By default
ساعتها اللي هيحصل ال Tie ال R اللي IP بتاعه
اعلى هيكون هو ال active والآخر standby.

r1 ## Show Standby ↵

r2 ## Show standby ↵

Mac ⇒ 0000.0C07.AC01

↳ بيساوى صفر AUI
↳ بيساوى مثبتاه لل HSRP
↳ رقم ال Group دا Hexa
يعنى لو رقم ال Group ١٥ هيكتبه ⇐ 0A

Hello time ⇒ 3 sec
hold time ⇒ 10 sec

يعنى كل 3sec ال 2 R بيبعتوا لبعض Hello علشان يعرفوا
بعض انهم شغالين

"الاستيلاء"
Preemption disabled

r2(Config-if)#standby 1 ?

※ standby ◦ 1 ◦ preempt

يعني لما R2 يقوم تاني يسترد هو الـ Active "يستولي عليه"

ويتعدى عـ الـ Priority الـ R اللي بيها Priority اعلى"

※ standby ◦ 1 ◦ Priority 150 ↵

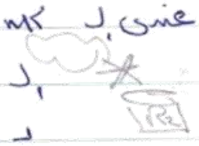
بعد عمل enable لـ preempt فإن الراوتر اللي له Priority اعلى

سيكون هو الـ active مجدداً بعد ما يصبح up مجدداً.

لو عندي الـ link بين الـ R والـ ISP وقع فأنا عاوزه اقبل

الـ int اللي واصل بالـ ISP اول مايقع يقلل الـ Priority

بـ 60 علشان كده ان R1 هيبقى الـ Active



- بفرض ان الـ int loop 2 هو اللي يرتبط بالـ ISP.

r2(Config)#Int loop2 ↵

r2(Config-if)# IP add# 2.2.2.2 255.255.255.255 ↵

r2(Config)#Int f0/0 ↵

r2(Config-if)# standby 1 Track loop2 60 ↵

↳ يقلل الـ Priority بـ 60

+ preempt should be enabled in conjunction with tracking ints.

r1(Config-if)# standby 1 preempt ↵

مشاكل HSRP ان الـ Timers عالية

hello ← → hold time

r2(Config-if)# standby 1 timers 1 3

ويمكن وضعها بالـ msec ولكنه غير مستحب.

- VRRP => هو هو ال HSRP مع بعض الفروق

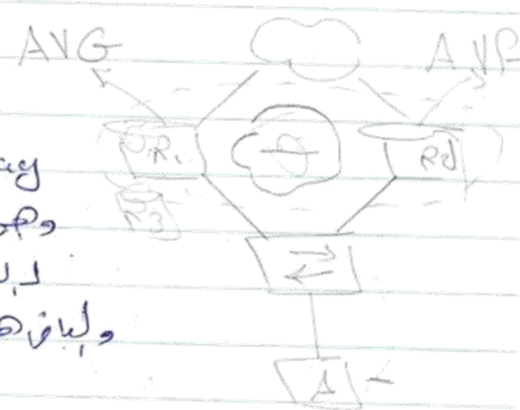
① "IEEE Standard"
② hello => 1 sec
③ hold => 3 sec + skew time.
④ preempt => enabled by default.
⑤ R3 => ينفع ياخد IP زي ال IP بتاع R من نفس ال Group بعكس ال HSRP

=> lab
re(config-if)# vrrp ?
vrrp 1 ?

#do show vrrp ↵

- GLBP => Cisco proprietary
"Gateway load balance"
انما ال HSRP بعمل الفكرة اني اعمل load balance

AVG => بيختار R من الموجودين ويعمله AVG
Active virtual Gateway
وهو مسؤول عن توزيع ال MAC
لل PC
والباقي هيبقى AVF => Active virtual forwarder.



f0/0 ↵
#GLBP 1 ?

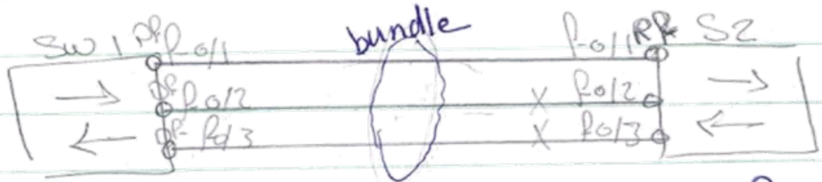
R(Config-if)#glbp 1 ?

ANG ← اللي هيبقى أعلى Priority ←

* weighting => " load balance " عن طريقه بأوزع ال

" Channel Group "

etherchannel
portchannel



الفكرة إني أخلي ال 3 interfaces بيبعتوا Data
بين هاتين بينهم " equal COST " على frame
load Balance ← بالتالي ← frame على ال سلك التاني
وكذلك على التالتة .

ومن حقي إني أوصل ال 2 sw ب 8 أسلاك .

lab:-

Sw2(Config)

* Int range f0/0 0 - 03
* shutdown
* channel- Protocol ?

2 channel protocol عندي

- on ⇒ (hard code eth channel) بعين بإيدي على كل Int

- LACP "link aggregation protocol" (control)

- PAgP (Port aggregation protocol) — Auto negotiation

↳ cisco proprietary

labs:-

sw2(config-if-range)# channel-group 1 mode ?

LACP → Active:- = desirable
↳ passive:- = auto

PAGP → auto = passive
↳ desirable = active

channel-group 1 mode on
no shut
⇒ sw1 → نفس الكلام
no shutdown

sw1# show spanning-tree ↵
show etherchannel 1 ↵ ⇒ علشان اشوف اللي انا عملته
summary ↵
(SU) ⇐ يعني اشتغل

~~ال STP بيتعامل مع ال channelgroup كأنه int واحد وهو ال Port channel.~~

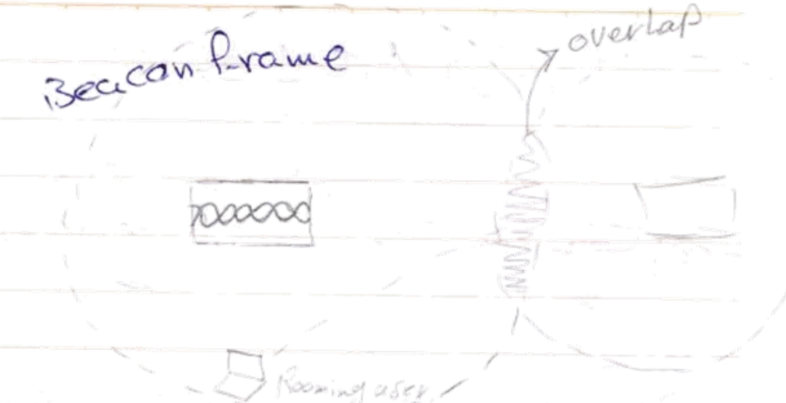
((wireless))

wireless Tech. اغلب بعض غرف شبكات لازم او معظمها شبكة (شركة مزود ، بالاجهزة)

	Ethernet	wireless
IEEE	802.3	802.11
media	Copper-Glass	air
data format	electricity-light	Radio waves

((wireless Topology))

- Ad-hoc (IBSS)
  - Independent basic service set.
  - No Access point
- infrastructure
  - BSS — Basic service set
    - one Access point
  - ESS — Extended service set
    - more than one Access point.



لازم ال user في منطقة ال overlap تكون قوة الشبكة
من 15% ـــ 10

ناخد config. على الشبكة بتاعتي <= Service Set
و ابنيها Broadcast على frame اسمها Beacon frame

Recommended مطلعهاش تتذاع علشان ال Security
واعمل Disable لل Beacon frame.

802.11 (2.4 GHZ - 1,2 Mbps) (frequency — speed)

802.11a (5GHZ - 54 Mbps) (frequency — speed)

802.11b (2.4GHZ - 1,2,5,11 Mbps)
↳ spreed spectrum

802.11G (2.4GHZ - 54 MbPS)

(b,G) => Compatable بيفهموا بعض

CSMA/CA ⇒

↳ Callision avoidance

Freq. يتجنب الـ Callision عن طريق بيبعت على Freq و بيشتغل على Freq

---

Bluetooth ⇒ V1 ⇒ 2.4GHZ → 10m
1Mbps

↳ V2 ⇒ 2.4GHZ → 35m → 2Mbps

---

wireless signal attenuation:-

- interference
- environmental variables العوامل الجوية
- Antenna type and length طول الـ انتنا ونوعها

---

wireless sequrity:-

- war drive ⇒

Attack ازاي احمي نفسي من انواع الـ

① عن طريق الـ MAC add ⇐ يعني الجهاز الـ Mac بتاعه مش هيطلع نت

٤) عن طريق الـ Authentication ⇐ باحط Key على شبكة الـ wireless بتاعتي

وعندي نوعين من التشفير → wep

wep: "ضعيف جدا" و "صغير جدا" (56bit) ويعتمد على نوع encryption ضعيف اسمه "TKIP"

→ WPA,V1,V2

أعلى .sec

ويتضرب برضو

والـ dynamic Key

بيتغير على طول.

٣) security applianse

اجهزة بتحمي الـ data زي الـ (IDS, IPS