University Of El Mansura
Faculty Of Engineering
Networking lap

CCNA Tracks

Prepared By

Eng. Ahmed Abdullah

DAY 1

network: is a group of devices connected with each other to make a specific service.

CCNA Track
Prepared by ENG:
Ahmed Abdallah

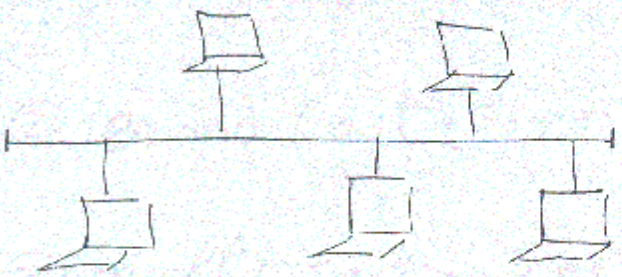
network advantages:

1- to make data share
2- can use one printer
3- can make live conversation

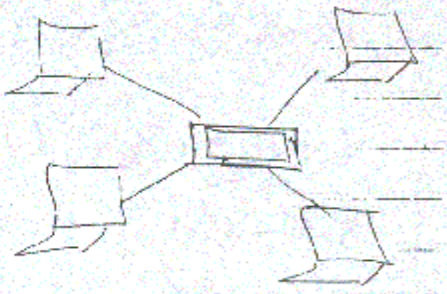
network has 3 main components:

1- computers
2- network devices
3- cables to make connections

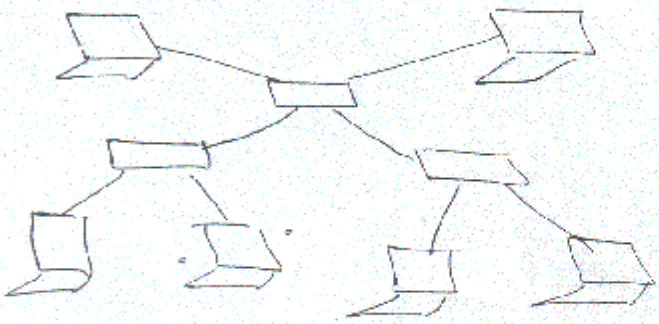
physical network topologies:



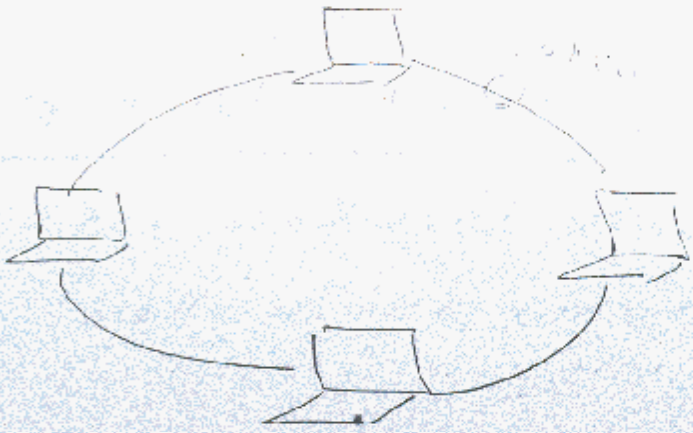
1 Bus topology



2 Star topology



3 Extended star



4 ring topology

تكلم عن مثالة كل نوع من الأنواع الأربعة السابقة

* logical topology

هي الطريقة التي سأرسل بها الـ data عبر الـ physical topology اللي إنت عملتها

يوجد ٣ أنواع

① uni cast: إرسال من جهاز لآخر

② Broad cast: إرسال من جهاز إلى كل الأجهزة الموجودة في الشبكة

③ multi cast: إرسال من جهاز إلى مجموعة معينة من الأجهزة الموجودة

types of network (size)

① LAN (local area network)

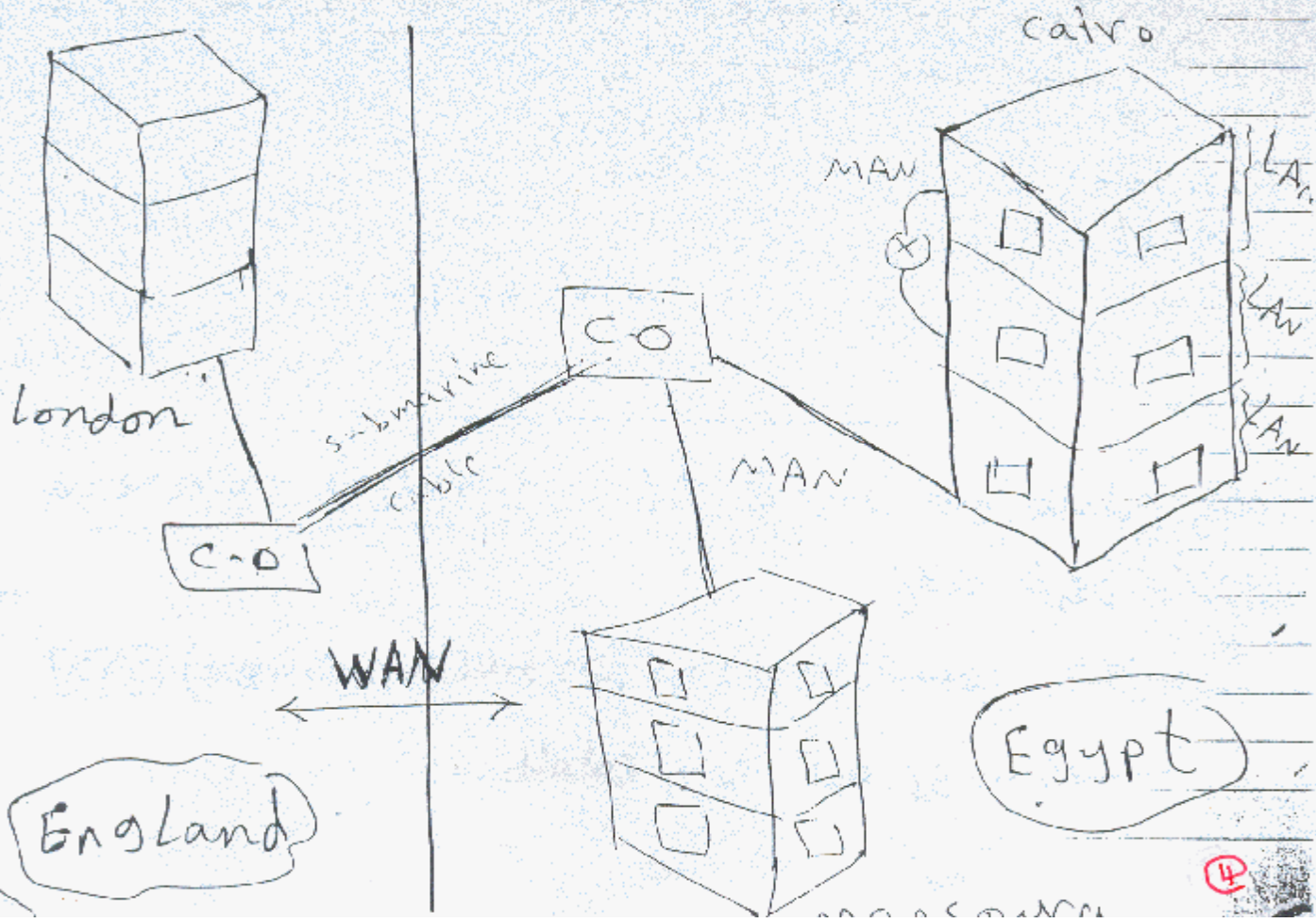
ex small network connected by ethernet cables

② MAN (metropolitan area network)

ex connection between some of LAN's

③ WAN (wide area network)

ex connection between LAN in egypt & another LAN in USA.



OSI reference model

open system inter connection

7 Layers في الشبكات بتقسيم كل الـ model هذا الـ تم

كما بالشكل

7	application
6	Presentation
5	session
4	transport
3	network
2	data link
1	physical

* **application layer:** user interface which you deal with

* **Presentation layer:** data formatting
  - encrypted data
  - Compressed data

protocol data unit

PDU : encrypted data

data الـ

* **session layer:** dst & src بين dialog يفتح

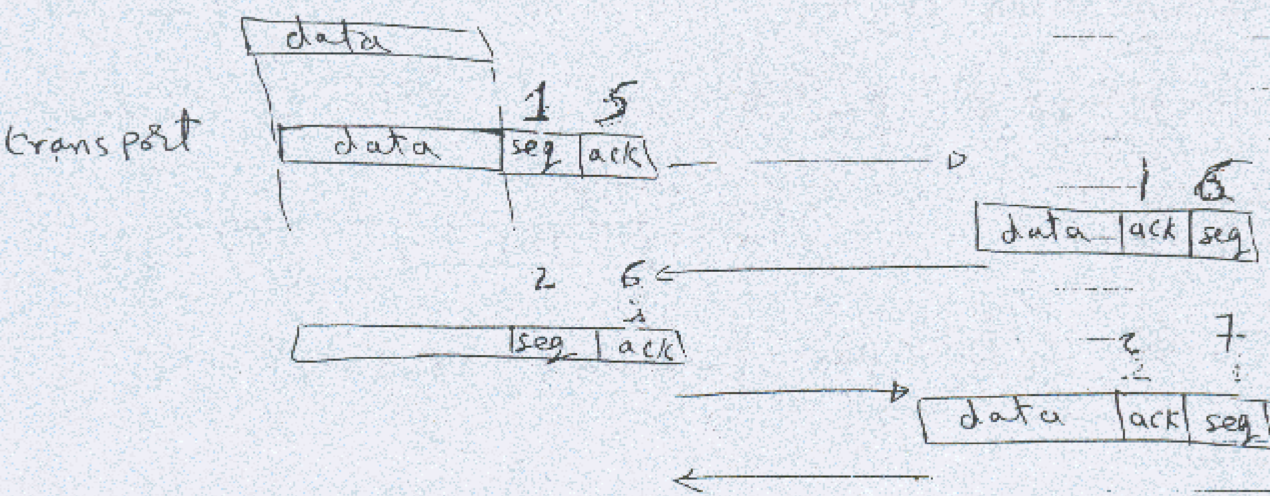
وينهاء عملية النقل

RPC (remote Procedure call) في (software) يتم

dialog. كل ما يحدث هذا الـ

* transport layer : إيه هي وظايف الـ layer دي

[1]
- → reliable service → it puts → seq. No / ack. No.
- → unreliable service → it puts → seq. No. only



عندنا هنا 2 protocols فيها → (transport layer)
اشهرهم

TCP (transmission control protocol) : → reliable service

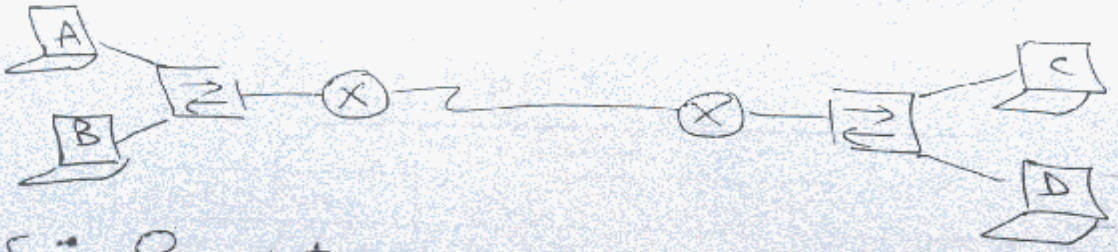
UDP (user datagram protocol) : → unreliable service

[2] ال data (بتقسمها) segmentation بتعمل ال transport layer

segment 1 | segment 2 | segment 3

PDU : "segment"

* network layer : best path selection

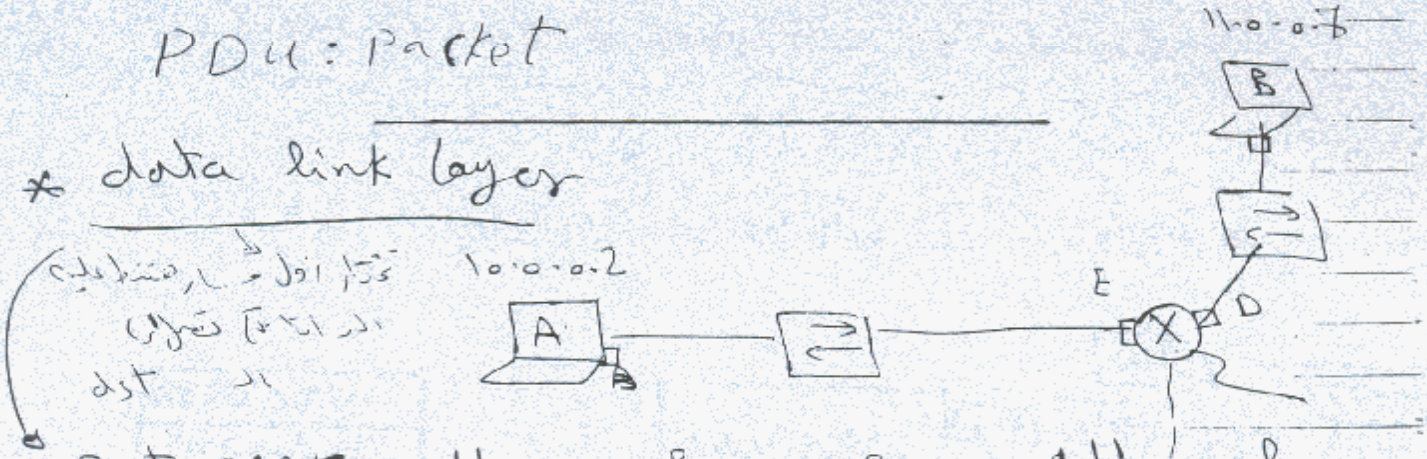


في هذه packet الراوتر CCA مهمتي data الذي routing يعمل dst Ip & src Ip

IP : internet protocol addressing يعني عنوان

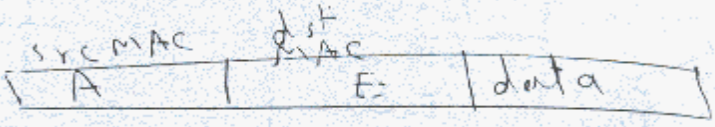
PDU : Packet

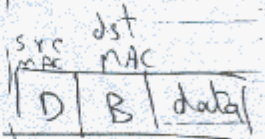
* data link layer



put MAC address of src & MAC address of dst on data frame

IP add: Logical address
MAC add: physical add





data logically moved from 10.0.0.2 to 11.0.0.7

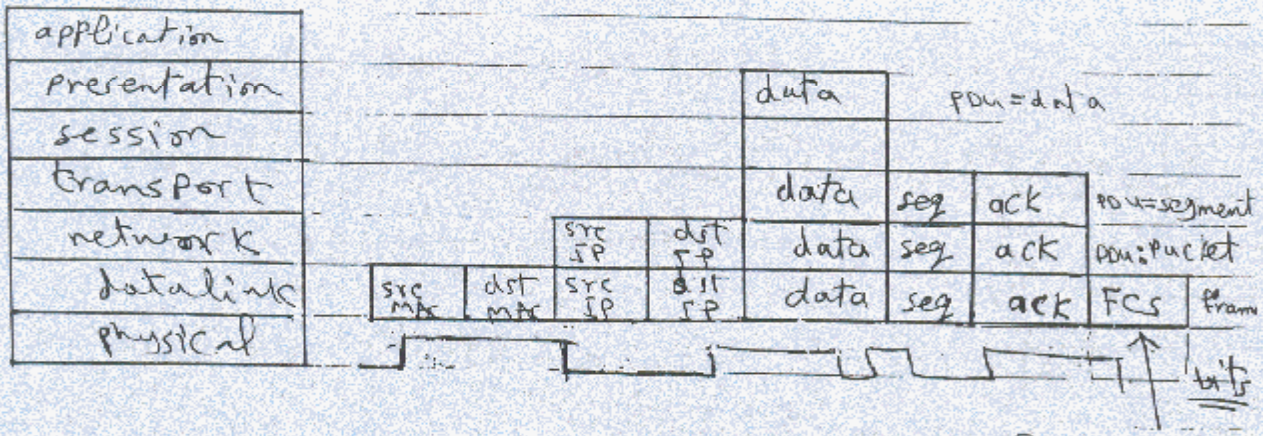
put physically it jump using MAC address

de-encapsulation & encapsulation يعني

PDU : "frame"

*physical layer : dealing with cables, repeaters & electerical signals

PDU: "bits"

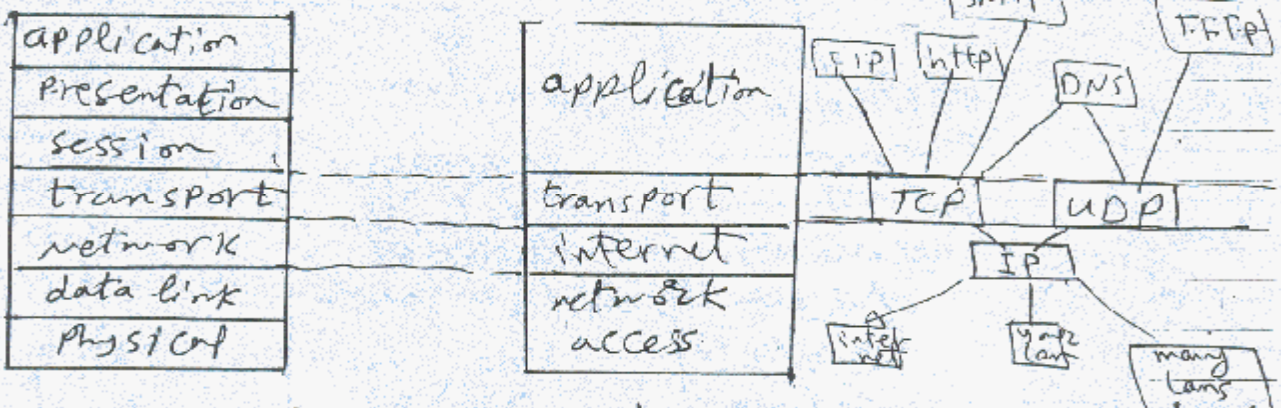


(seq no) مش، بيعملوا Frame لل error detection بيستخدموا اللي

dst frame لل drop بيعمل FCS مش، مضبوط مع

OSI Vs TCP/IP

TCP IP لل OSI دا فهم تم



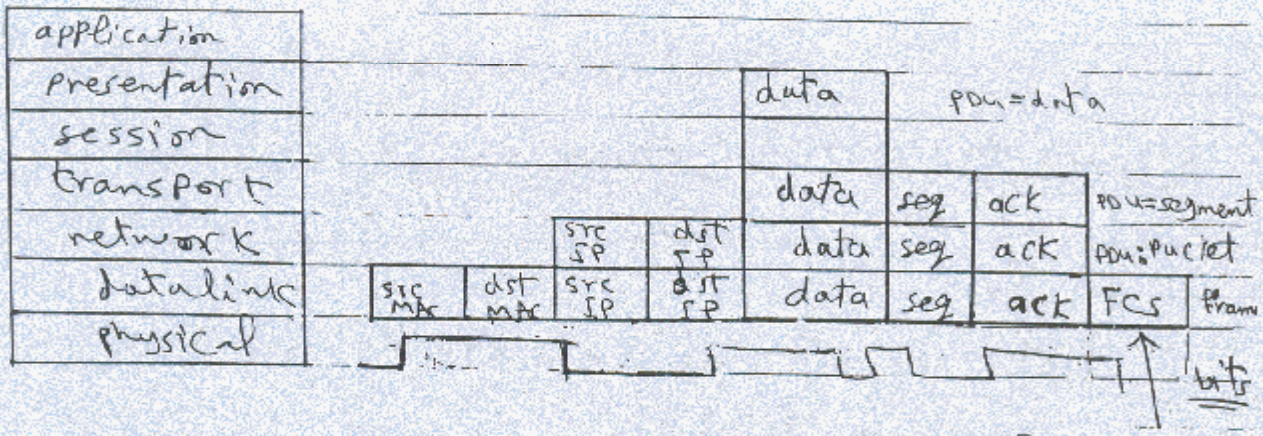
(applications) protocols لل (application layer) فيه بروتوكولات

بتاعة TCP او UDP ، ومن الآخر الـ IP protocols هي اللي بتعمل

routing data على الـ backbone

* physical layer : dealing with cables, repeaters & electerical signals

PDU: "bits"

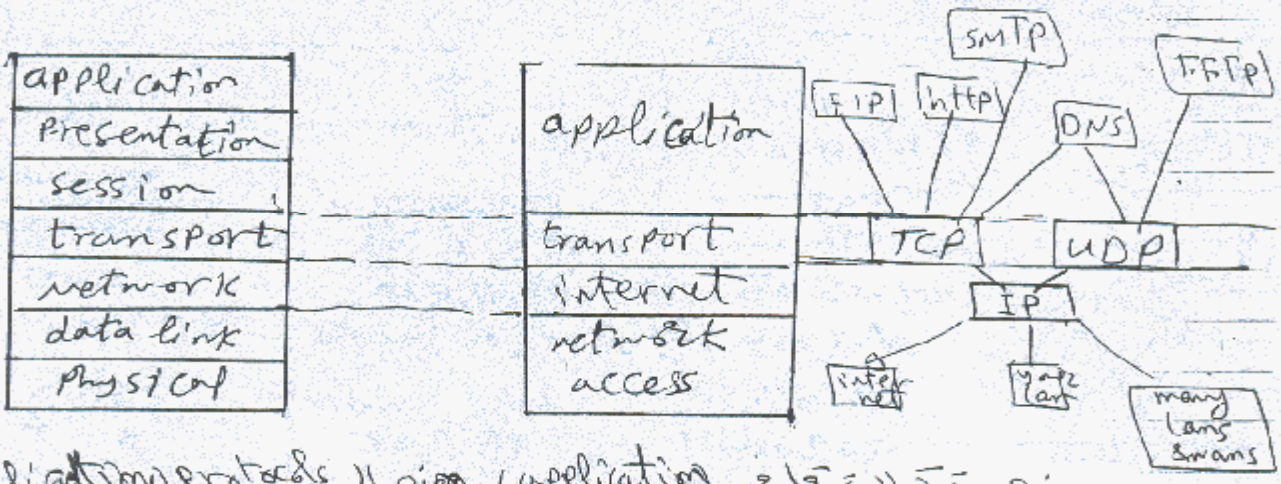


(seq no) في Header الـ Frame وال error detection بيتعمل

dst الـ Frame الـ drop بيتعمل FCS في حالة

OSI Vs TCP/IP

TCP IP الـ OSI بنفهم كيف بيتعمل الـ



(applications) protocols الـ (application layer) في بروتوكولات تتعامل

TCP او UDP ومن الـ TCP الـ IP protocols بتخدم

data الـ backbone هو الـ

application layer بروتوكولات

(FTP, TFTP (trivial)) → sending files

(HTTP) → web browser

(telnet) → remote Login

(SMTP, POP3) → sending & receiving Emails

ملحوظة

TCP → reliable service → connection oriented
src & dst are up

UDP → unreliable service → connection less oriented

Ethernet LAN

cables types

Fiber

singlemode — core — clade — غطاء — واحدة

5/125 (core / clad)

- ST connector

multimode — signal — core clad 50/125

- use SC connector

Cupper cables

1. UTP unshelfed TP — يقل وصلة حتى ١٠٠ متر وبعد ذلك نزود بتابع (repeater)
   STP sheild TP — النحاس المعدني
2. coaxial cable — 100 Mbps — حتى 500m

Twisted pair ← 10Mbps يعمل بـ UTP يستخدم

ex: 10 Base T → Twisted pair
10 Mbps
base band

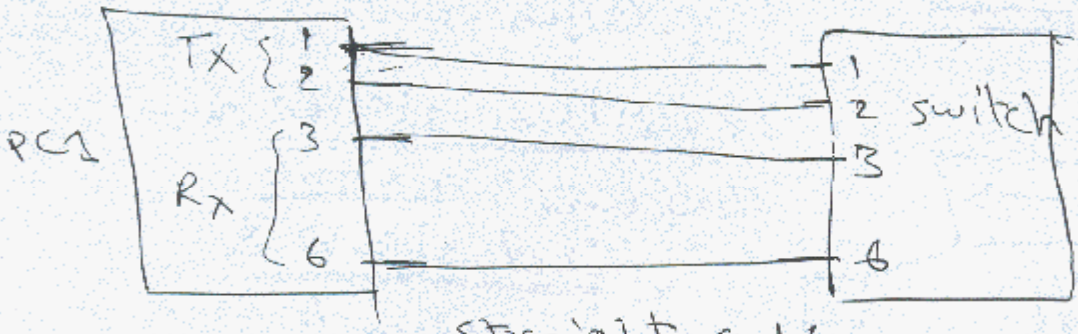
ex: 10 Base 5 → Thicknet يسمى هذا الكابل
10 Mbps
500 m ← coaxial

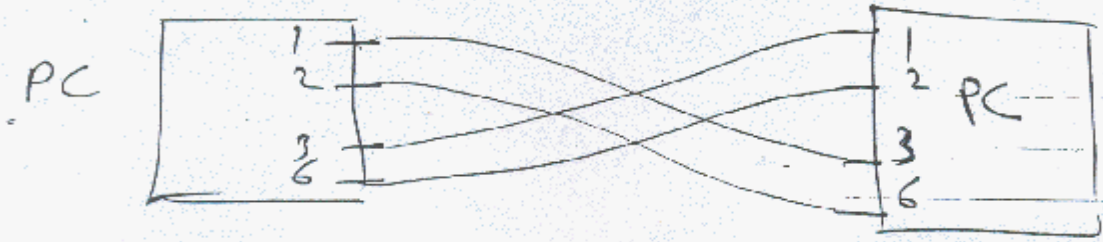
ex: 10 Base 2 ← Thin net
200 m

ex: 100 Base TX
100 Mbps
Twisted pair
Full duplex

ex: 100 Base FX ← fiber optics

Connection of UTP (straigh & cross over connection)





data terminal equipment

DTE	DCE
PC	modem
router	Hub
	switch

← data Communicating equipment

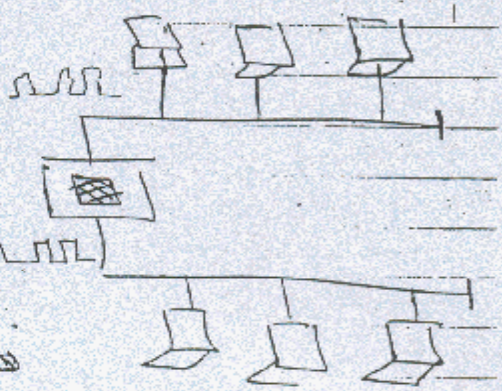
DTE → DCE → straight

DTE → DTE or DCE & DCE → cross

* Layer 1 devices

1) repeater

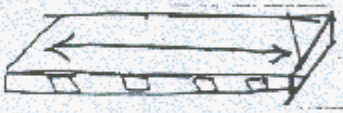
- 2 segments
- make signal regeneration



4 repeaters ملاحظة: لا يمكن إنشاء أكثر من داخل نفس الـ LAN

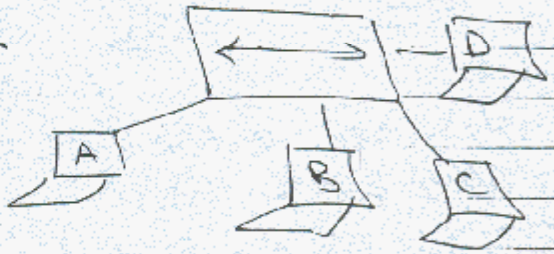
2) HuB : → multi repeater

→ half duplex يستقبل ويرسل في نفس الوقت



→ single collision domain & single B-C domain

broad cast



DAY 2

CCNA course prepared by ENG: ahmed abdallah

ether net over view :

1 MAC address [media access control]

consits of 12 hexa decimal bits = 48 bits

123F.ABBC.1245

OUI — serial No. of NIC card

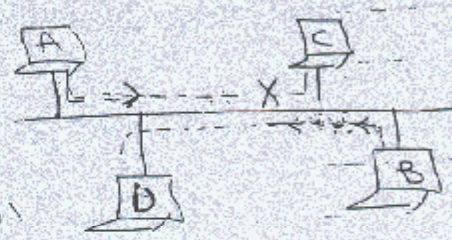
organization unique identifier
وهو كود الشركة المصنعة للكارت

2 CSMA/CD [carrier sensing multiple access with collision detection]

وهو متبع في Bus topology للتغلب على حدوث collision
Bus topology ← half duplex

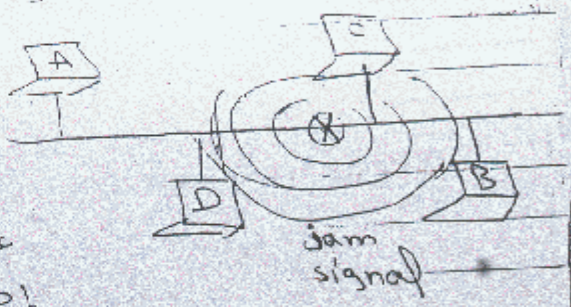
طريقة العمل operation :

لو أنه أي جهاز يريد إرسال (Bus) عبر الكابل
sense أن هناك data فإنه يقوم بعمل
للكابل فلو وجد أنه هناك بيانات ترسل فإنه
يجاهد على الكابل sense حتى يجده فارغ وبعد ذلك يمكنه استخدام
الكابل لإرسال البيانات



المشكلة : لو أنه الكابل فارغ وقام الجهاز A والجهاز B بعمل sense
للكابل في نفس اللحظة فوجدوه فارغ فيقوم كلاهما بإرسال البيانات
وبالتالي يحدث collision وللتغلب على هذه المشكلة تم عمل أي

الجهاز الذى يستقبل الـ collision وليكن C

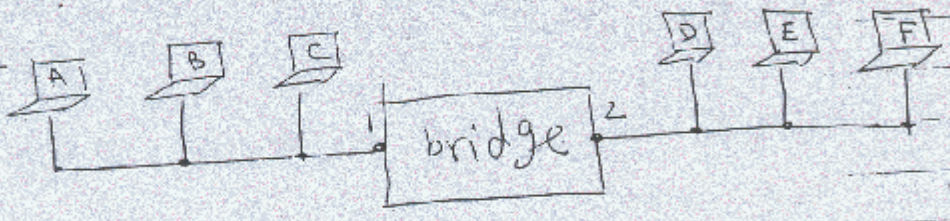


يقوم بإرسال Jamsignal لكل الأجهزة التى بالشبكة يقول لهم توقفوا عن الإرسال فقد حدث إصطدام فيتوقف الجميع ويقوم بإعطاء كل واحد فيهم فترة زمنية يتوقف فيها ثم يعاود الكابل ولكن كل فترة زمنية عند أى جهاز مختلفة عن الجهاز الآخر لتفادى حدوث الـ collision مرة أخرى.

* Layer 2 devices

1. NIC: MAC address is burned on it

2. Bridge:



A	B	C	1
D	E	F	2

- إذا أراد A أن يرسل لـ B فإن الـ bridge يقوم بعمل Port 1 & port 2 لأن A & B فى نفس الـ segment أما إذا أراد A أن يرسل إلى D فإن الـ bridge يقوم بعمل port 2 (port 1) لأن D (data) فى segment آخر وكذلك E & F فى نفس الـ segment أيضاً.
- تقوم عملية الـ Forwarding فى الـ bridge بـ software حيث يحتوى على جدول به الـ MAC's الخاصة بالأجهزة المتصلة به

- switching in Bridge depend on Software

[3] switch:

- more ports Than bridge
- faster Than bridge (depend on hardware ASIC)

ASIC: application system I.C's

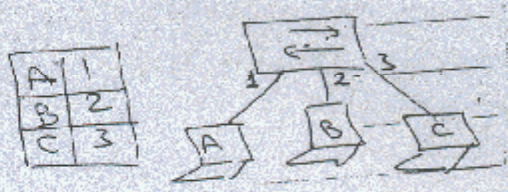
→ we know That Hardware processing is faster Than software processing

switch fns

1- address learning: → check The source MAC in The frame

في البداية الأجهزة موصلة بال switch ولم تقوموا بالإرسال فبالتالي صولم يتعلم بعد

وإذا قام أي جهاز من هذه الأجهزة بالإرسال فإنه يسجل في الجدول عنده صاحب الـ MAC ويسجل أيضاً رقم الـ Port التي أتى منها



يتم تكوين الجدول

2- Forwarding: how switch Pass The data

ⓐ Floading: قبل أن يتعلم الـ switch أين يذهب الـ data في الجدول خارج

يفترض أنه A أرسل data فإنه يقوم بإرسالها إلى كل البورتات الأخرى (Floading) وكلهم ما عدا الذي عرف أنه الجهاز B موجود

أي عمل Floading فيتم تخزينه في الجدول - فيحدث الـ Ports

مع Floading

→ unknown unicast

- broad cast, multi cast

(b) Forwarding by micro segmentation:

في هذه الحالة يكون الـ switch قد تعلم مسبقاً وتعرف على كل الـ devices الموصلة به.

for known unicast, switch often adedicated link between source & destenation

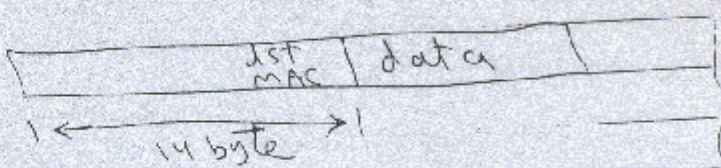
→ There are 3 Actions during The forwarding

(A) store and forward:

check all The frame to prevent errors

(B) cut Through:

don't check any errors, switch read first 14 byte to determine The dst.



(C) Fragment free

switch read first 64byte

أي يقرأ الـ dst MAC، ويقرأ جزء من الـ data وسمي الأقل تتبع صناعية وجود errors من أنواع الـ runt frame error ←

* Errors type

CRC error	runt Frame error	giant frame error
0 → 1 1 → 0	smaller Than 64byte due to collision	greater-Than 1518 byte (Frame الزيادة) due to encapsulation

3 Remove Layer 2 Loops

يعرف انها عملها بتشغيل switch الاكبر

ويعرف انه A اراد انه يرسل لـ B

يقوم X switch بانه

يعمل Flooding وكنه عارف انه

port 1 الجهاز A موجود ع الـ

switch 2 & switch 3 data تتضيف الـ

ويقوم كمان مخزنا بعمل flooding وكمان

علم انه اذا اراد انه يرسل لـ الجهاز switch 2

A فانه يرسل من port 4 وكذلك switch W

فانه يرسل من port 9

port 6 & port 7 من switch 2 هيقبض data تعمل الـ

وبالتالي فانه يخزن الجدول الخاص به وهذه مشكلة حيث

انه اذا اراد انه يرسل لـ الجهاز A فانه سوف يفكر انه جزء من

port 6 ولا من port 7 (Loop) ويستمر هذا action ولا يقوم بارسال

الـ data دائما الطبيعي بالنسبة لـ switch يوجد port محدد للوصول لـ

host محدد

حل المشكلة السابقة: نقوم بعمل

STP [spanning tree protocol]

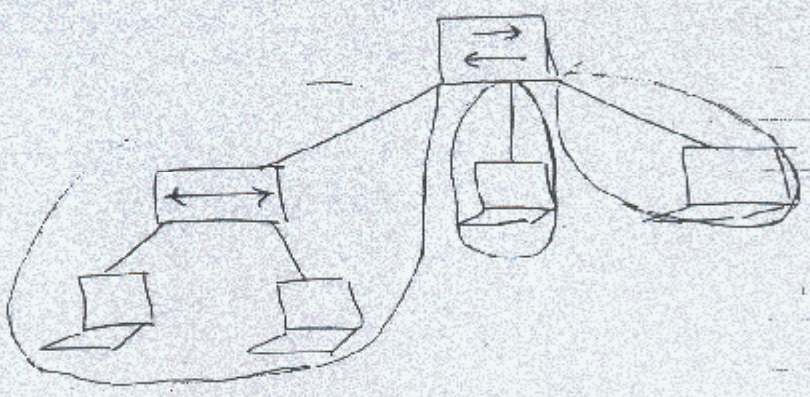
وتفعل الـ switch فيقوم هذا البروتوكول بتعطيل أحد المسارات المؤدية إلى الجهاز A ويكون هذا المسار واحد يعمل وإذا حدث disconnect يتم تفعيل المسار الآخر (الإحتياطي) فإنه stp

وسوف نتحدث عن STP بالتفصيل عند الحديث عن switching

hint

switch ports → single broad cast domain
→ multiple collision domain

example: find number of collision domains and number of broad cast domain in the network below?



No. of broad cast domain = 1

No. of collision domain = 3

Revision

decimal system: (النظام العشري)

وهي الأرقام من 0 ← 9

Binary system (النظام الثنائي)

ويتكون من العددان 0 و 1

example

$$\begin{array}{r} 1 \\ 1+ \\ \hline 10 \end{array}$$ ← يمثل 2 في النظام العشري

example

$$\begin{array}{r} 1+ \\ 1 \\ 1+ \\ \hline 11 \end{array}$$ ← يمثل 3 في النظام العشري

converting from decimal to Binary:

ex $(16)_{10} = (\quad)_2$

2 | 16		
2 | 8	0	
2 | 4	0	
2 | 2	0	
2 | 1	0	
0	1	

يكتب هذا الرقم مع كتابة الصفر على اليسار ← 10000

ex $(115)_{10} = (\text{-----})_2$ → 1110011

2	115	
2	57	1
2	28	1
2	14	0
2	7	0
2	3	1
2	1	1
	0	1

converting from Binary to decimal

ex $(101)_2 = (\text{-----})_{10}$ (5)

$a_2\ a_1\ a_0$

$= 1*2^0 + 0*2^1 + 1*2^2$

$= 1 + 0 + 4 = 5$

ex $(1100111)_2 = (\text{-----})_{10}$ (115)

$a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0$

$= 1*2^0 + 1*2^1 + 0*2^2 + 0*2^3 + 1*2^4 + 1*2^5 + 1*2^6$

$= 1 + 2 + 16 + 32 + 64 = 115$

CCNA track

Prepared by ENG: Ahmed Abdallah

Internet [network] layer :

- support logical IP address
- perform routing (best path selection)
- connect different data link technologies together [ethernet, token ring, ---]

* layer 3 Protocols :

- IP: internet Protocol & IPX & APPLE TALK
- ICMP: internet control message protocol
  ↳ provide message to describe network action like [Ping]
- ARP & RARP ← [illegible]
- Routing Protocols: software on router to help it to find best path to reach to dst

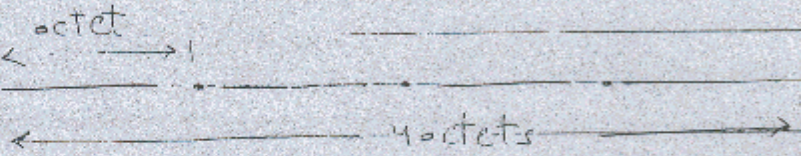
IP : internet protocol

- provide logical addressing

IP addressing : each host in the LAN must have

- a unique IP address
- IP address identify the network ID & host ID in one address

IP V.4 :



- 32 bit address in doted form [4 octets] each has 8 bits
- can be presented in dotted decimal form
  [each octet value 0 → 255]

ex : 1100 0000 . 0000 1100 . 0000 0111 . 0000 0001

OR 192 . 12 . 7 . 1

1000 0000 → 128	0000 0001 → 1
1100 0000 → 192	0000 0011 → 3
1110 0000 → 224	0000 0111 → 7
1111 0000 → 240	0000 1111 → 15

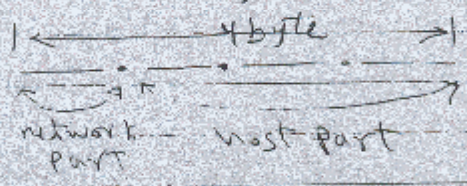
هو هيئة عالمية مسؤلة عن توزيع الـ IP's لـ

[IANA] internet associate for network addressing

لازم يكون عندي real IP عشان أقدر أدخل على الإنترنت إذا احتاج

IANA شركة

IP classes

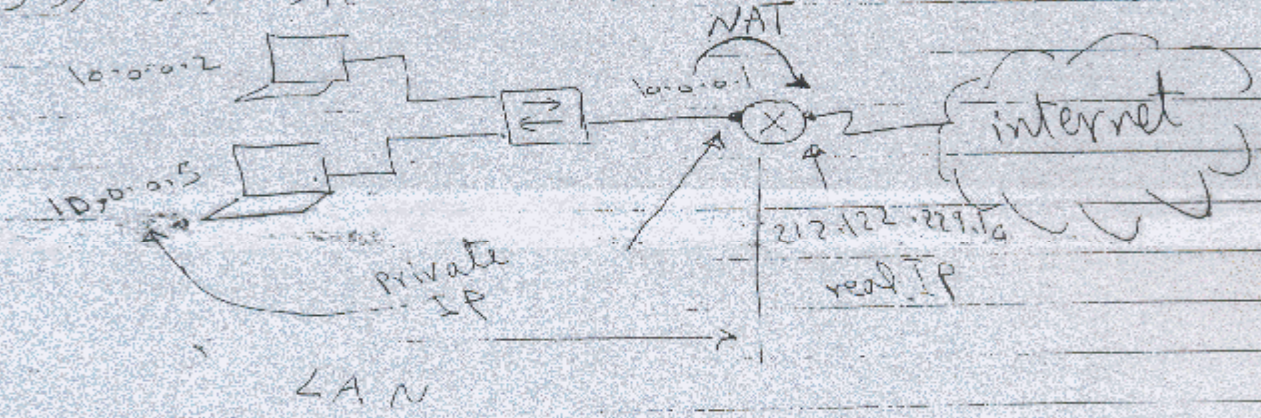
CLASS	First bit	address range	No. of bits in the network part
A	0	0 → 127  note: network starts with 0 or 127 don't use in addressing	8
B	10	128 → 191 	16
C	110	192 → 223 	24
D used for multi casting	1110	224 → 239	
E used for experimental purpose	1111	240 - 255	

- Private IP addressing : used in LAN That don't connected directly to internet

CLASS	Private IP range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

- real IP () private IP يتحول الى نفس على النت

الراوتر (NAT) software من خلال (NAT tech.) وهو عبارة عن



- real IP : directly connect to internet

private IP : not directly connected to internet

Catagories of IP address:

[1] network address : host part = 0 (network address)

ex The network address for 12.1.1.3 is 12.0.0.0
↑ class A

[2] Broad cast address: host part = 1

ex 10.255.255.255 is the Broad cast address of network 10.0.0.0

[3] host address :

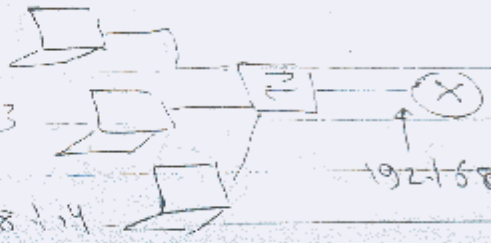
ex 192.168.1.1 → host add.
192.168.1.0 → network add.
192.168.1.255 → B-C-add.

Hint :
no. of valid hosts in each network $= 2^{\text{no. of host bits}} - 2$

in this example

class C

No. of valid hosts $= 2^8 - 2$



في هذه الشبكة فإن الـ IPs من 192.168.1.1 ← 192.168.1.4

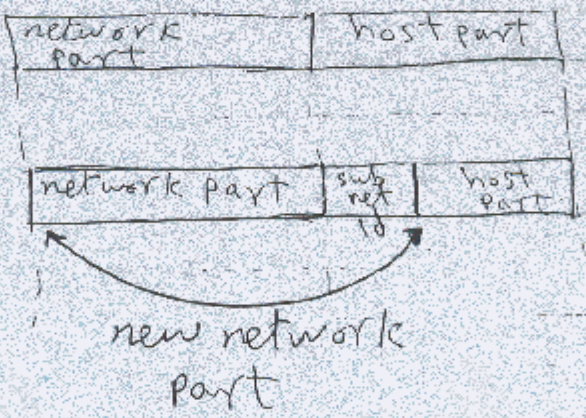
مستخدمة أعلاه IPs من 192.168.1.5 ← 192.168.1.255

غير مستخدمة وبالتالي أصبح لدينا IP's مهدورة

ولا يمكن استخدام هذه الـ IP's إلا بعمل subnetting

subnetting: divide major network in to smaller networks

* subnetting is done by taking part of hostbits and add it to the network part



* subnet Mask :

- 32 bits mask used to identify the network part and the host part
- subnet mask is consists of 1's following by continous 0's
- 1's determine the network part of the add
- 0's ——— host part in the address

- representation of subnet mask

1- dotted decimal ← 192.3.1.1

IP: 1100 0000 . 0000 0011 . 0000 0001 . 0000 0001

sm: 1111 1111 . 1111 1111 . 1111 1111 . 0000 0000

→ 255.255.255.0

default subnet mask for classes

A ⇒ 255.0.0.0

B ⇒ 255.255.0.0

C ⇒ 255.255.255.0

ex: network 192.168.1.0 contain 256 IP

we divide it to 4 subnets each contain 64 IP

sol

192.168.1.0 → class C & 4 subnets = $2^{2 \text{ bits}}$

∴ sm = 255.255.255.00000000

∴ new sm = 255.255.255.11000000

= 255.255.255.192

∴ Hop count = 256 − 192 = 64

∴ The subnets are

192.168.1.0 / 26

192.168.1.64 / 26

192.168.1.128 / 26

192.168.1.192 / 26

hint slash notation → sm تكتب التخمين عن

ex IP: 10.0.0.1
sm: 255.0.0.0 → 10.0.0.1/8 ← عدد الواحدات في sm

ex: 192.168.1.0
sm = 255.255.255.192 → 192.168.1.0/26

Ex Find the subnet that the following IP lie on it

IP → 192.168.1.65

SM : 255.255.255.192

sol

This IP class C

∴ HopCount = 256 − 192 = 64

∴ The subnets are

192.168.1.0 → network

192.168.1.64 → network
192.168.1.65

192.168.1.128 → network

192.168.1.192 → network

∴ 192.168.1.65 lie in the network 192.168.1.64

ex Find no. of subnet bits, no. of subnets & no. of hosts in each subnet

1. IP: 10.0.0.1
   SM: 255.0.0.0
   sol
   no of subnet bits = 0
   no of subnets = 0
   no. of hosts / subnet = $2^{24} - 2$

2. IP: 10.1.1.2
   SM: 255.255.255.0
   sol
   no of subnet bits = 16
   no. of subnets = 2^{16}
   no. of hosts / subnet = $2^8 - 2$

ex: identify if this IP is host IP or subnet IP Broadcast IP
172.16.5.0 / 23
sol
class B & SM = 255.255.1111 1110.0
254
∴ SM = 255.255.254.0
∴ Hop count = 256 − 254 = 2

∴ 1st subnet → 172.16.0.0/23

2nd subnet → 172.16.2.0/23

3rd subnet → 172.16.4.0/23

172.16.5.0/23

172.16.5.255/23

ith subnet → 172.16.6.0/23

network address

host

B.C address

∴ 172.16.5.0/23 is host addressing

ex: divide network 192.168.1.0/24 to as much as possible subnets where each subnet contain 7 hosts

so

7 hosts + 2 = 9

(2: network address + B.C add.)

$9 = 2^4$

∴ no. of host bits = 4

∴ no. of subnet bits = 8 − 4 = 4

∴ no. of possible subnets = 2^4 = 16 subnet

192.168.1.0000|0000

network part

∴ S.M = 255.255.255.240

∴ Hop count = 256 − 240 = 16

∴ 1st subnet 192.168.1.0/28

2nd subnet 192.168.1.16/28

Problems for studient

[1] is This IP 192.168.24.59/30 a Broad Cast address or host

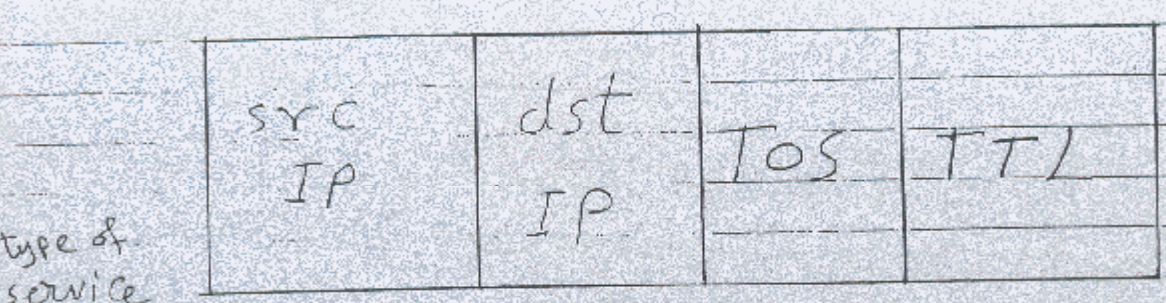
[2] is This IP 172.31.128.255/18 a Broadcast address or host

[3] The B.C address of 172.16.64.0/20 is ----------

[4] The B.C address of 192.168.82.90/28 is ----------

very important hint

* IP Packet



type of service

TOS: تحدد الأولوية priority أعرب له مثال بسيط تفهم

لو عندك packet بتاعة video لو وصلت لـ dst متأخرة جدًا

حيث تقطيع في عرض الـ video لذلك تم وضع Tos field

علشان يكون عندك ترتيب الأولويات.

TTL: (time to live)

لو بعت رسالة من pc لـ pc وكانت هذا الـ packet تاهت في network لذلك تم وضع field

هذا الـ TTL ويتم وضع فيه رقم ما ولنقل 18 وكل روتر تمر عليه

هذا الـ packet يتم طرح 1 - فلو مرت على 3 Routers لكي data

فإن الـ TTL التي تصل للـ pc تكون 18-3=15

التعرف على ذلك نعمل الـ ping بالهوست المراد معرفة الـ TTL

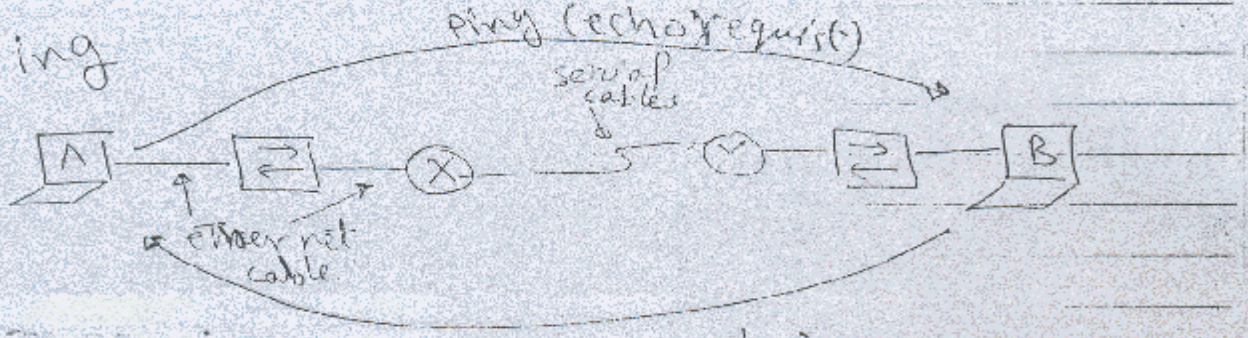
ping -t www.yahoo.com

DAY 4

CCNA Track
Prepared By
ENG: Ahmed Abdallah

ICMP: internet control message protocol
- Provide message to describe network action

ex: ping



* types of messages:

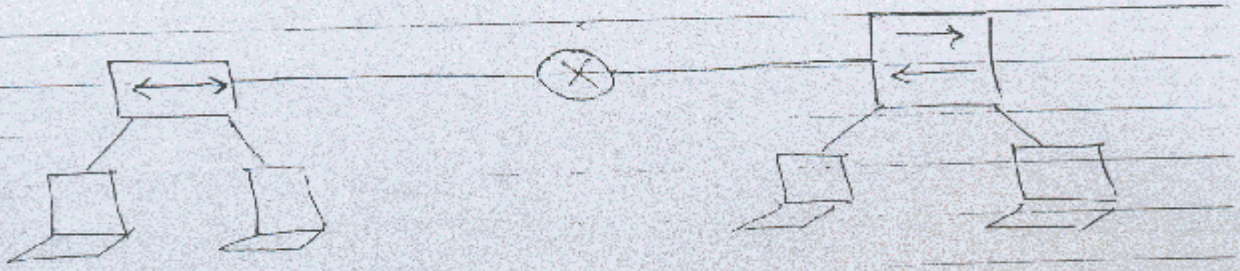
- echo requist , echo reply
- network unreachable
- host unreachable
- TTL expired
- source quench message (SQM)

لو A بعت لـ B وفي router على الطريق بعت SQM لـ A عشان يبطئ لان router مش قادر

layer 3 device : [Router]

- find the best path for the packet
- Router ports are multiple Broad cast domain & multiple collision domain

ex: find No. of Broad cast domains & no. of collision domains?



sol

no of BC domains = 2

no of collision domains = 4

* Needed parameters to send from one host to another:

src MAC	dst MAC	src IP	dst IP	data

note → each router interface has an IP address and MAC address to be used in transmission

[1] source MAC: burned on The NIC

[2] source IP:

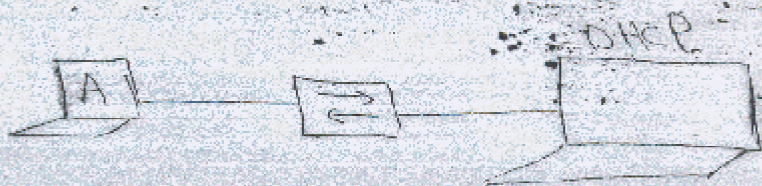
a- static : given by The administration

b- dynamic : → RARP (reverse address resolution protocol)
→ Boot P
→ DHCP

في حالة dynamic لو عندي 1000 جهاز وعاوز أدي لكل واحد فيهم

IP هل أدخل لكل جهاز الـ IP بنفسي "الموضوع مرهق جدا"

الحل: أضع DHCP server (جهاز كمبيوتر موضوع عليه DHCP application)



MAC	IP
A	10.0.0.7

DHCP discovery message:
- my MAC is A
- what is my IP?
- your IP is 10.0.0.7
- and your gateway is ___ & your sm is ___

RARP و BootP كانوا مستخدمين قديما وكانوا بيعطوا

للجهاز الذي يريد IP كانوا بيعطوه الـ IP فقط ولكن DHCP

بيعطي IP و gateway و subnet mask

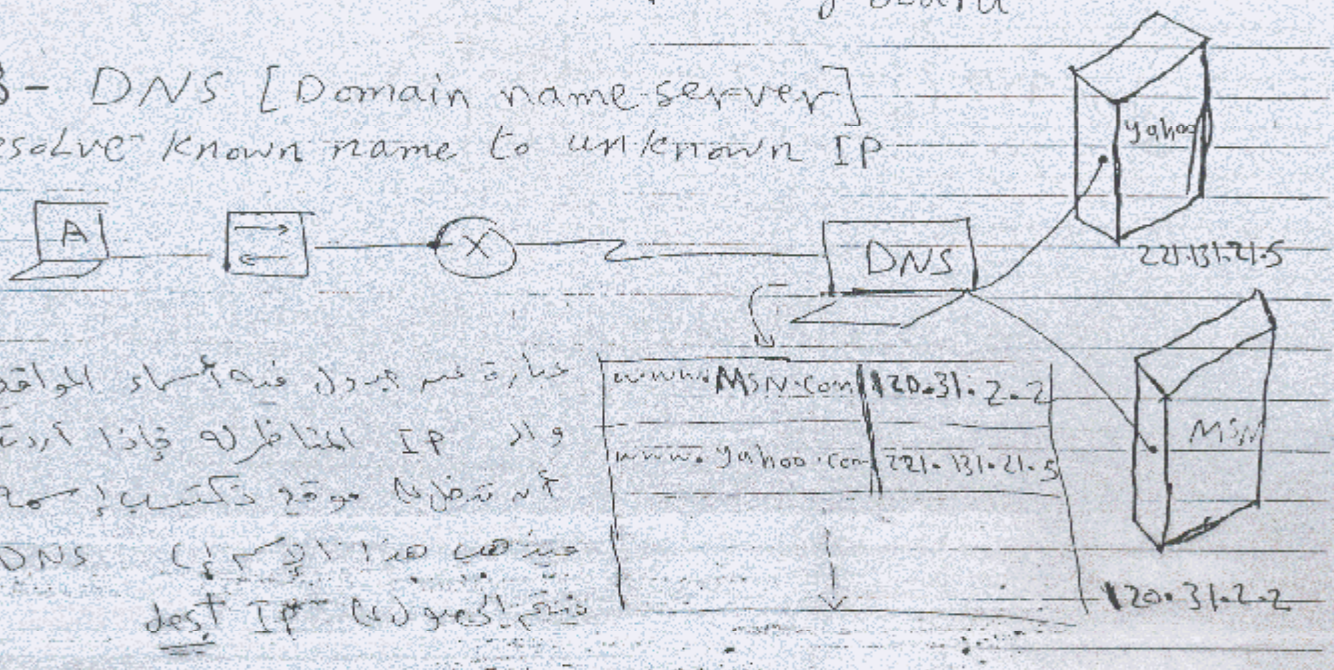
3 destination IP :

a- \\10.0.0.5

↑ double back slash from key board

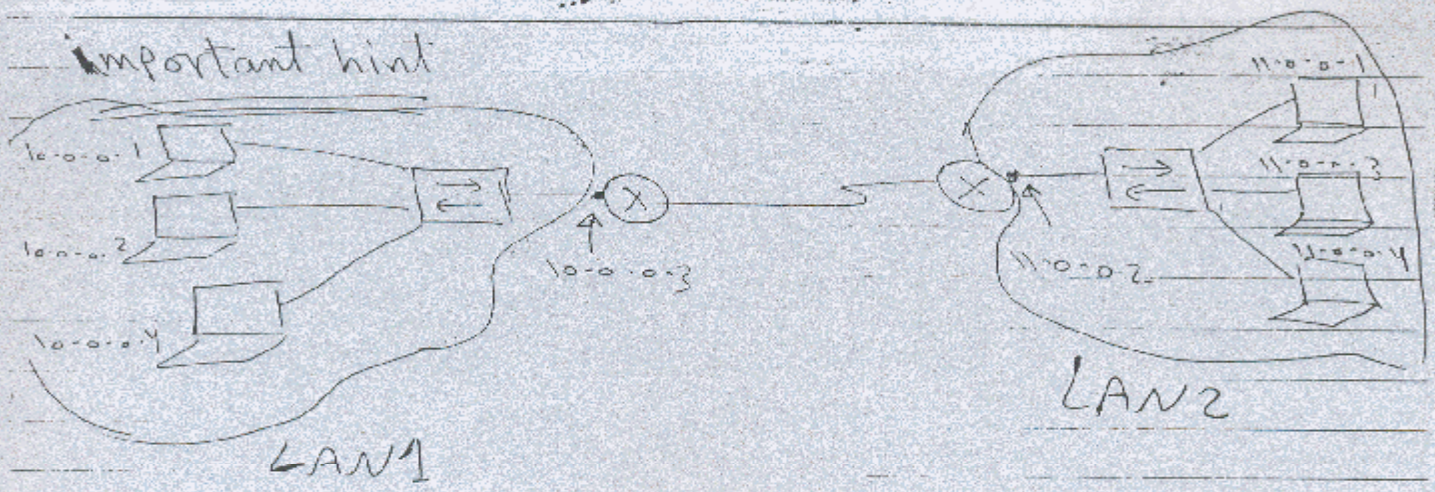
B- DNS [Domain name server]

Resolve known name to unknown IP



عبارة عن جدول فيه أسماء المواقع
و الـ IP الخاصة فيها فإذا أردت
أن تدخل موقع ذكتب له
DNS يبحث في هذا الجدول عن
الـ dest IP الذي كتبته

Important hint



→ The default gate way of LAN 1 is 10.0.0.3

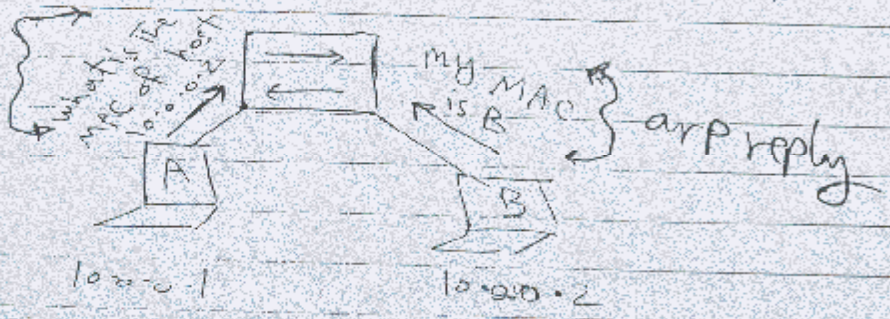
→ ——— ——— ——— ——— ——— LAN 2 is 11.0.0.2

→ default gateway: العنوان الـ router الموجود على الـ LAN و الذي يتبع له الـ IP

to get destination MAC :

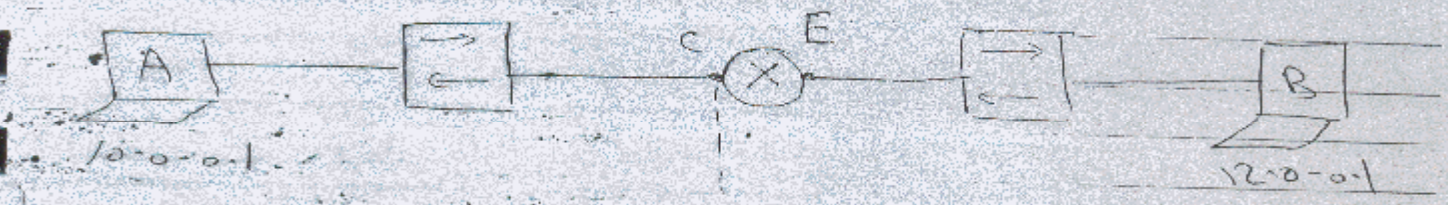
1- if the dst host inside your LAN

use ARP [address resolution protocol]



2- if the dst host out side the LAN

use proxy ARP



what is the MAC of the host 12.0.0.1

send your frame to MAC C

what is the MAC of host 12.0.0.1

my MAC is B

take the frame

Transport layer:

Functions:

1- segmentation → divide data to small segments

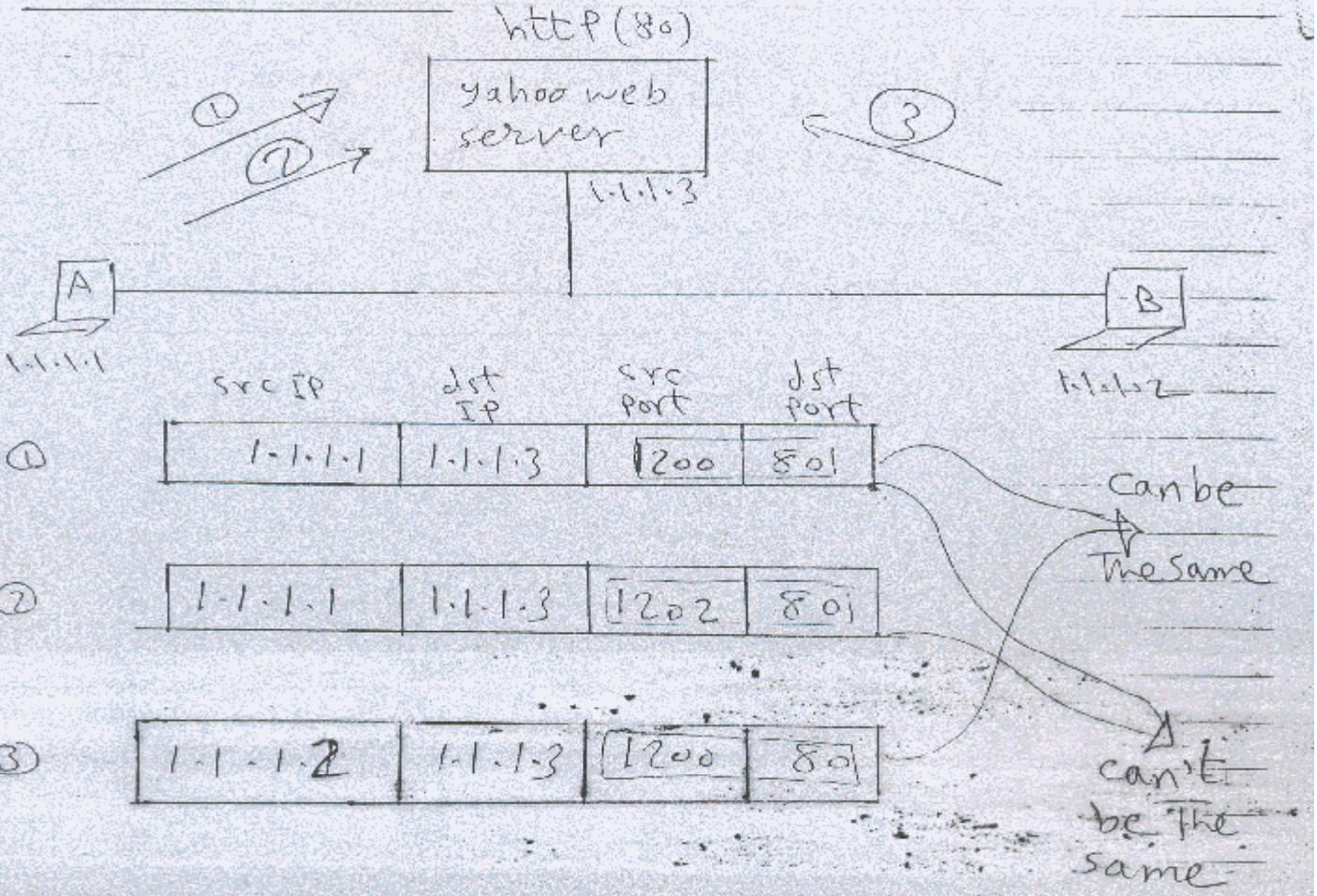
2- addressing depends on Port No.: each application is assigned a unique Port No.

Types of Port number:

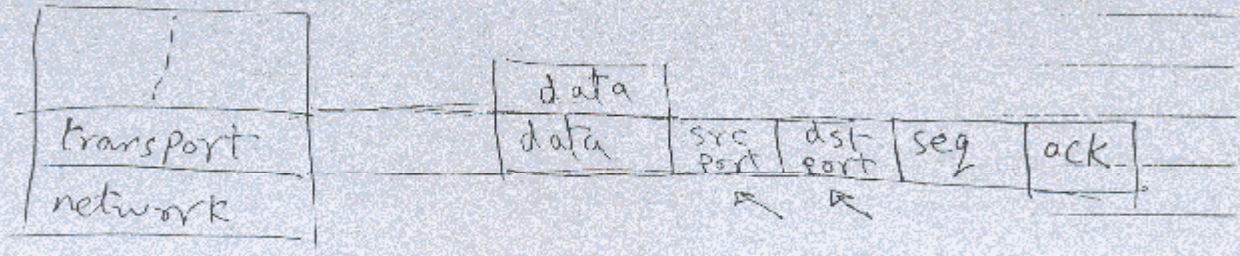
① well known ports (0-1023)
reserved for application
Ex: FTP (20,21) & telnet (23) & HTTP (80)
SMTP (25), DNS (53)

② user defined Ports (1024-65535)
→ randomly given by the O.S for the local application source port

3- multiplexing :



Packets ~~ Collision ~~ ~~ Port No. ~~

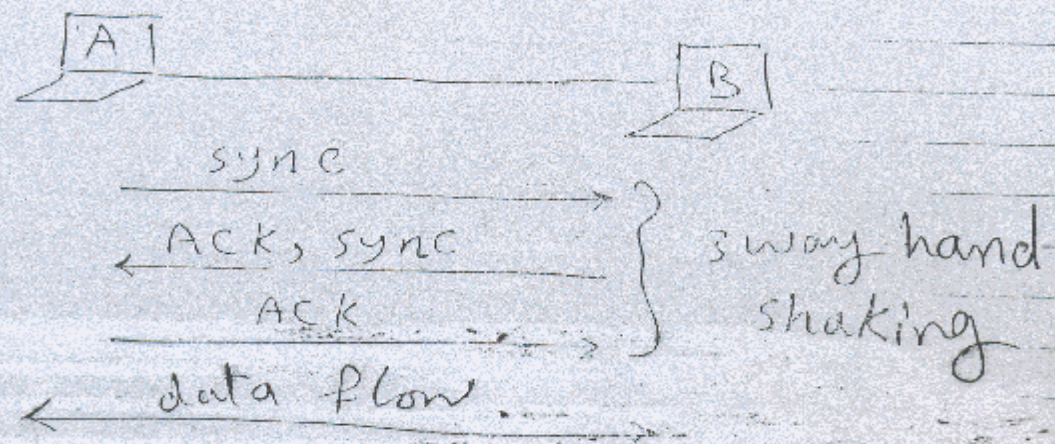


[4] Reliable service & unreliable service

TCP: connection oriented, reliable

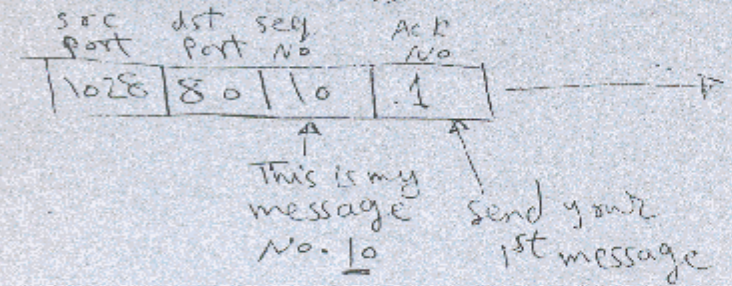
UDP: connection less, unreliable

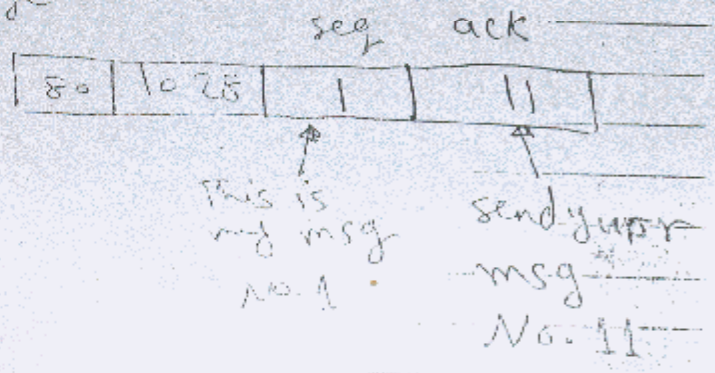
[5] establishment The connection:



[6] Management of connection:

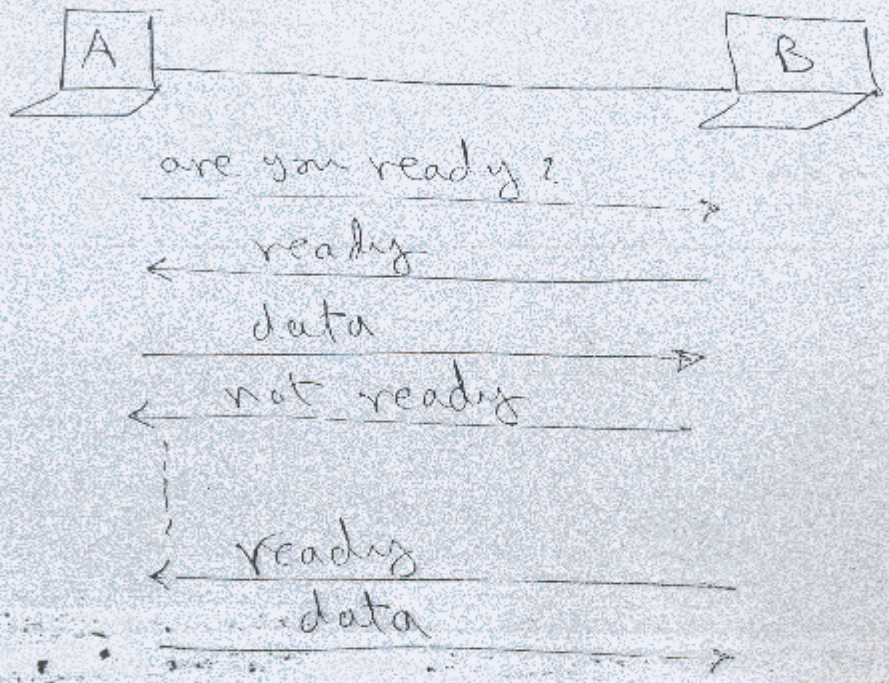
a- sequencing: each segment has a sequence





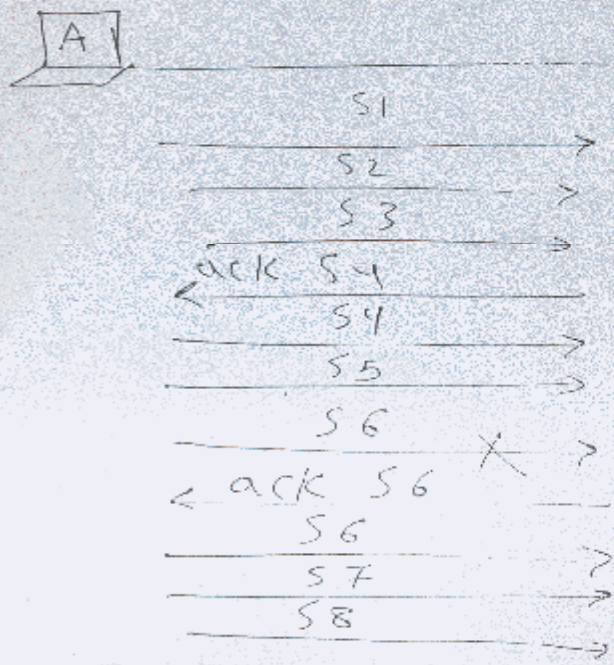
b - Flow control :

① - congestion avoidance [ready / not ready]



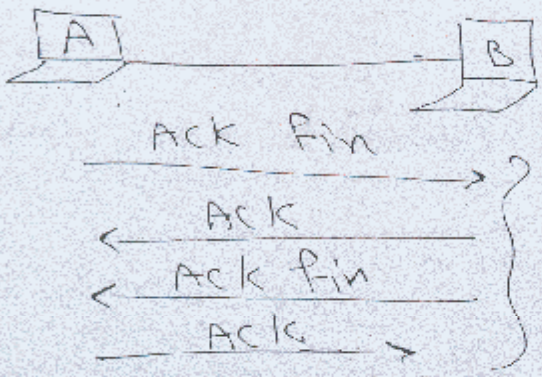
② windowing (PAR) : positive Ack retransmission

- Provide reliability, flow control
- windowsize : The amount of sent data before Ack



يقوم بإرسال A يقوم بإرسال
البيانات يتفقد B
ويقول لا ، لست فقط ، تعال
ثم يقول Segment
B بالأمر ، يستقبل ، ثم يرد الواجبة
Segment يتم الإرسال من
على هذا الأساس B و A

7-closing The connection :



applications That use TCP protocol	applications That use UDP protocol
FTP	TFTP
HTTP	DHCP
SMTP	SNTP
POP3	BOOTP
telnet	

DAY 5 & 6

CCNA Track
Prepared by
ENG: Ahmed Abdallah

Cisco Products IOS For Routers, switches:

* Cabling & device connectivity using UTP ethernet cable

DTE	DCE
PC router	hub switch modem

* straight cable from DTE to DCE
* cross cable from DTE to DTE or from DCE to DCE
* rollover cable (consol cable): connected in consol port to configure the router

* Router IOS (internet operating system):
it is the operating system that installed on router
* configuration file: a program file that contain a set of commands ordering the router to perform processes [configured and saved on router]

* CLI (command line interface): The user interface that accept configuration

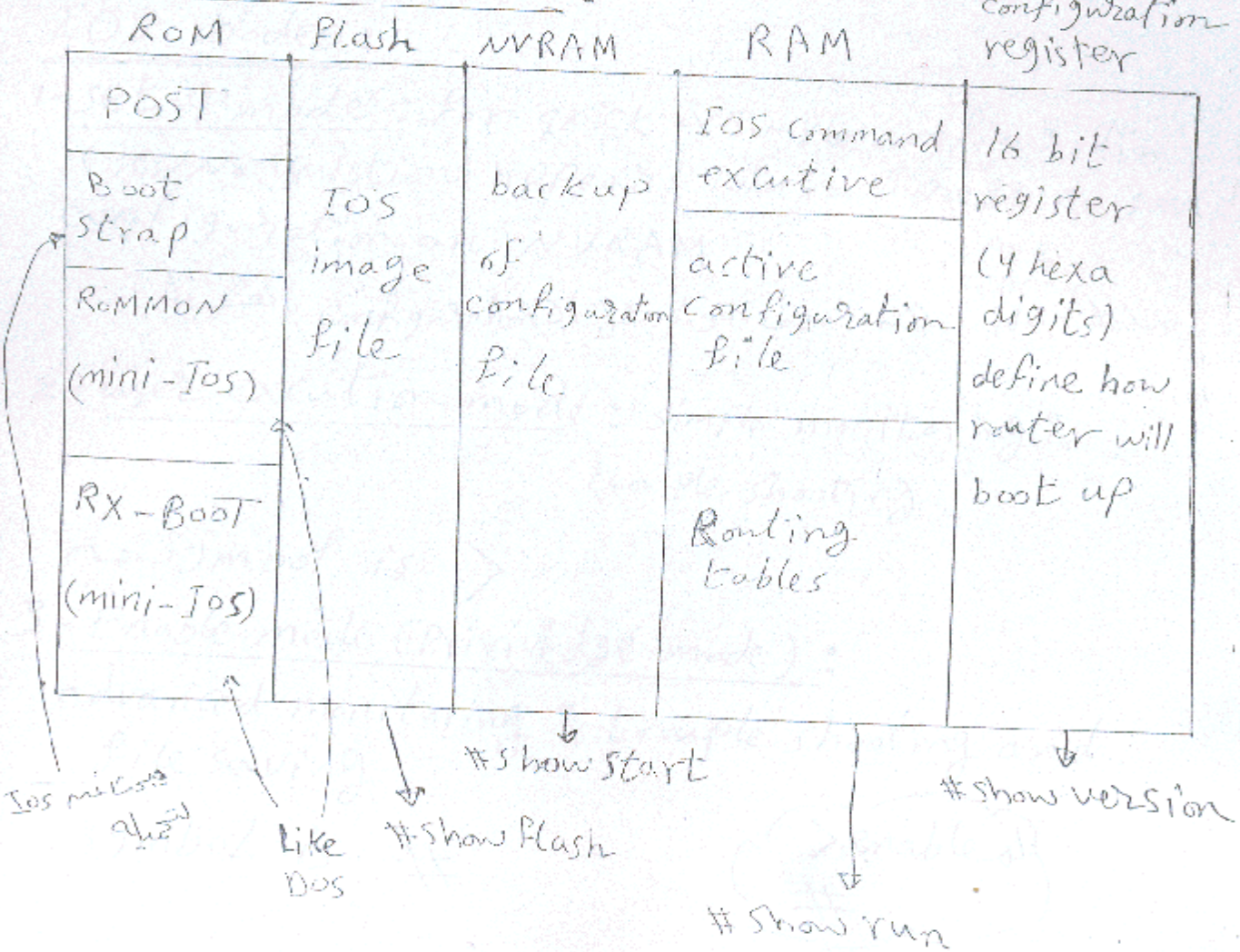
* device start up:

1- POST (Power on self test)
   ↳ check on hard ware

2- Load IOS

3- Load configuration file

* Router components:



* The default value of configuration register

0X2102

↳ boot from flash

0X2100

↳ boot from ROMMON

0X2101

↳ boot from RX boot

0X2142

↳ by pass NVRAM

IOS modes:

1- setup mode: for quick & simple configuration (yes/No qustion appears when there is no saved configuration on NVRAM

لإنشاء configuration أول مرة لما يكون No بعمل

2- user exution mode: simple monitoring & trouple shooting

↳ symbol is >

3- Enable mode (Priviledge mode):

advanced monitoring & trouple shooting and file saving

symbol is #

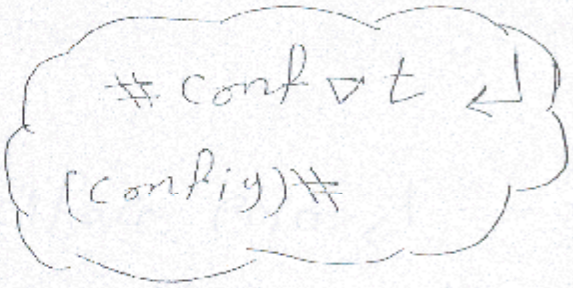
> enable
#

4- Global configuration mode:

define configuration globally on the router
(affect the configuration file)

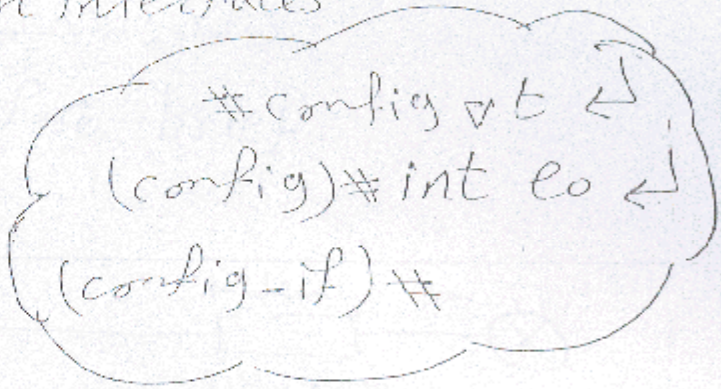
Router يدخل فيه من هذا mode اذا شاف ال

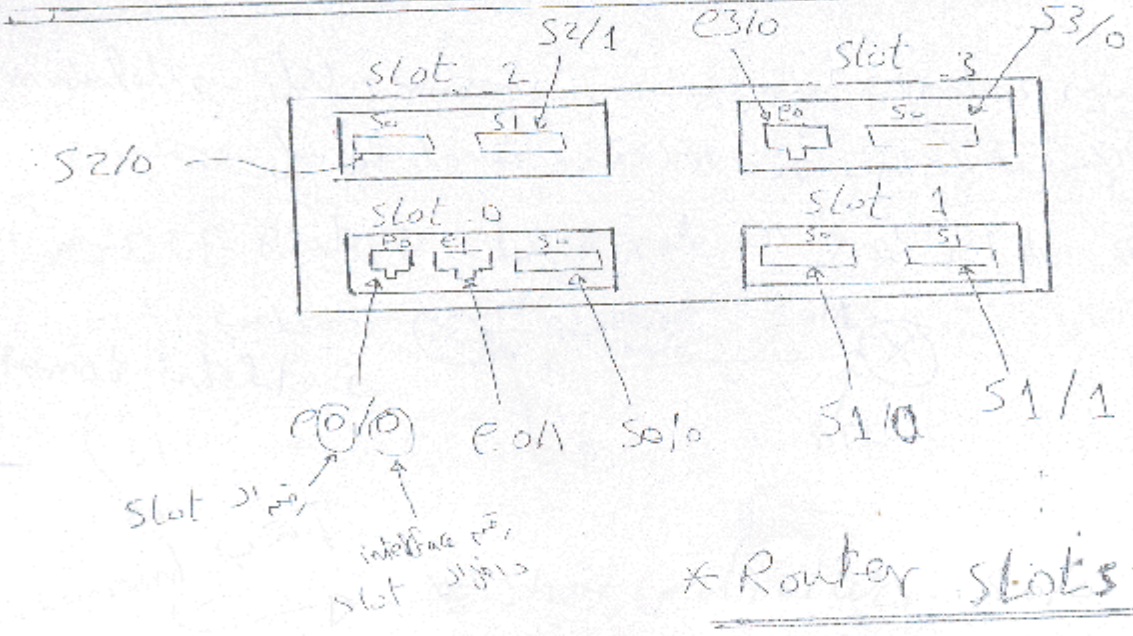
symbol => (config)#



5- sub configuration mode: This is the mode that affect on interfaces

(conf-if)#





* Router slots & interfaces

Router simple commands:

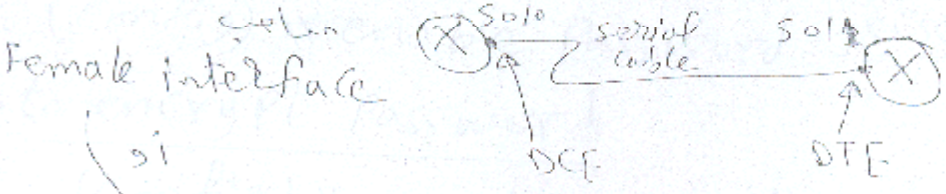
IP = 10.0.0.1
SM = 255.0.0.0

لازم أدخل على الـ int e0/0 عشان أعمل له

router > enable ↵
router # config t
router (config) # interface e0/0 ↵
router (config-if) # no shut down ↵
router (config-if) # IP address 10.0.0.1 255.0.0.0
لازم أكون في الـ enable mode عشان أقدر أعمل
show IP interface brief

modulation بعمل 2 modems عشان أحول الـ 2 routers من
2 routers digital إلى analog عشان يقدروا يتواصلوا.
وكمان تم الاستغناء عن هذه الطريقة.

لازم DCE Router أعمل clock rate على الـ serial cable



command أكتب
show controllers s0/0

clock rate لازم أعرف

(config) # interface s0/0
(config-if) # clock rate 56000

interface BW لازم أعرف أد إيه أقصى

bandwidth

(config-if) # bandwidth 64

64 Kbps

Trouble shooting

show run ⟵ لازم أعرف كل الأوامر اللي مكتوبة

(RAM الموجودة في)

show Flash ⟵ to see IOS file name

show start ⟵ to see configuration file which saved in NVRAM

reload ⟵ to make restart to router

- set password on enable mode

(config) # enable password cisco

- to encrypt password

(config) # enable secret

- to erase password

(config) # no enable password

- set password on consol:

(config) # line consol 0
(config-line) # password cisco
line) # Login

- telnet password

(config) # line vty 0 4 ← سمح بدخول 5 أشخاص
(config-line) # password cisco
(config-line) # Login

- to encrypt all passwords

(config) # service password encryption

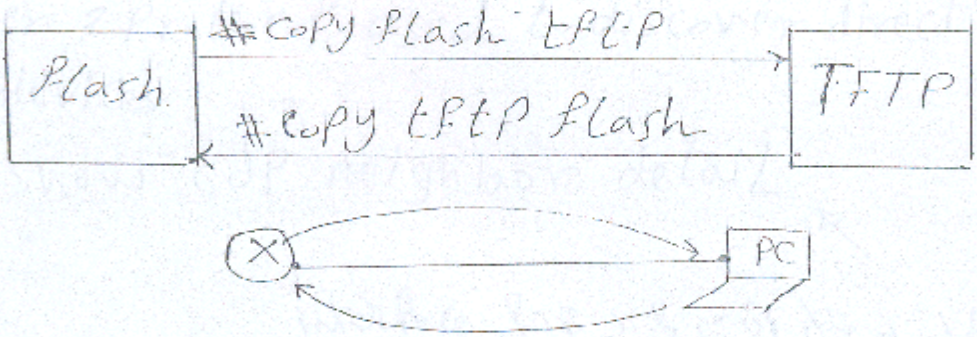
- message of The Day

(config) # banner motd hello

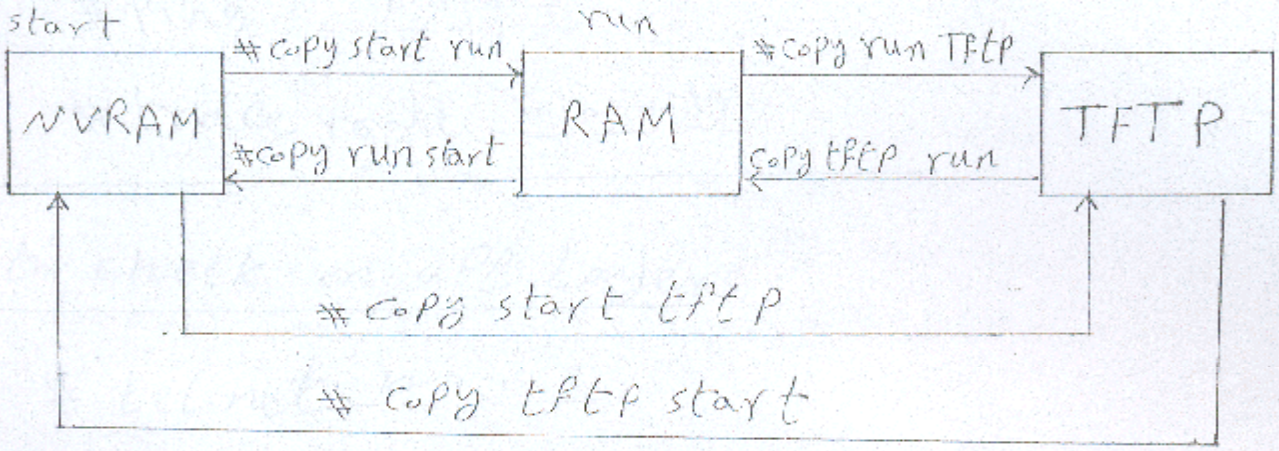
- to change Router name

router (config) # host name scc
scc (config) #

- to save IOS file



- to save configuration file



- to save # copy run start

to erase # erase NVRAM

erase Flash

- CDP : cisco discovery protocol

layer 2 protocol used to discover direct connected devices

#show cdp neighbor detail

للحصول على بيانات الموجه المجاورة مثل الـ IP & الـ interface

- to check on layer 3 :

#ping 10.0.0.7

#traceroute 10.0.0.19

- to check on all layers

#telnet 10.0.0.2

interface state :

#show IP interface brief

	interface	line protocol
1	administratively down	down

(config-if)# no shutdown

2	down	down

→ interface or cable failure (No keep alives)
→ mis match speed & duplex → half duplex / full duplex

3	up	down

→ different encapsulation type (PPP, HDLC, FR, --)
→ there is no clock rate is assigned to DCE (female interface)

4	up	up

→ in this case Port is up & work with out any problems

• password recovery

يقوم بها في حال وضع pw على الروتر

enable pw
pw on consol
pw on telnet

ماذا تعني كلمة تدخل هنا اذا pw وضعت على configuration للروتر ؟ اسهل يتعطل الـ router من زر التشغيل

١- ضغط ctrl + break ومنها نعرف أن الروتر قد فتح على

RoMMon 1 > config 0x2142 ← configuration file لـ bypass لعمل

RoMMon 2 > reset ← to make restart

والآن تم وضع الـ pw على

٣- بعد ذلك يقوم الروتر بعمل restart ويفتح على (user exution) mode

٤- ادخال CLI وبالتالي يمكن أن نرى الـ pw

show start

← إذا حاولت فتح الـ pw كانت encrypied لا يمكن أن نرى أو تعامل معها بأي شيء

(A) # copy start run

↓ pw وبعد كتابة غير الـ

(config) # enable pw - aa

(B) # erase NVRAM ← حذف الـ configuration file

(config) # config-register 0x2102

copy run start

٥- لاننسى أن نفتح الأمر restart حتى لا تعمل config.file في حال تم

Router Configuration (router commands) لأوامر

[1] Router Boot up from Config. register

0x2102 → Boot from Flash

0x2100 → Boot from ROMMON

0x2101 → " " RxBoot

0x2142 → by pass NVRAN

[2] > enable ↵ enable mode (الدخول)

#

config t ↵ (config) (الدخول) (config mode)

(config) # int e0/0 int (الدخول)

(config-if) #

router(config) # hostname R1 لتغيير اسم الروتر

~~router(config)#~~

show IP interface brief لرؤية كل الـ interfaces و الـ IP الروتر

الدخول الروتر ووضع IP على كل interface

1- (config-if) # no shutdown

2- (config-if) # IP address 10.0.0.1 255.0.0.0

بالنسبة لـ serial interface نفعل الكونفيج بالطريقتين لكن لازم نحط clock rate على الـ DCE router ["DCE router" على الصورة]

(config)# int s0/0
-if)# IP add 10.0.0.1 255.0.0.0
-if)# no shutdown
-if)# clock rate 64000

serial int لازم نحط band width وهي أيضاً

(config-if)# bandwidth 64

#show run ---> لنرى كل الأوامر الموجودة في RAM (لا يتم تخزينها)

show start ---> لنرى الـ config.file المخزنة في NVRAM

show flash ---> لنرى نسخة IOS واسم وإصدار الـ version

reload ---> restart لإعادة

copy run start ---> config. لـ save لإعادة

erase NVRAM: ---> لمسح الـ config.file المخزنة في NVRAM

erase flash ---> لمسح الـ IOS

---

① *(config)# enable password cisco ---> لإعطاء كلمة سر لـ enable mode

③ (config)# enable secret cisco

* لتشفير كلمة السر هكذا لو حاولنا عمل #sh run تظهر مشفرة

② (config)# service password encryption

لتشفير كل كلمات السر الموجودة بالراوتر

① + ② = ③

- set password on consol cable

(config)# line consol 0
-line)# password ... cisco
-line)# login

- set password on telnet

(config)# line vty 0 - 4
-line)# password - cisco
-line)# login

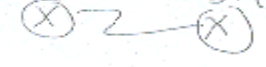
#(config)# banner motd - hellow Ahmed
هي إذا حاولت الروتر ودخلت عليه يظهرلك هذه الرسالة

#show CDP neighbor detail
لمعرفة معلومات الروتر المجاور للروتر بتاعك يظهرلك
1- إسم الروتر المجاور
2- ip للروتر المجاور

#Ping - 10.0.0.1
trace route - 10.0.0.1
ping لكل
بتقدر تعرف المسافة بينك وبين
10.0.0.1 = IP الجهاز صاحب ال router
# telnet 10.0.0.1 ← لعمل إختراق للروتر من مكان بعيد

---

show controllers



DCE و DTE لمعرفة نوع كابل الروتر.
DCE لمعرفة نوع الروتر وتضع clock rate لو نسيتم

DAY 7

CCNA Track:
Prepared by
ENG: Ahmed Abdallah

Routing

- layer 3 PDUs

- best path determination
- done by routing protocols using routing table

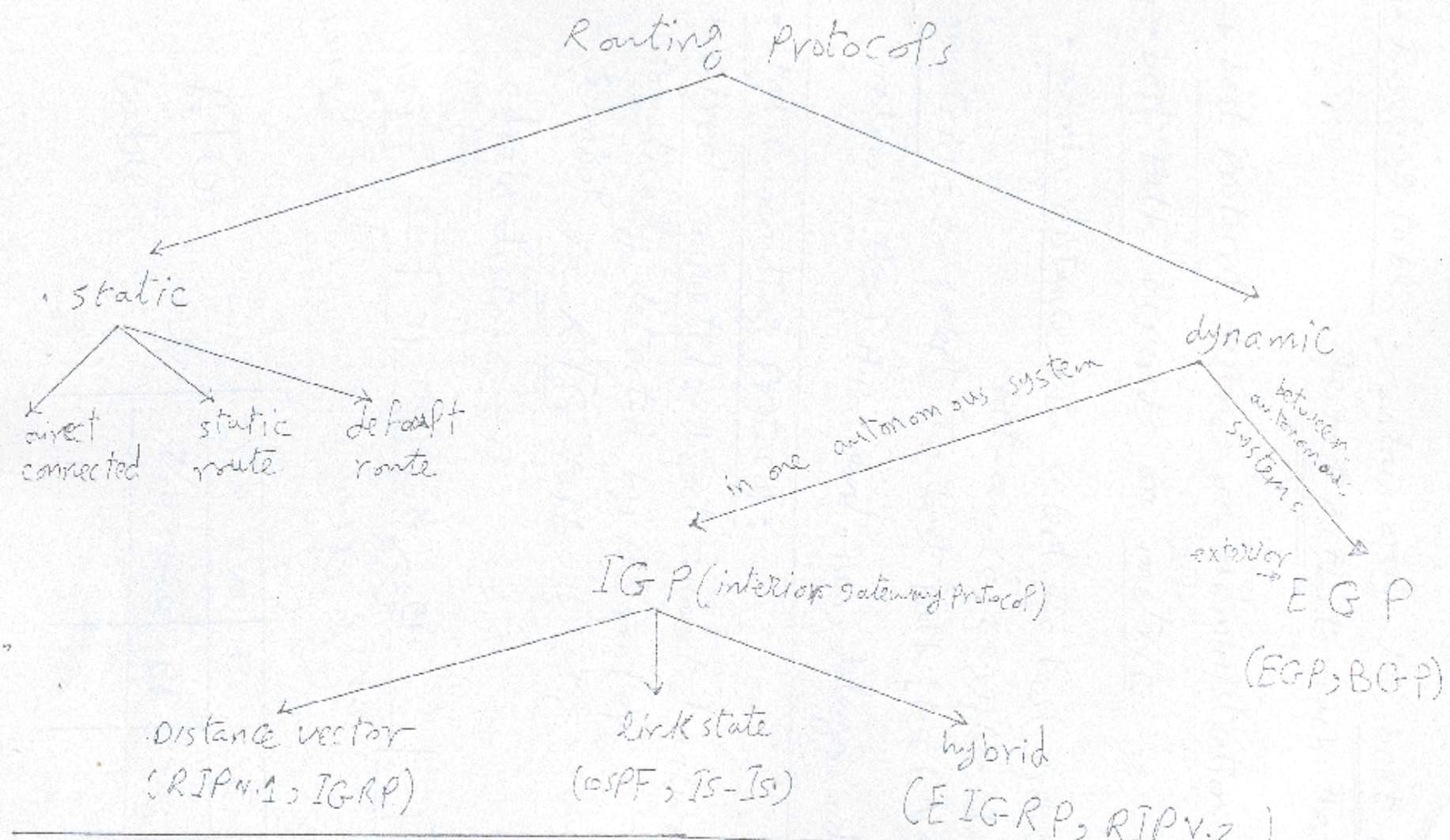
Routing Protocols VS Routed Protocols

Routing Protocols: Data لل routing هي بروتوكولات تقوم بعمل (Routing table) وهي اللي بتكون عندها

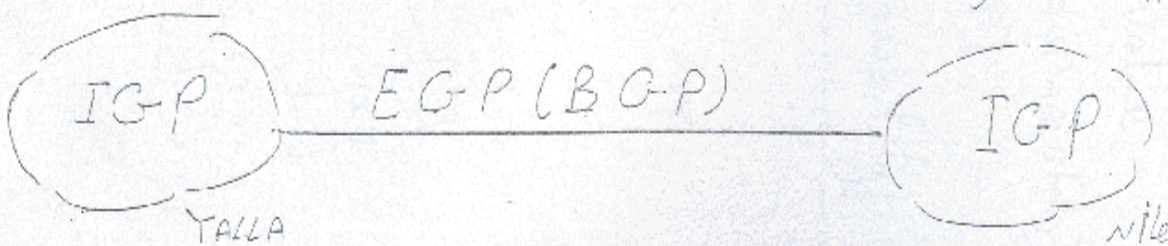
ex RIP, OSPF, IGRP, EIGRP

Routed Protocols: هي اللي بتتحرك على IP packet وهي اللي routing protocols بتعمل لها routing

ex IP, IPX, APPLE TALK



AS : autonomous system : ar. area that work under single administration & policy



58

- Routing table : contain only the best protocol and the best path to reach the dst N.W.

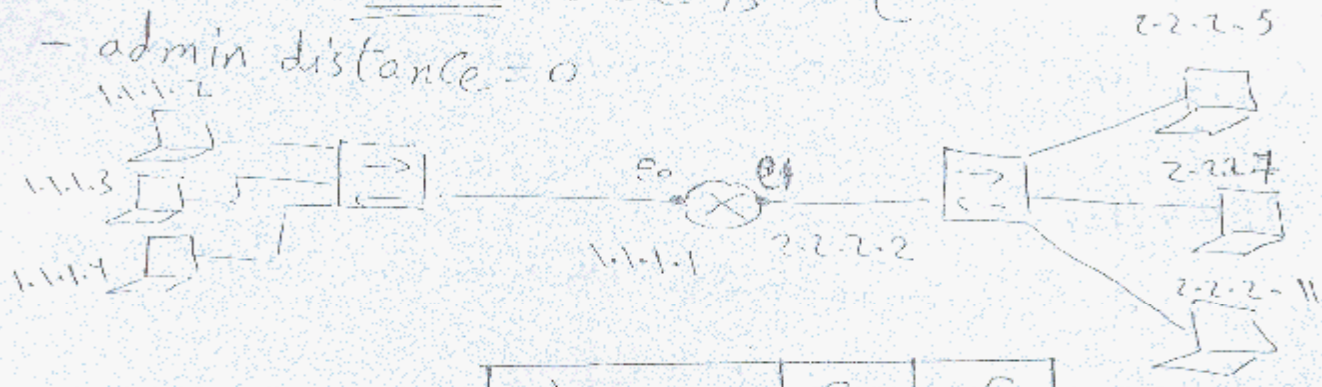
→ best protocol depends on administration distance

→ best path depends on metric

- admin. distance : to select the best protocol value between (0-255) [less admin distance is better]
- metric : to select the best path [less is better]
  metris is like [Hop count, BW, delay, Load, reliability]

- static routing protocol :

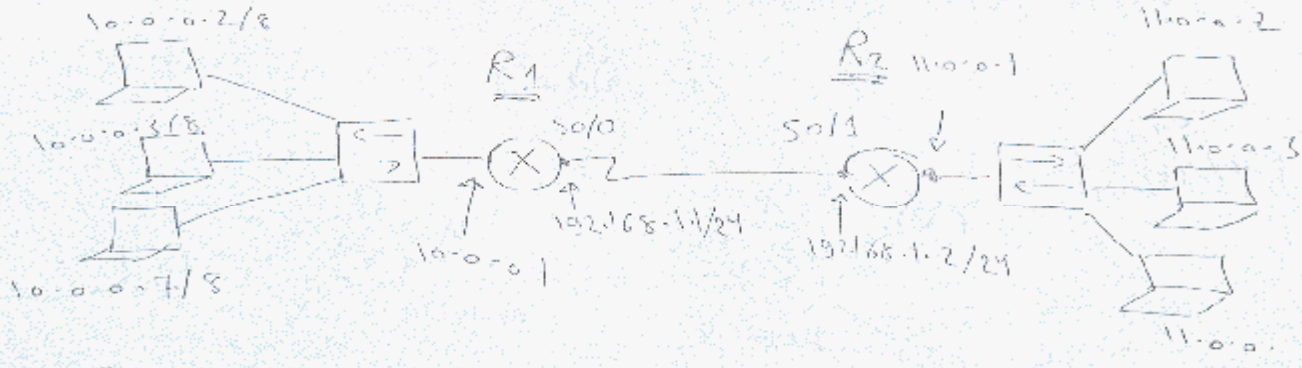
1- Direct connected :- direct connected networks are automatically detected by the router
- Symbol in RTG table is "C"
- admin distance = 0



RTG table

1.0.0.0	e0	C
2.0.0.0	f0	C

- **static route**: manually you can define a path to reach a certain destination



R1 → can see network 10.0.0.0/8 & network 192.168.1.0/24
but it can't see network 11.0.0.0/8

network 11.0.0.0 إلى الوصول لـ R1 لـ (static route) عمل

R1(config)# IP route 11.0.0.0 255.0.0.0 S0/0
IP sm out interface

interface S0/0 من خروج sm = 255.0.0.0 (N) network 11.0.0.0 لـ ① توصل لـ

عكس اتجاه الأمر حتى يتم الخروج

R1(config)# IP route 11.0.0.0 255.0.0.0 192.168.1.2

next Hop IP

لـ interface لـ من خروج network 11.0.0.0 لـ ② توصل لـ

IP: 192.168.1.2 لـ Router

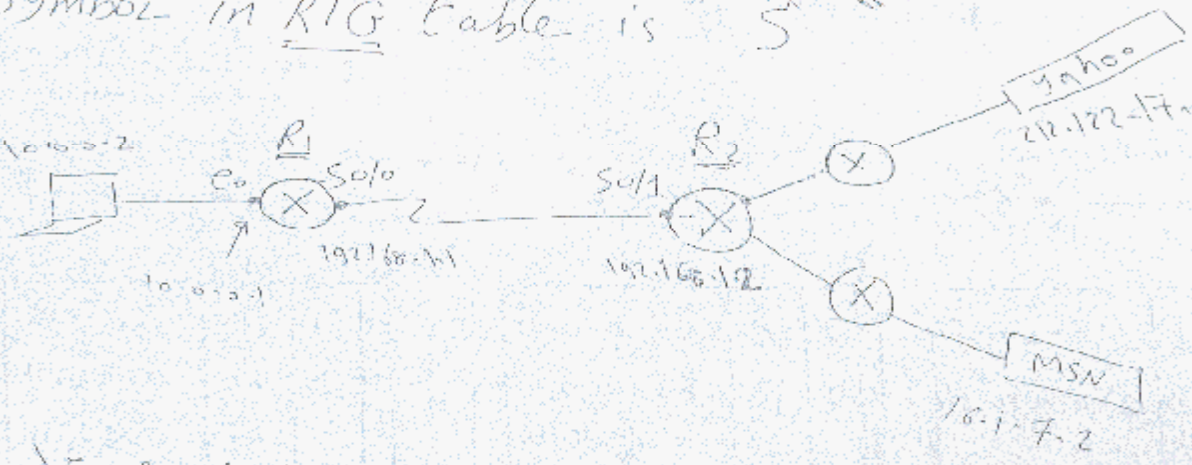
ملحوظة: R2 على networks 11.0.0.0 و 192.168.1.0

network 10.0.0.0 على R2 حتى يصل لـ

؟؟؟

- **default route :**

- define Path that used by packet when There is no path to dst in RTG table [gateway of last resort]
- symbol in RTG table is " S* "



لـ تمرير الوصول لأي شبكة أخرى (static route) يدوياً
والتطلب على من الشبكة تشير
(default route) routing لهذا الـ

R1(config)# IP route 0.0.0.0 0.0.0.0 192.168.1.2
or
S0/0

(0.0.0.0 0.0.0.0) يعني أي شبكة أردت أن تصل لها
IP=192.168.1.2 للـ int الخاص
أو int S0/0 من

RTG table of R1 →

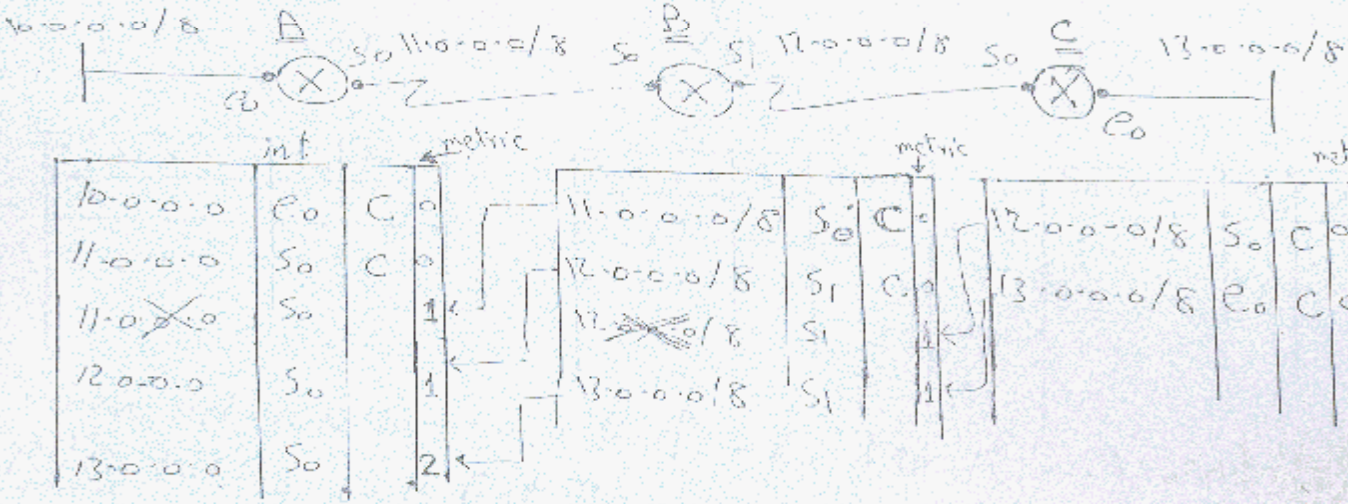
10.0.0.0	Eo	C
192.168.1.0	S0/0	C
0.0.0.0	S0/0	S*

Dynamic Routing Protocols

IGP: interior gate way Protocol

1- distance vector Routing Protocol

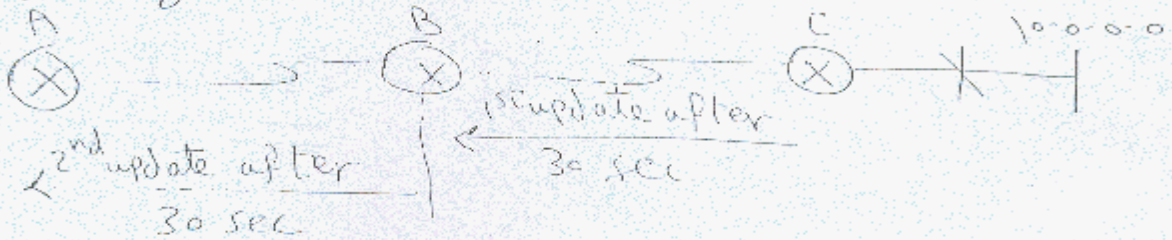
2- operation:



- At first: each router detect its direct connected networks and form the initial routing table, after that every router send its RIG table to all routers to form the final RTG table (convergence)

- after convergence: periodic updates are sent to indicate any change in the N.w

- at change: (network failure) the change will appear after sending the periodic update



60sec ay network failure (network 10.0.0.0) ayn Router A =

- Problems of distance vector:

- slow convergence.
- routing loops ← هاذيه نقوم بعمل له routing loops

C	10.0.0.0	e0	down

	10.0.0.0	S0	down
	12.0.0.0	S1	3

	10.0.0.0	S0	2

- when network 10.0.0.0 fails - Router A will send its RTG tables to B (at the periodic update)
- before B send its Periodic update to C. Router C send its Routing table to B with a path to network 10.0.0.0 So, B think that 10.0.0.0 can be reached Through C while C depends on B for that (Loop)

اذا network 10.0.0.0 ← C راسل B عن طريق

(network 10.0.0.0) ← B راسل C عن طريق

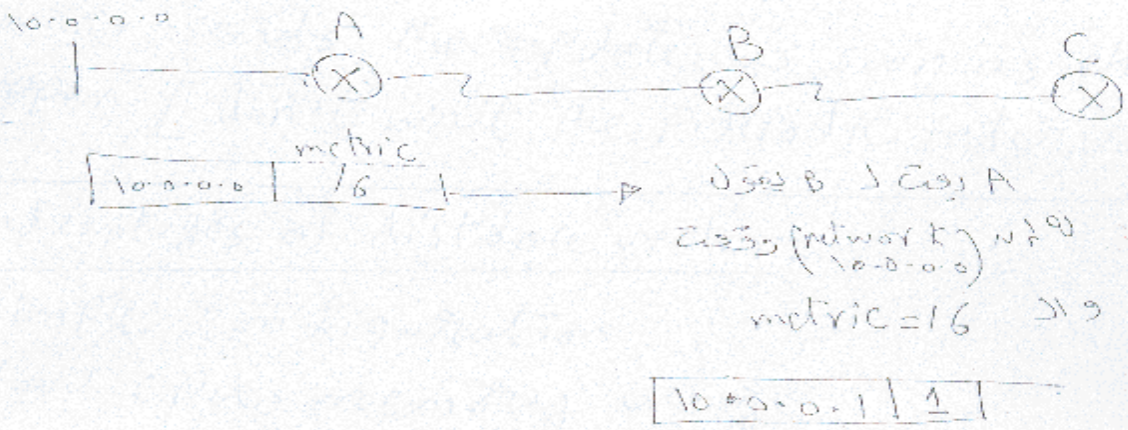
Routing Loops ← هذه المشكلة

• solution for the Routing loops

1- TTL in The packet :

TTL in The packet = 16

2- Poison route , Poison reverse :



A يقول لـ B

network (10.0.0.0) وصلت

metric = 16 و الـ

10.0.0.1 | 1

B بالتالي بدخل network 10.0.0.0 بجدول الـ routing و يعتبر انو صار عندو 1 Hop و بالتالي الكلفة الجديدة

الآن وصلت و B جاهز و جاهز يبعت لـ C بس periodic update يجي و يبعت لـ C بحيث metric = 1 في حال

A (أو أي جهاز) يقول لـ B بأنو عندو وصلة و B يعتبر هي أفضل / أو أنها كاذبة

3- split horizon :

Router learned from interface can't be sent back on the same interface

يعني الراوتر الي تعلم من interface معين لا يمكن أنه يبعت هي المعلومات على نفس الـ interface

4- hold down timer:

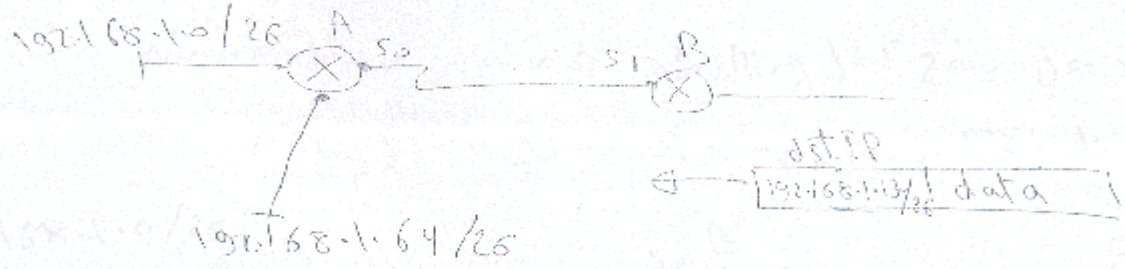
router that informed by a faild route don't accept any update about it for a time equal to the hold down time

hold down time = periodic update time = 30 sec

5- triggered update:

router sends the update as soon as change happen [don't wait the periodic interval]

- advantages of distance vector:
  - simple configuration
  - low CPU, memory usage
- di's advantages
  - BW waste (periodic update)
  - slow convergence
  - updates sent on broad cast (affect PC's)
  - classfull [don't support discontigous network]
    - ↳ don't sent subnet mask in updates



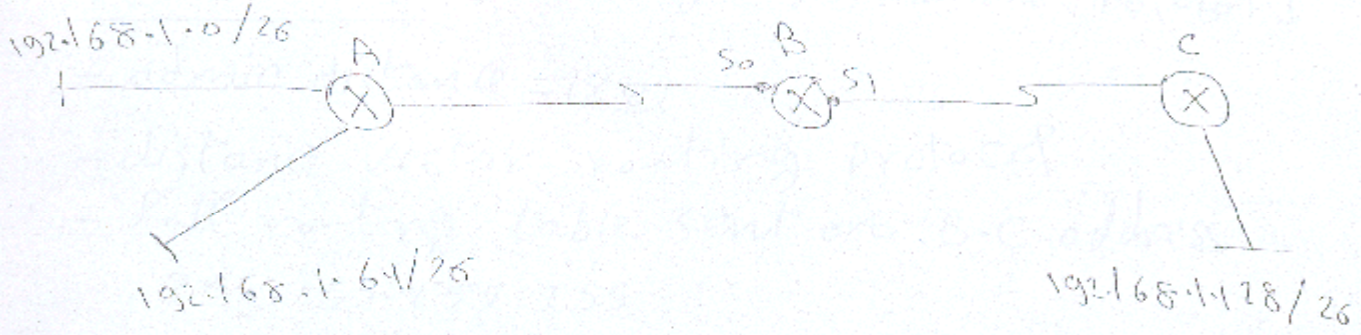
يفرض انه فيه data مطلوب ارجاع لل dst 192.168.1.63/26 ومرت ع S0
الخطوات الشبكات summary عند B وكمان نعلم انه B
بالراوتر A فينظر لل IP ويقول ان هذا ال IP موجود ع
ع الشبكة 192.168.1.0/24 وانه أعلم انه هذه الشبكة عند
الراوتر B فيقوم بارسالها لل الراوتر A عن طريق Int S1
الراوتر B فيقوم بارسالها لل A () data وعندما تذهب ال data
للاب انه تذهب الى network 192.168.1.128/26 وهذه الشبكة غير متصلة

بـ فيقوم بعمل drop لهذه ال Packet

:: إنت شغلت ال serial cable ع الاغلى
وكمان طلبت الراوتر يشغل ال Processing الاغلى
(distance vector protocol) وهذا هو من ضمن عيوبه
classfull لا وهو

III — مثال على subnetting لـ network address بنفس

(لاحظ) لا يوجد router بين A و B



- لو أرسل A الـ periodic update (بالبث) لـ B وطبعاً فيها summary لـ network (192.168.1.0) عشان الوصول لـ B يتم عن طريق الـ int S1

- لو أرسل A الـ periodic update (بالبث) لـ B فيقوم B بتسجل أن (network 192.168.1.0) عشان الوصول إليه عن طريق S1 وبالتالي B أصبح عنده مساريين عن طريق S0

فيقوم باختيار الطريق بناءً على أقل metric

قاعدة: لو عاوز تعمل (subnetting) وتستخدم (distance vector routing protocol)

:: لازم تكون عارف نفس الراوتر

إوعا عقلك يخيلك إنك عارف كل الـ subnets على كل الراوترات دة غلط

(distance vector) تحالي تحت أنواع البروتوكولات الذي يستخدم

II RIP V.1 [Routing information protocol]

- admin distance = 120
- distance vector routing protocol
- full routing table sent on B-C address
  255.255.255.255

→ After convergence,

- periodic updates every 30 sec
- metric Hob count [metric = 16 is an reachable]
- use bellman ford algorithm
- at change triggered upate
- hold down timer = 180 sec
- symbol in RTG table "R"
- support load balancing over pathes to the same dst. if they have the same metric

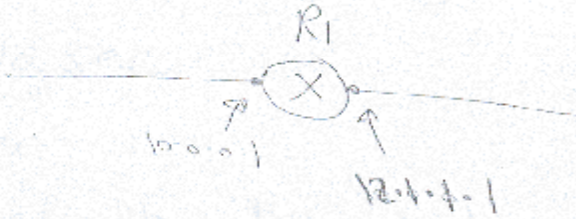
- classFull → don't send SM in the update

RIP configuration

(config) # router rip

(config-router) # network ← direct connected major networks

ex



R1(config)#router rip

R1(config-router)# network 10.0.0.0

R1(config-router)#network 12.0.0.0

طريقة عمل البروتوكول بأي جهاز وتأكيد عمله

trouble shooting

#show IP route ⟶ to view RIB table

show IP protocols ⟶ to view active routing protocols

debug rip ⟶ rip يعطي كل action يتم

أي خطأ يحدث بالـ rip

[2] IGRP : [interior gateway routing protocol]

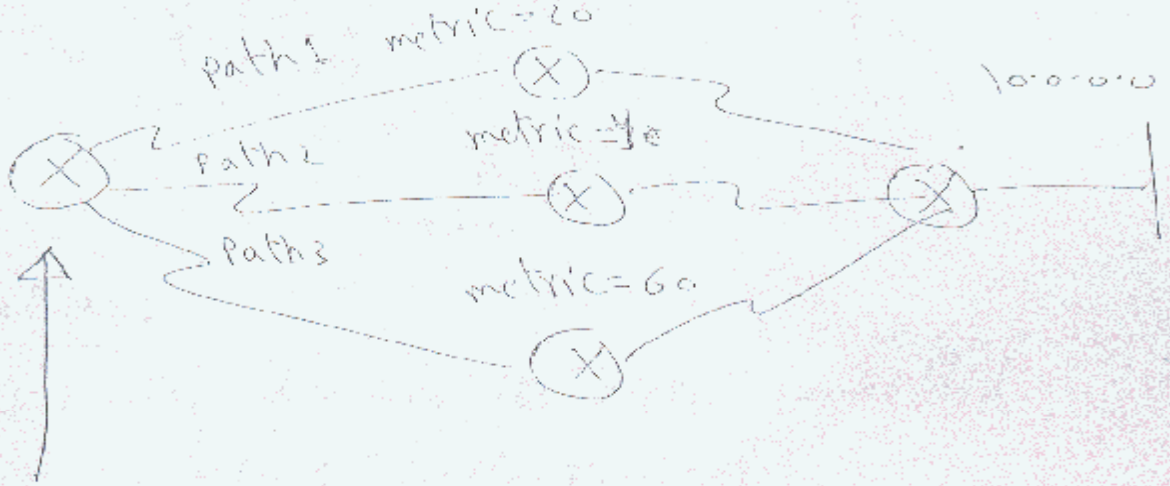
- distance vector protocol
- cisco proprietry [works on cisco routers only]
- Full RTG table sent on 255.255.255.255
- Periodic update every 90 sec
- hold down timer = 270 sec
- metric {Bw, delay} — default metric but can be load, reliability
- admin distance = 100
- max hop count = 255
- use bellman ford algorithm
- at change triggered update
- support load balancing : for paths that have unequal metric
- class full

IGRP configuration

(config)# router igrp ..AS No.
(router)# network direct connected networks

autonomous system

- to support load balancing:



(Config)# router igrp 100
(config-router)# variance 2
(config-router)# traffic-share balance

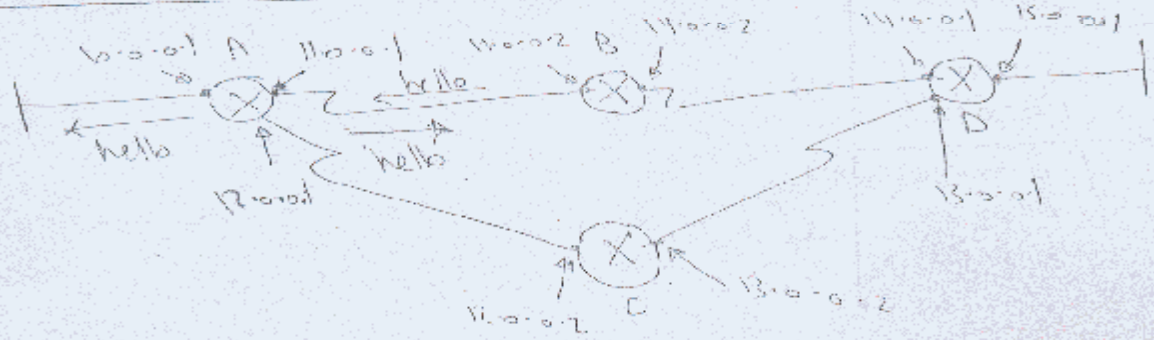
best Path =20
range used = 20 * 2 = 40
∴ Pathes are used between 20 → 40
Path (1 & 2)

load balancing

DAY 8

CCNA Track
Prepared by
ENG: Ahmed Abdallah

Link state Routing Protocol:



operation:

- every router discover its direct connected neighbors using "hello protocol"
- each router form a packet called (LSA): link state advertisment describing its interfaces

(LSA) ← A Router

10.0.0.1/8 11.0.0.1/8 12.0.0.1/8	A

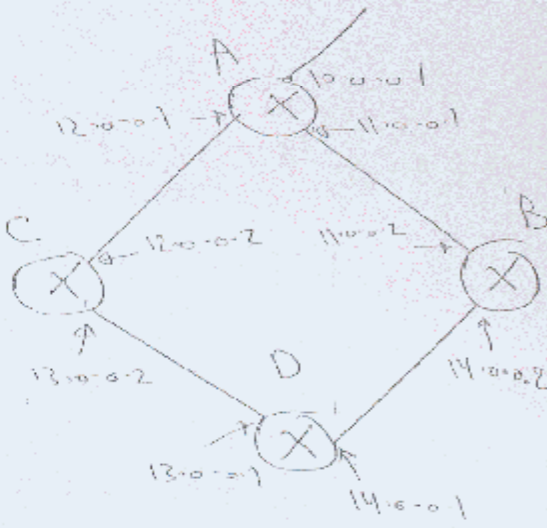
- Routers flood LSA's to all neighbors on a special multicast address

- From the received LSA's each router form the LSDB [link state data base]

Copy all LSDB of all router of it →

A	10.0.0.1 11.0.0.1 12.0.0.1
B	11.0.0.2 14.0.0.2
C	12.0.0.2 13.0.0.1
D	13.0.0.1 14.0.0.1 15.0.0.1

- each router will form the tree that describe the actual network connection and apply the Dijekstra algorithm to form the routing table



After convergence:

no periodic updates

→ At change : triggered update (LSA with failed route) is sent → so all link state process repeated again

- advantages:
  - loop free Protocols
  - No BW waste [no periodic update]
  - Fast convergence.
  - Classless
- DFS advantages:
  - complex configuration
  - high CPU memory.

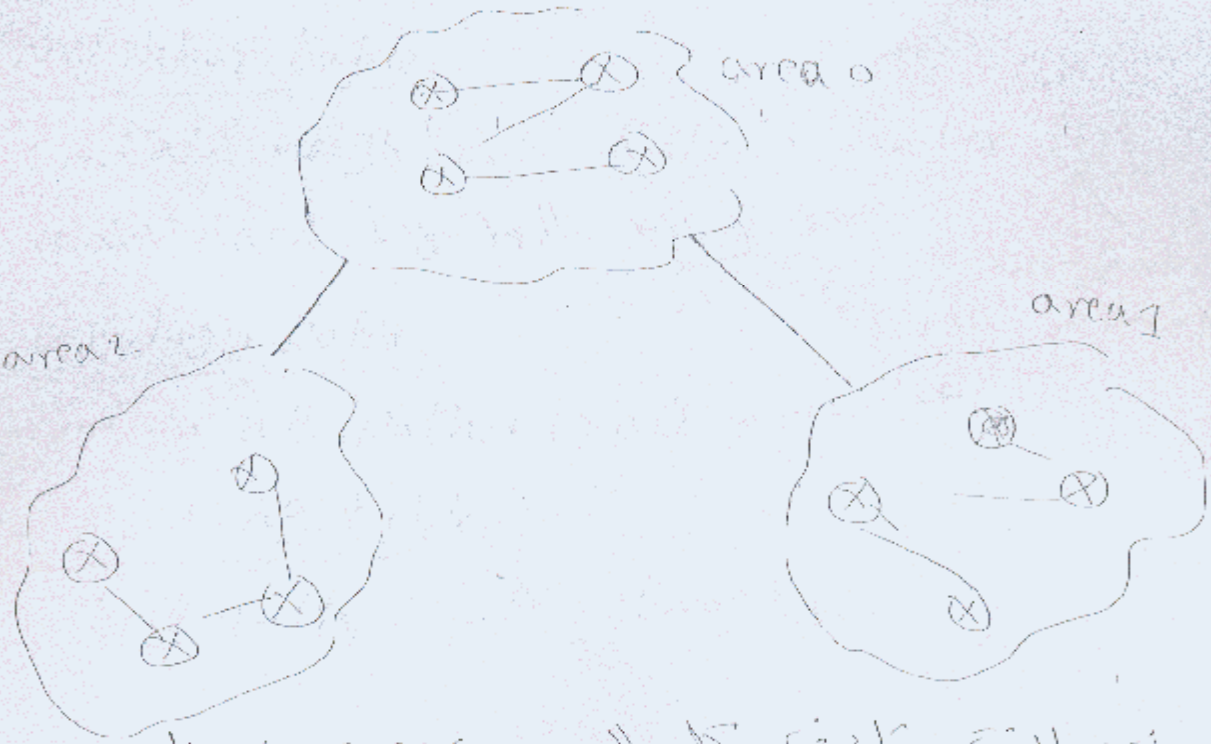
OSPF Protocol: [Open shortest Path First]

- link state Routing Protocol
- admin distance = 110
- metric (cost) = $\frac{10^8}{BW}$
- loop free Protocol → Routing loop ما فيه
- classless [send subnet mask in updates]
- use Dijekstra algorith.
- symbol in RTC table "O"
- send upate in multicast address 224.0.0.5 to reach neighbor only

- support hierarchical multiple area design by deviding ospf network to multiple areas to prevent frequent calculations [change in any area affects routers inside it only]

conditions

- area 0 is back bone area (zero)
- other areas must connected to area0



- other areas يجب ان تكون متصلة الى area 0

after convergence:

no periodic update except LSDB refreshment message every 30 min

at change: partial triggered update

اذا اذا حدث تغيير في الشبكة فإنه يرسل
LSA فقط معلومات عن الراوتر (الـ) الذي حدث فيه التغيير

---

ospf tables:

1- Neighbor table

- contain neighbors RID's [router ID]
- maintained by hello msg

الراوتر الذي له أصغر IP address يكون هو الـ RID

2- topology table

- contain all paths to all networks

3- Routing table

- best path to all networks

Router ID

- every router in the OSPF area is defined by Router ID (RID).
- RID is

1- The highest address of any logical interface (the highest loop back address)

(config)# int loop back _No._

(config-if)# ip address _IP_ _sm_

2- if no loopback address configured RID is the address of the heighest active physical interface. ←

IP أعلى

أعلى رقم

إذا ما في (loopback address) بيروح على الـ RID وبعاود أعرف

(loop back address) أعلى رقم

interfaces لـ IP أعلى رقم بتكون الـ RID

OSPF topologies:

1- Point to Point

2- broad cast multiple Access (BMA)

① operation in point to point

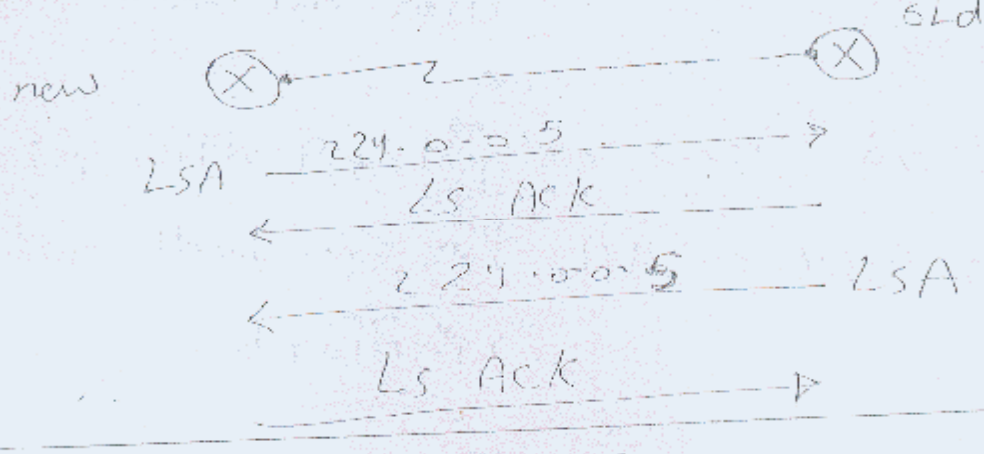
1- neighbor discovery:

- send hello on multicast address 224.0.0.1
every 10 sec on fast links (≥1.54 Mbps)
30 sec on slow links (<1.54 Mbps)
- dead interval = 4 * hello time
= 4 * 10 = 40 sec on fast link
= 4 * 30 = 120 on slow link

conditions for ospf router to be neighbors:

They must have
1- same area ID
2- same hello, dead interval
3- same authentication password

② route discovery



③ route selection: from the RTG table

2. BMA topology :

1- neighbor discovery : by hello protocol

2- DR, BDR selection :

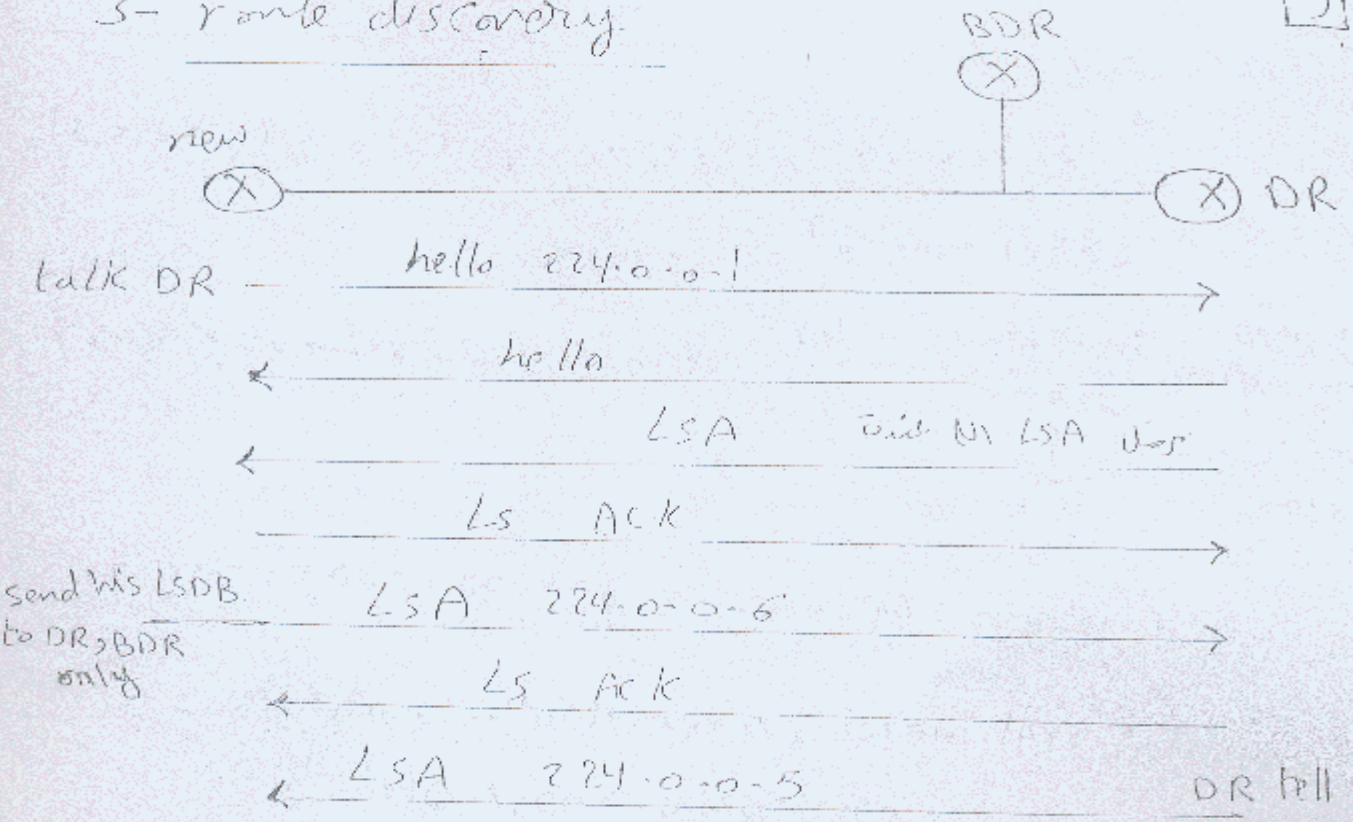
- DR : designated router
is the router with the
① highest Priority -> value from 0 -> 255
(default = 1) configured on Router

if the same Priority, DR is the router that have
② highest RID

- BDR : [back up DR]
- the second highest priority or RID
- works when DR fails

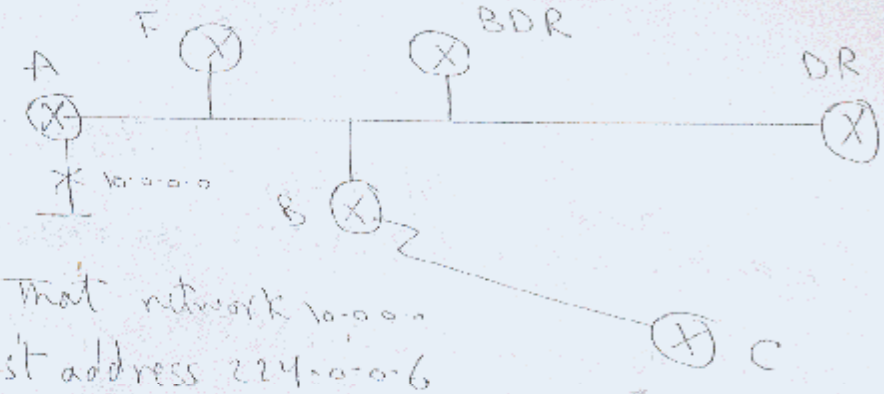
#note
- router with Priority = 0 can't be DR or BDR
- routers that are not DR or BDR called
drothers

3- route discovery



4- route selection from routing table

at change:



- A, B are brothers
- A tell DR, BDR that network fails on multicast address 224.0.0.6
- DR tell other routers on 224.0.0.5
- B tell C (point to point on address 224.0.0.5)

DR مقدار priority اذا كان اكبر من router جهاز DR مقدار

OSPF configuration

(config)# router ospf 1 — process id (1 → 65535)

(config-router)# network IP wildcard mask area area-id

sm ↔ wcm

area-id: zero-based number

if sm = 255.255.255.0 ∴ WCM = 0.0.0.255

area: determine which area contain this interface (if single area → use area 0).

IP: Network IP

ex

(config)# router ospf 1

(config-router)# network 192.168.1.0 WCM 0.0.0.63 area 0 (zero)

(config-router)#network 192.168.1.64 0.0.0.63 area 0

interface IP

(config)# router ospf 1

(config-router)# network 192.168.1.1 0.0.0.0 area 0

-router)# network 192.168.1.65 0.0.0.0 area 0

Trouble shooting

show IP route → to view RTG table

show IP ospf interface → to view RID area ID, Process ID & priority

show IP ospf neighbor → to view neighbor table

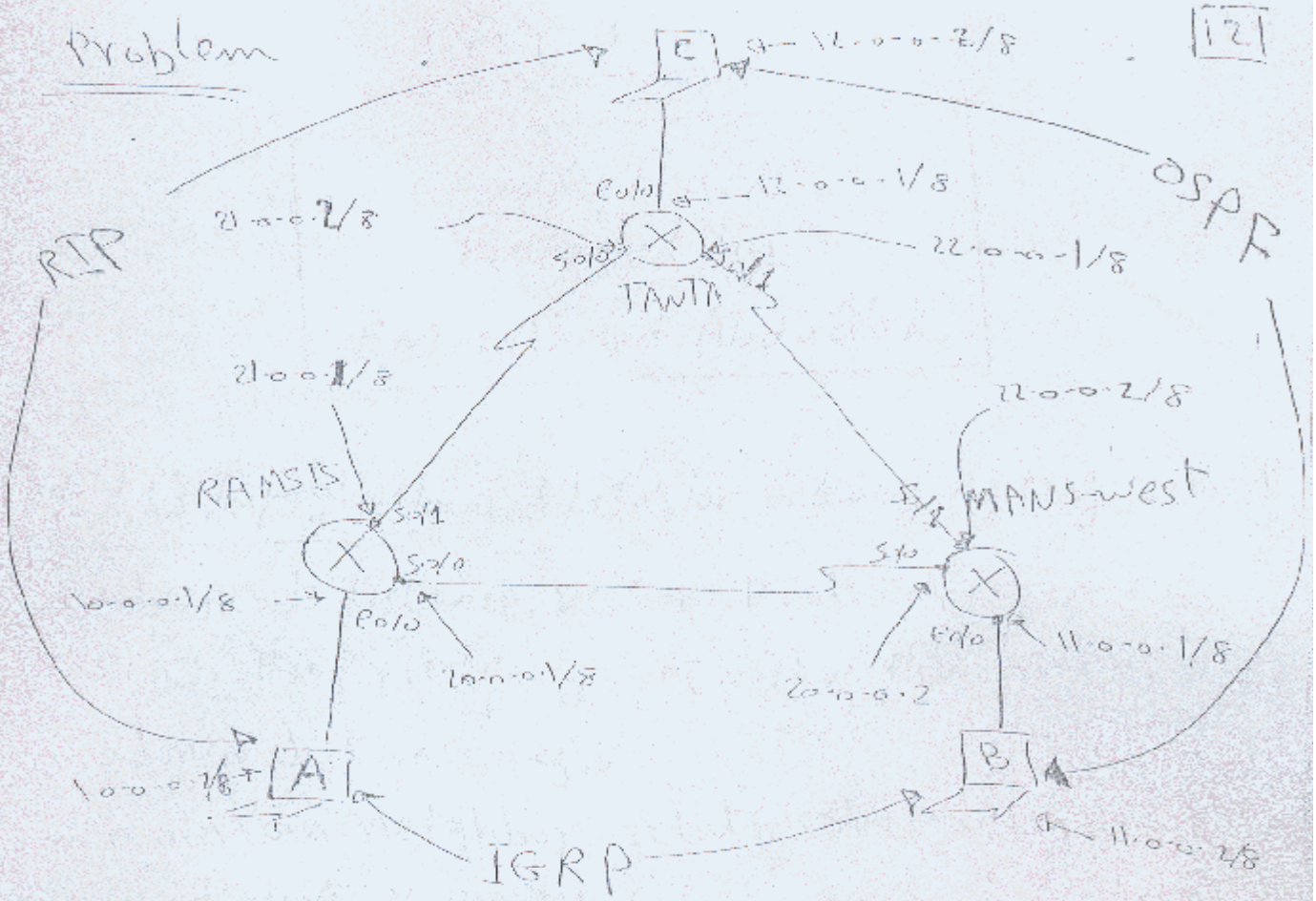
debug ip ospf adjacency → to view any action done by ospf protocol

⇒ to change router priority

(config) # int e0

(config-if) # ip ospf priority 0-255

Problem



RIP routing Protocol معناه C شايف A على Routing جدول

IGRP routing Protocol معناه B شايف A

OSPF routing Protocol معناه C شايف B

DAY 9

CCNA Track
Prepared by,
ENG: Ahmed Abdallah

EIGRP: enhanced interior gateway Routing Protocol

- advanced distance vector Protocol
- cisco Proprietary --> (work on cisco routers only)
- admin distance = 90
- maintain neighbor relationship using hello Protocol
- send hello's every 5 sec on fast links & every 60 sec on slow links
- dead interval = 3 * hello time
  = 3 * 5 = 15 sec on fast links
  = 3 * 60 = 180 sec slow links
- Rapid convergence
- reduce BW usage [no periodic update]
- send updates on multicast 224.0.0.10
- use "Dual" algorithm [store backup route for every best route]
- symbol in Routing table is "D"

- support multiple layer 3 protocols
  [IP, IPX, APPLE TALK]
- define seprate routing table for each
- support load balancing over equal & unequal metric pathes
- differentiate between internal & external routes

protocol	network	admin distance
D	192.168.1.0	90
D EX	10.0.0.0	170

- admin distance for internal routes = 90
- admin distance for external routes = 170

autonomous systems

جدول الـ routing الخاص بـ R1 يحتوي على network

- Compatable with IGRP in the same AS

EIGRP metric = 256 * IGRP metric

↓ store in 32 bit

↓ store in 24 bit

(Bw, delay)

- EIGRP routers to be neighbors:

1- They must be in the same AS

2- They must have the same metric factors (k-values)

note: ...

$$\text{EIGRP metric} = \left[K_1 \times Bw'' + \frac{K_2 \times Bw''}{256 - load} + K_3 \times delay + \frac{K_5}{reliability + K_4}\right] \times$$

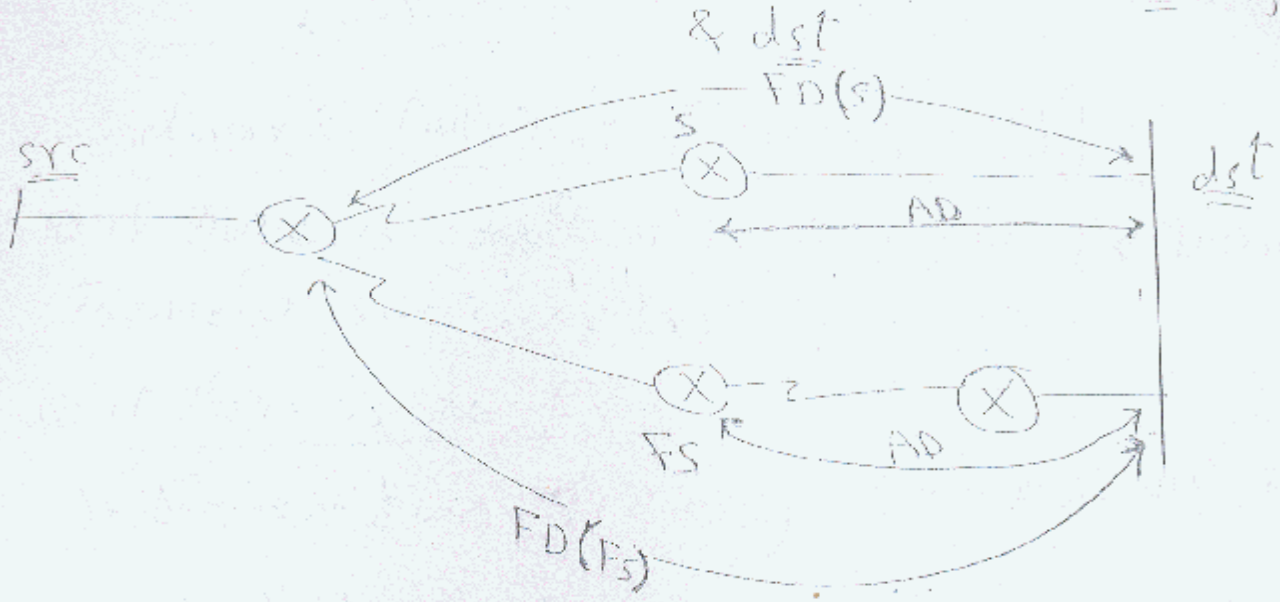
where $Bw'' = \frac{10^7}{Bw}$, delay in terms of ms

- max Hop count = 224
- reliable
- class less

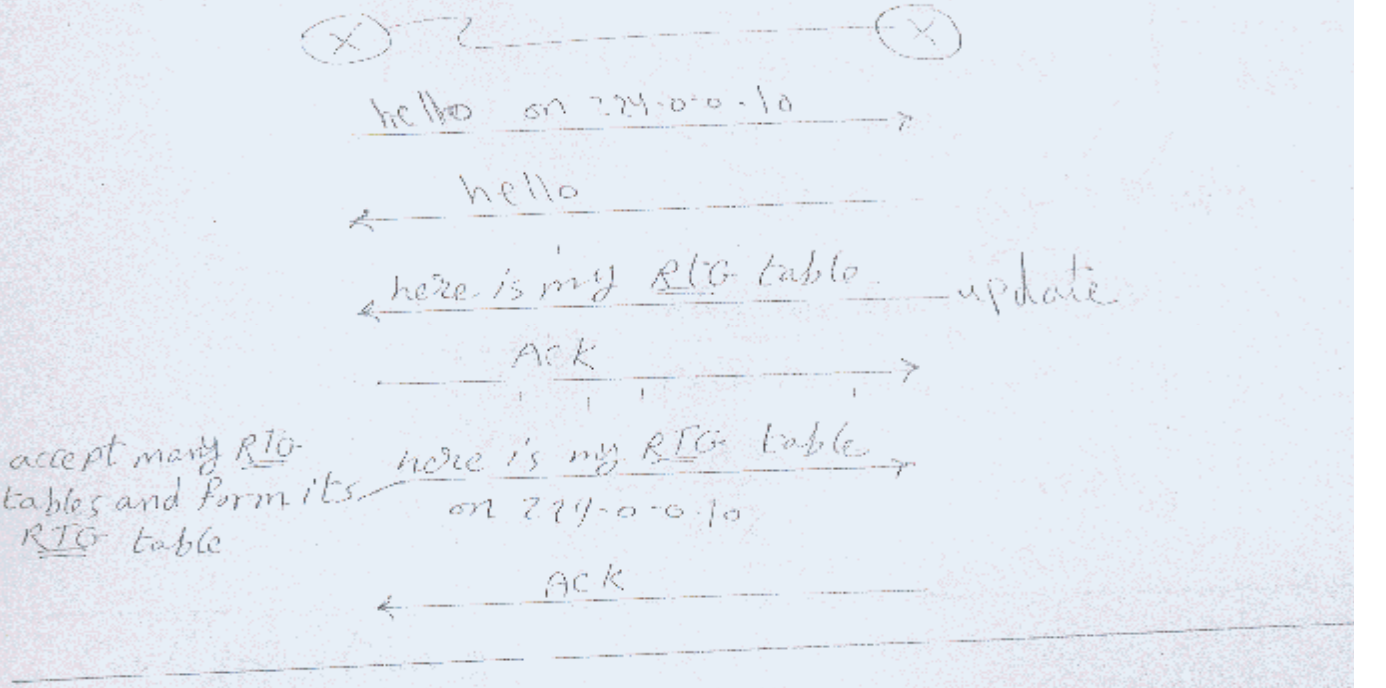
EIGRP terminology

- neighbor table : list of all neighbors
- topology table : list of all pathes to all destinations
- Routing table : best pathes to all destinations

- successor (s) : neighbor lead to best route which is stored in RTG table
- Feasible successor "FS" : neighbor lead to backup route which is stored in topology table only
- Feasible distance "FD" : metric between src & dst
- advertised distance "AD" : metric between src neighbor & dst

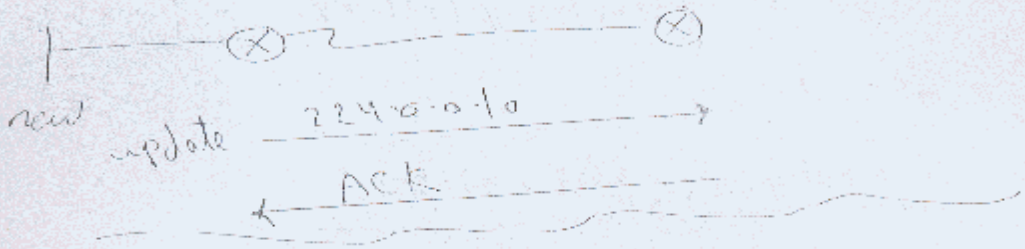


operations at start up



-at change :

1- new network appear :



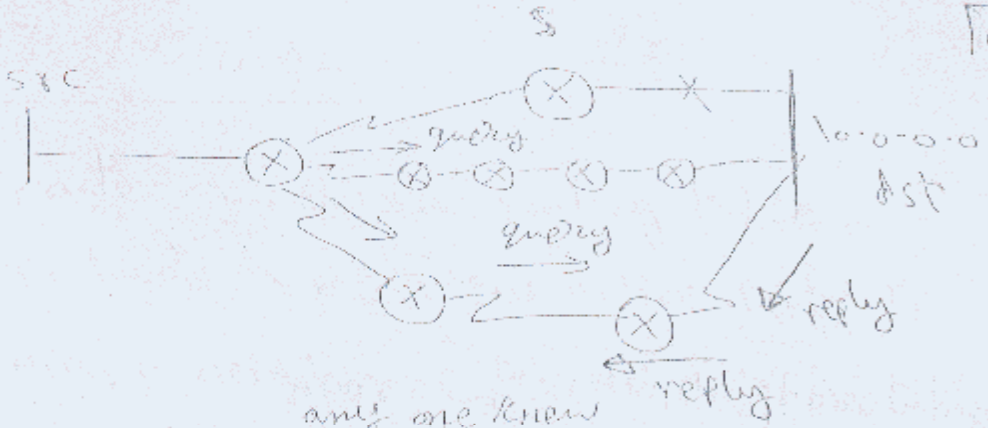
2- network Failure : [successor Paild]

① if there is a back up Fs Then The Fs become The new successor (s)

② if There is No Fs :

إجراءات يتم اتخاذها في حالة عدم وجود (memory msg) لدى الجار

(88)



query → (any one knew Path to 10.0.0.0)

← yes/no — reply

ack →

Configuration:

(config)# router eigrp ___automomous system No.

(config-router)# network ___ IP
↑ subnet IP

ex: 192.168.1.1/26 → ⊗ ←192.168.1.66/26

(config)# router eigrp ---100

(config-router)# network 192.168.1.0

(config-router)# network 192.168.1.64

Trouble shooting-

sh IP route → to view routing table
sh IP protocols → to view active protocols
sh IP eigrp neighbor → to view neighbor table
sh IP eigrp topology → to view topology table
debug IP eigrp → to view any action done by e

RIP V.2 :

- advanced distance vector routing protocol
- no periodic updates (only triggered)
- admin distance = 120
- update sent on multicast 224.0.0.9
- symbol in RIB table is "R"
- metric → hop count [metric 16 unreachable]
- class less

---

configuration :

(config) # router rip
- router) # version 2
router) # network -- IP --
↑
subnet IP

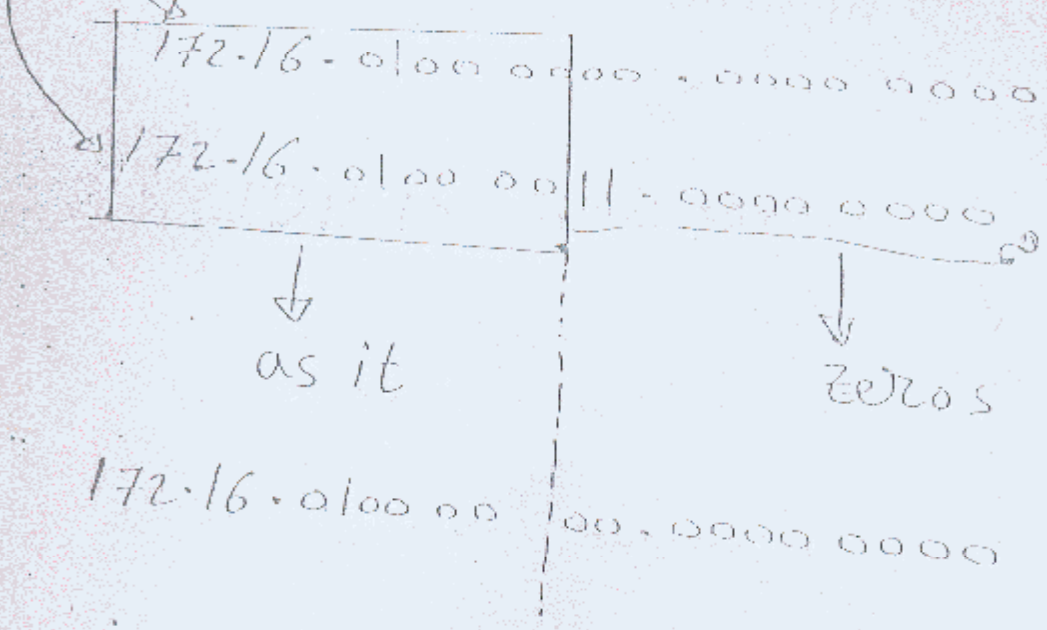
int (فيديو) ثم ip address 192.168.1.69

Route summarization :

Groping block of subnets in one address

ex

172.16.64.0/24
172.16.65.0/24
172.16.66.0/24
172.16.67.0/24



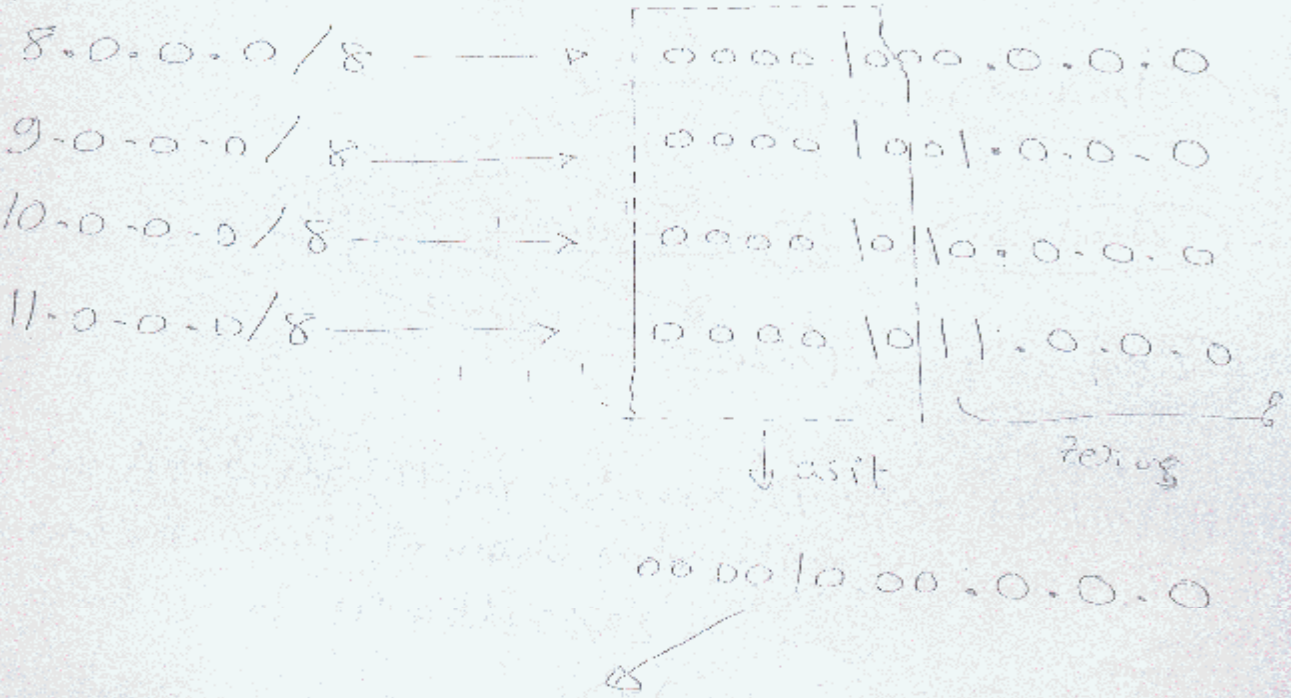
∴ Summary is 172.16.64.0/22

No. of common bits

CIDR : (classless interdomain routing)

↳ grouping of major networks in one address

ex



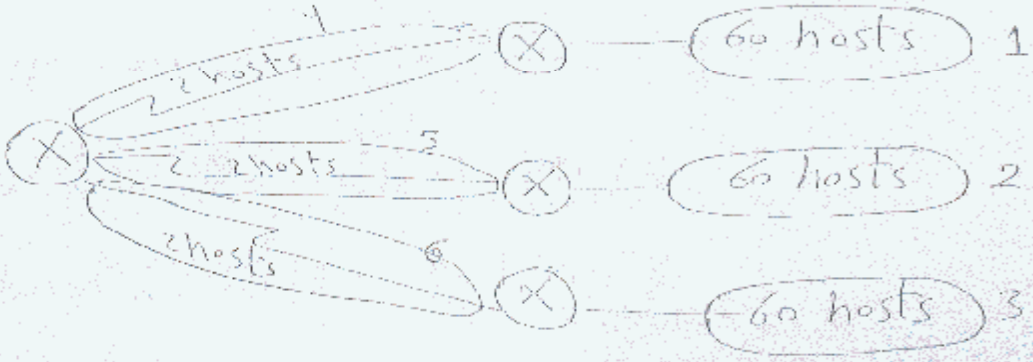
∴ CIDR is 8.0.0.0/6

No. of common bits

VLSM : variable length subnet mask

- support only by classless routing protocols
- used to utilize using addresses

ex



You have the major network IP : 192.168.1.0/24 and we want to made subnetting to reduce the number of IP addresses

solution

for networks 1, 2, 3 are need 60 hosts

- SM = 255.255.255.192
- Hop count = 256 - 192 = 64
- 1st subnet : 192.168.1.0 /26
- 2nd subnet : 192.168.1.64 /26
- 3rd subnet : 192.168.1.128 /26

to → 192.168.1.191 /26

→ starting from address 192.168.1.192

give addresses to subnet 4, 5, 6

2 hosts → we need 2 bits subnet

∴ Sm = 255.255.255.252

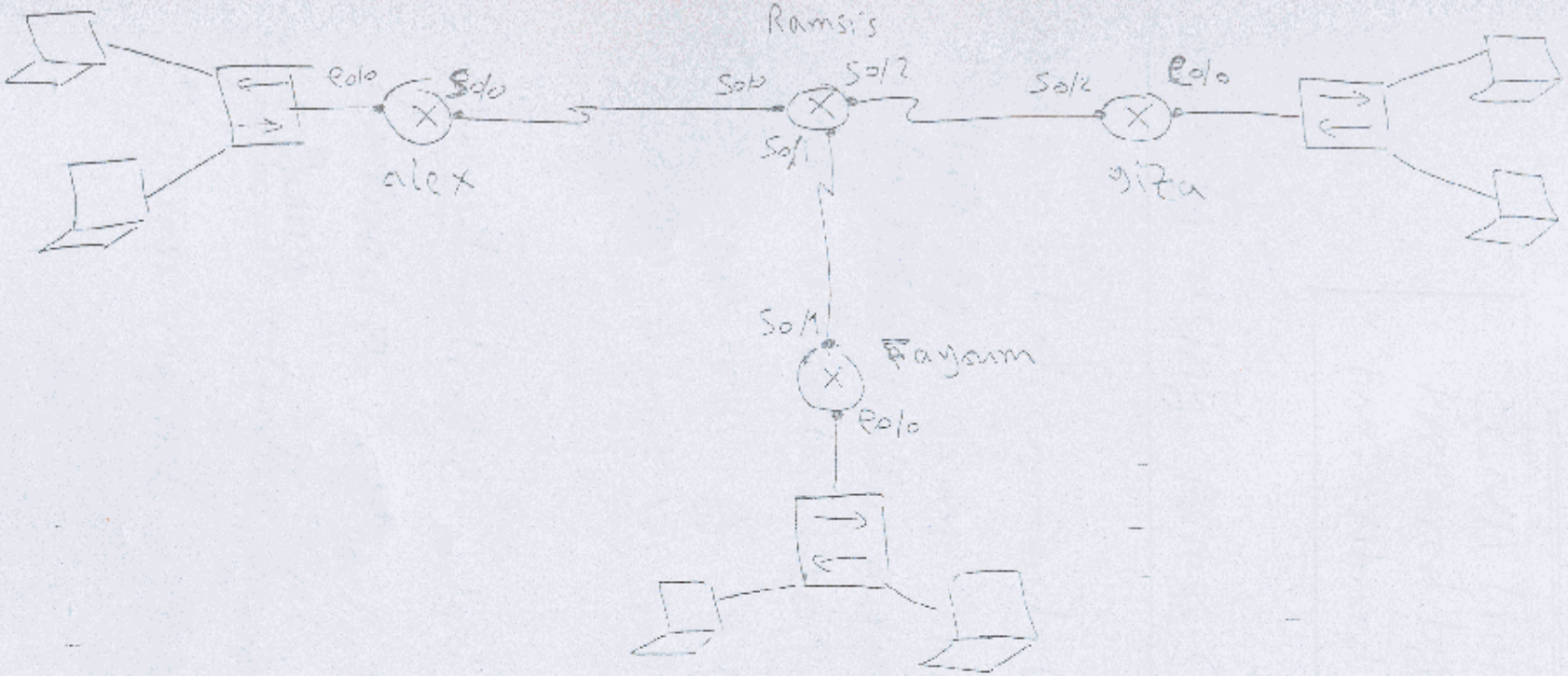
∴ Hop count = 256 − 252 = 4

∴ 4th subnet : 192.168.1.192/30

5th subnet : 192.168.1.196/30

6th subnet : 192.168.1.200/30

note that → VLSM is supported only by classless routing protocol



هذه الـ network 200.17.11.0/24 : سنقوم أولا بعدد ٣ IP's ثم نقسم بعد ذلك subnetting بـ

هذه الروتر بـ ٣ سنقوم RIP v.2 أو EIGRP

DAY 10

CCNA Track
Prepared by
ENG: Ahmed Abdallah

#security using Access control list (ACL)#

ACL: a set of commands (lists) grouped to gather by a group "numbered or named" that are used to filter traffic entering "inbound" or leaving "outbound" certain interface

مجموعة من الأوامر تم تجميعها تحت اسم واحد أو رقم وتستخدم لفلترة الـ traffic الداخل أو الخارج من واجهة معينة بالسماح أو المنع deny or permit

ip → host

inbound → traffic entering the interface
↳ Process the ACL before routing process

out going → traffic leaving the interface
↳ Process the ACL after routing process

Types of ACL

Standarded ACL

- Permit or deny all traffic from certain src "host or N.W"
  - Numbered ACL
    - has a unique No.
      - "1 → 99"
      - "1300 - 1999"
  - Named ACL
    - ACL has a unique name.
- match on → src IP address in the IP packet

extended ACL

- Permit or deny certain type of traffic from source to destination "host or N.W"
  - Numbered ACL
    - from "100 → 199"
    - or "2000 → 2699"
  - Named ACL
- match on → src and dest IP addres

ACL Processing

- statement in ACL is processed top to down
- once a match [permit or deny] is found, no forther statement processed
- order of statements are important
- IF no match is found the packet is droped due to there is a default imaginary statement at the end of each list called → implicit deny = deny any
- ACL must contain at least one permit condition or otherwise it will drop all traffic
- in numbered ACL you can't delete specific statement "delete all only"
- when ACL is made you can't add entry between old entries, any added entry goes to the end of the list.
- you can have 1 ACL per each protocal ("IP, IPX, NPPLE TALK") applied to an interface in each direction.

6 ACL

II Standered numbered ACL

① Forming.

(config) # access-list {1-99/1300-1999} {permit/deny}
src IP [WCM]

optional

subnetworks & major نوع تقوم بين أن تريد إذا فقط

② activation.

(config) # int so ← ACL نختار الواجهة التي تريد وضع

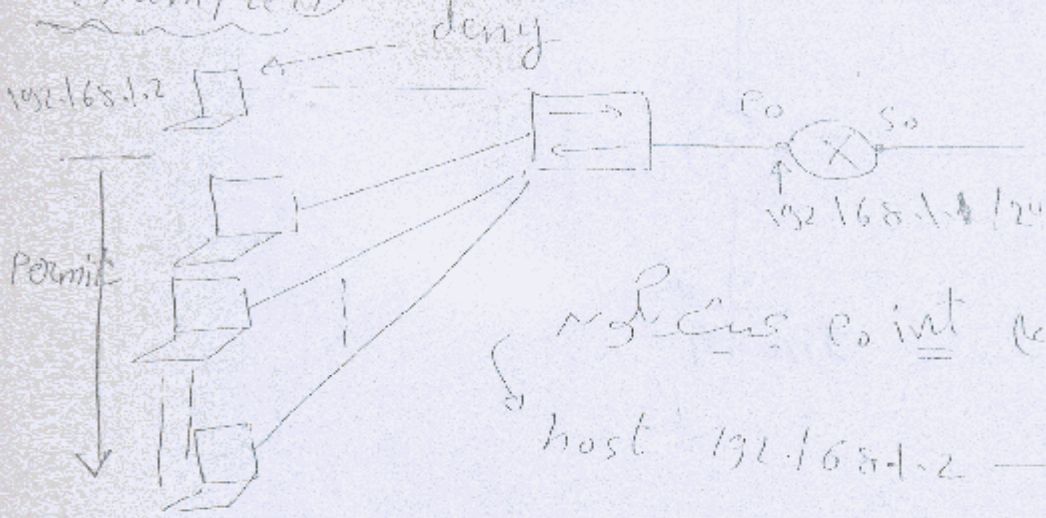
(config-if) # IP access-group {1-99/1300-1999} {in/out}

ACL نختار رقم

inbound

outbound

example ①



نريد نمنع Fo int ع ACL نحط

host 192.168.1.2 → deny

any other host → Permit

solution

① Farming

(config)# Access-list 1 deny host 192.168.1.2

access-list 1 permit 192.168.1.0 0.0.0.255

WCM

② Activation

(config)# int Fo

(if)# IP access-group 1 in

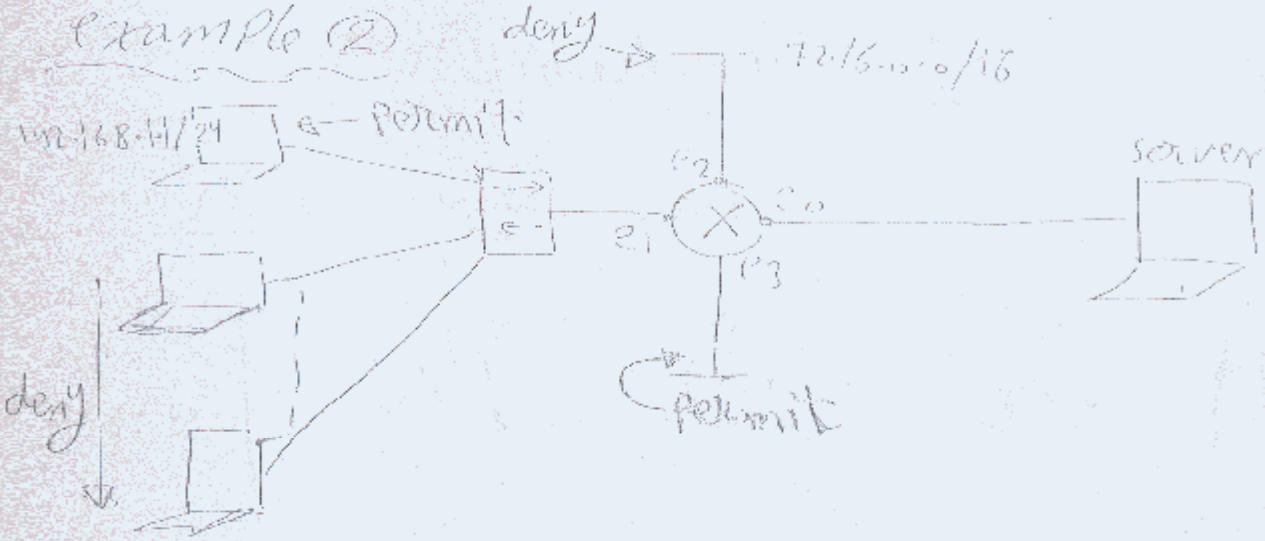
ACL هلأ عم ؟ نعم وكمان على So int ع ACL حط

بس Fo ع ACL حط بردو لازم routing يشتغل

بدل ما الـ packet يعمل routing ثم يروح للـ

drop يعمل

example (2)



sol

(config)# access-list 2 permit host 192.168.1.1

(config)# access-list 2 deny 192.168.1.0 0.0.0.255

(config)# access-list 2 deny 172.16.0.0 0.0.255.255

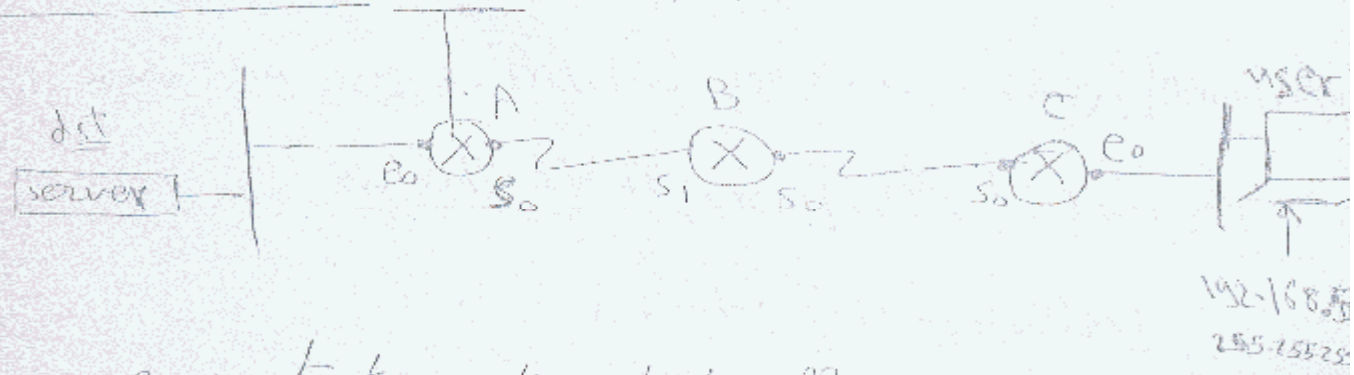
(config)# access-list 2 permit any

(config)# int e0 ↵

(config-if)# ip access-group 2 out

• Placement of standered ACL

Example (3) 192.168.2.0/24



→ we want to restrict traffic from user x to server

A(config)# access-list 1 deny host 192.168.5.1

A(config)# access-list 1 permit any

A(config)# int e0

A(config-if)# IP access-group 1 out

∴ standered ACL placed as close as possible to destination (dst)

2 extended Numbered ACL

1- Forming

(config)-# access-list {100 -> 199 / 2000 -> 2699} {permit/de

protocol src IP [wcm] dst IP [wcm]

[protocol information]

note:

- Protocol -> IP, ICMP, TCP, UDP

- protocol information -> [operator + dst. port No. o
application name] OR

ICMP msg type

- operator:

lt -> less than
gt -> greater than
eq -> equal to
neq -> not equal to

ICMP msg types

- echo
- echo reply
- host-unreachable
- network-unreachable
- traceroute

2. Activation

(config)# int e0

(config-if)# IP access-group ---- {in/out}
(number)

Ex

(config)# access-list 100 permit tcp any 172.16.0.0 0.0.255.2

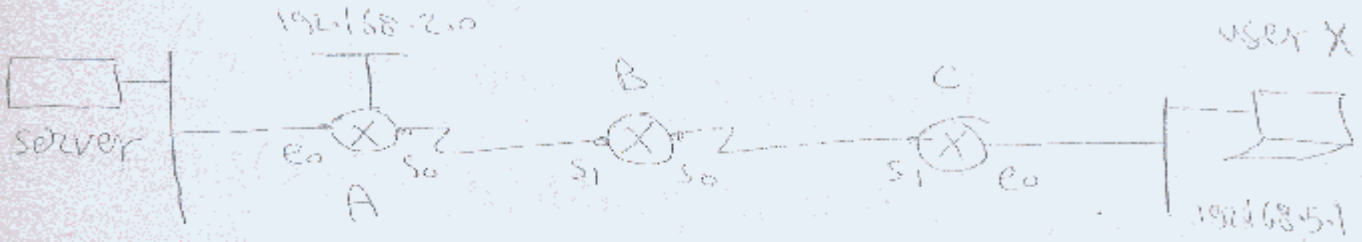
(config)# access-list 100 permit udp any host 172.16.1.1 eq dns

(config)# access-list 100 permit tcp 172.16.0.0 0.0.255.255 host 172.16.12.1 eq (23) ... telnet application

(config)# access-list 100 permit ICMP any 172.16.0.0 0.0.255.2 eq echo-reply

(config)# access-list 100 permit ip any any

Placement of extended ACL



192.168.1.1/24

→ we want to restrict telnet from user X to server

C(config)# access-list 100 deny tcp host 192.168.5.1 host 192.168.1.1 eq telnet (23)

C(config)# access-list 100 permit IP any any

C(config)# int e0

C(config-if)# ip access-group 100 in

→ Extended ACL placed as close as possible to source

→ we want to restrict IP packet from user X to server

C(config)# access-list 100 deny IP host 192.168.5.1 192.168.1.1

[3] Named standered ACL

(config)# IP access-list standared name

(config-std-ACL)# {permit/deny} src IP [WCM]

[4] extended named ACL

(config)# IP access-list extended name

(config-ext-ACL)# {permit/deny} protocol src IP WCM dst IP WCM [protocol information]

activation

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

* to erase ACL,

(config)# no access-list # of ACL (number) or name of ACL

* to erase a statement from named ACL

(config-std-ACL)# → no {permit/deny} + statement

(config-ext-ACL)# → no {permit/deny} + statement

For numbered ACL you can't delete a statement but you can delete all the statement

(config)# no access list 100

Trouble shooting

#sh ip access-lists ---> ACL ترى كل

IP Packet

#sh access-lists ---> ACL كل ترى كل

#show access-lists 100 ---> 100 ترى

#show IP interface Solo

In bound ACL

out going ACL

DAY 11

CCNA Track
Prepared by
ENG: Ahmed Abdallah

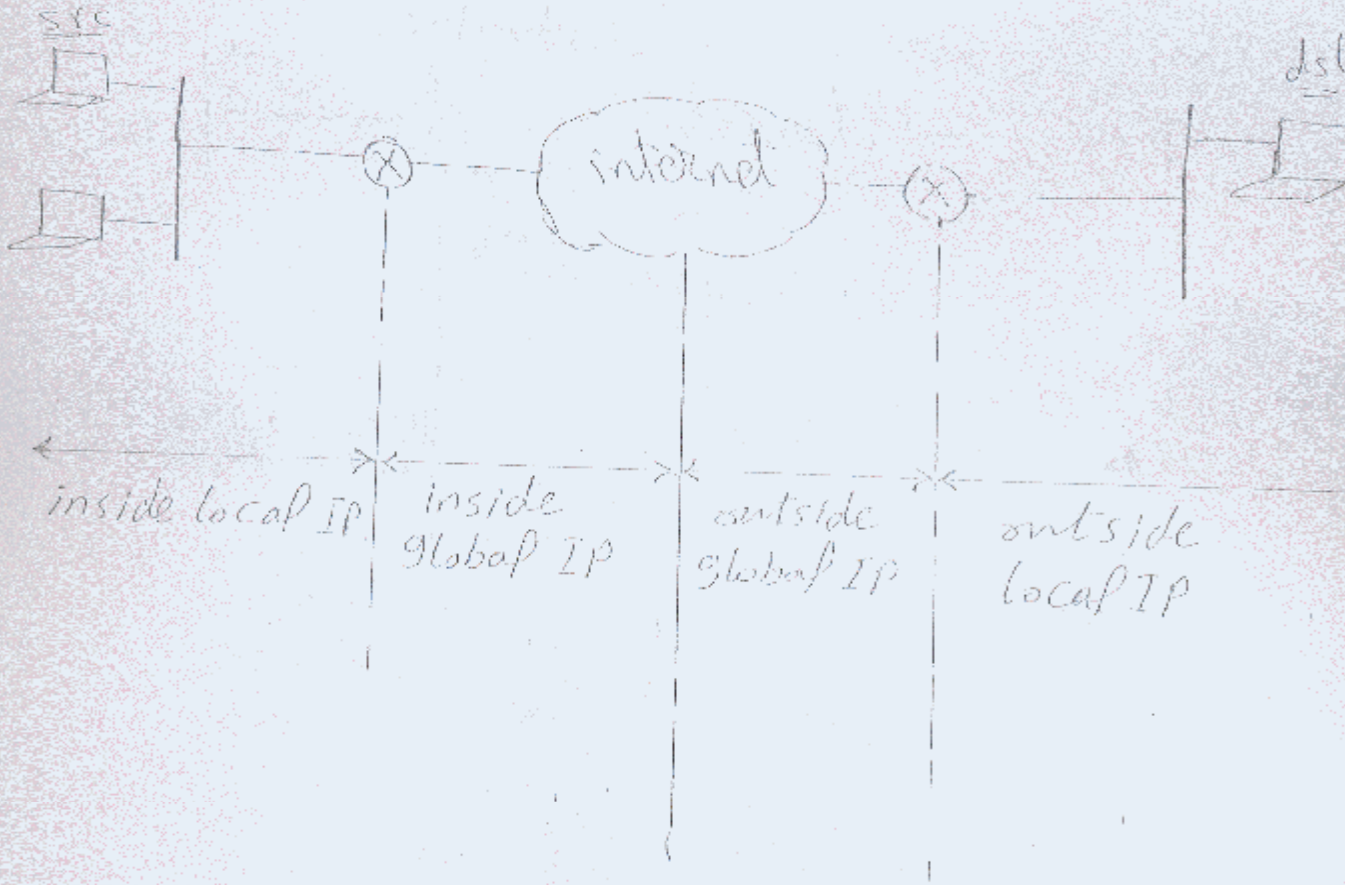
NAT: "network address translation"

- NAT :- translate one IP address to another
  "Can be src or dst"
- solve 2 problems
  - handling a shortage of IP address
  - hiding new address schemes

NAT terminologies

- inside => device located on inside of your nw
  "local device"
- outside :- device located on outside of your nw
  "outside device"
- global => public IP
- local => private IP
- inside local IP :- local device has an assign private IP

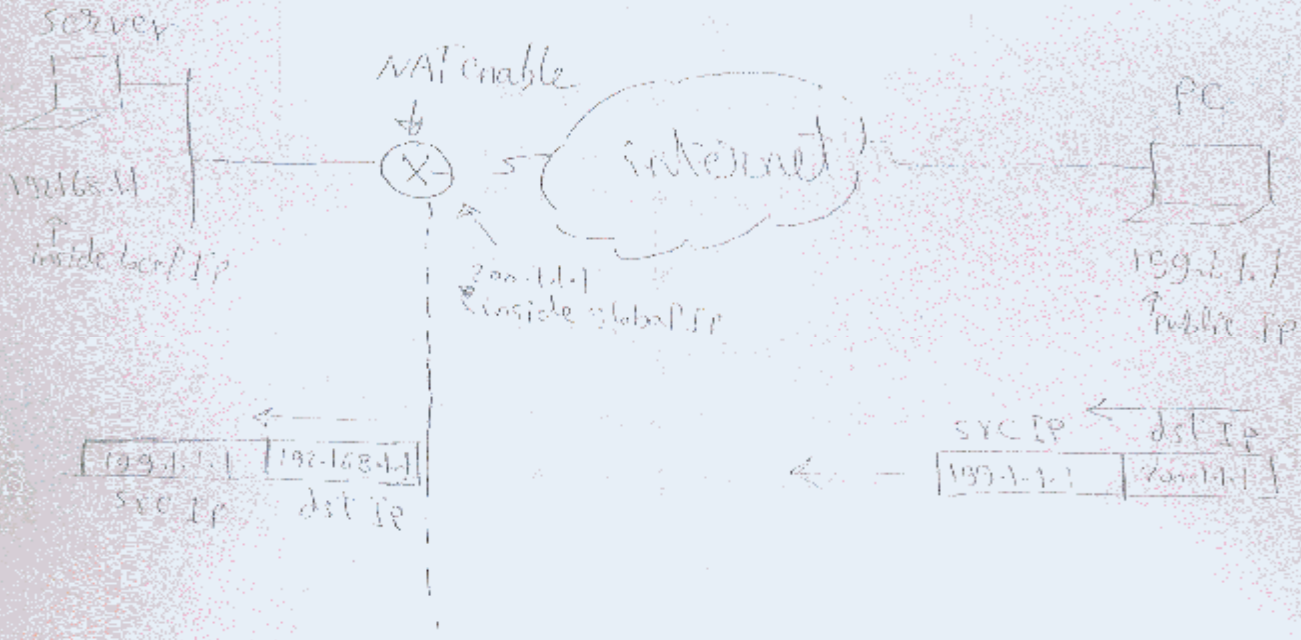
- inside global IP → Local device has a registered public IP address
- outside global IP → outside device has a registered public IP address
- outside local IP → outside device has a registered private IP address



Types of address translation

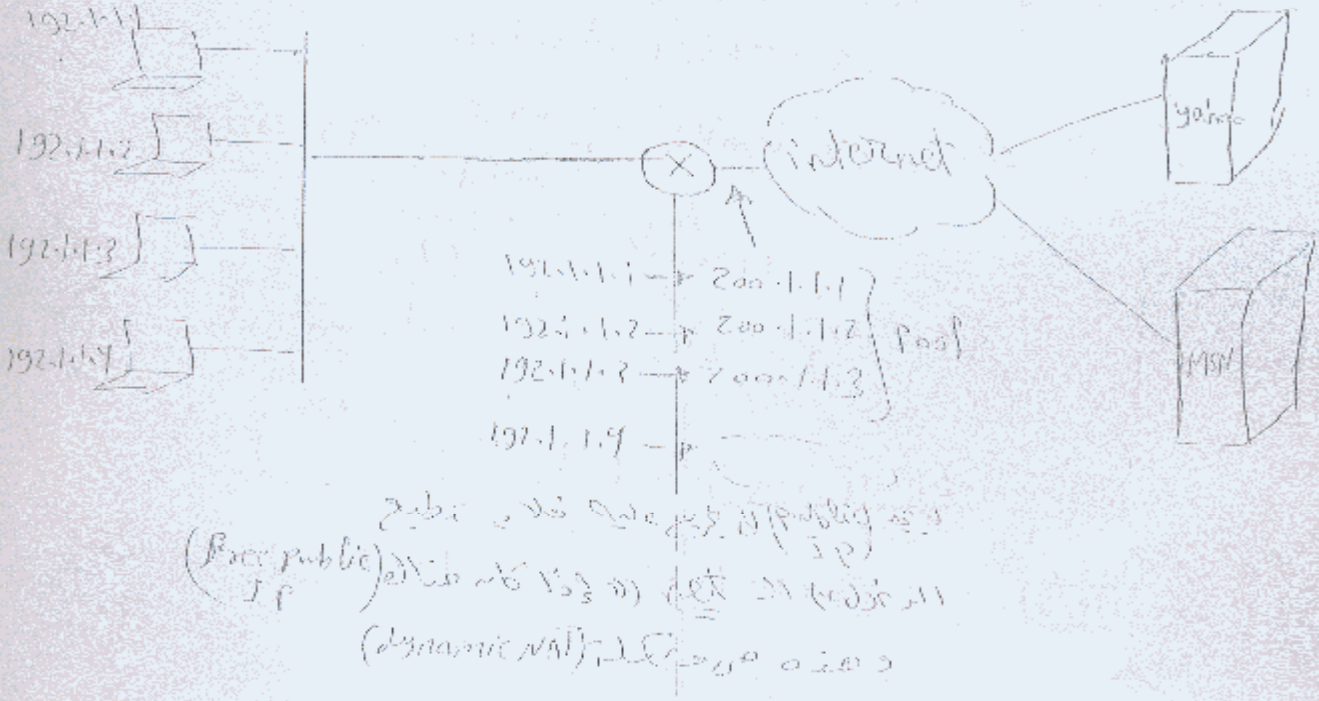
1) Static NAT:

- manual translation of one IP address to a different one IP address
- used to translate dst address in IP packet when outside device want to access your internal resources



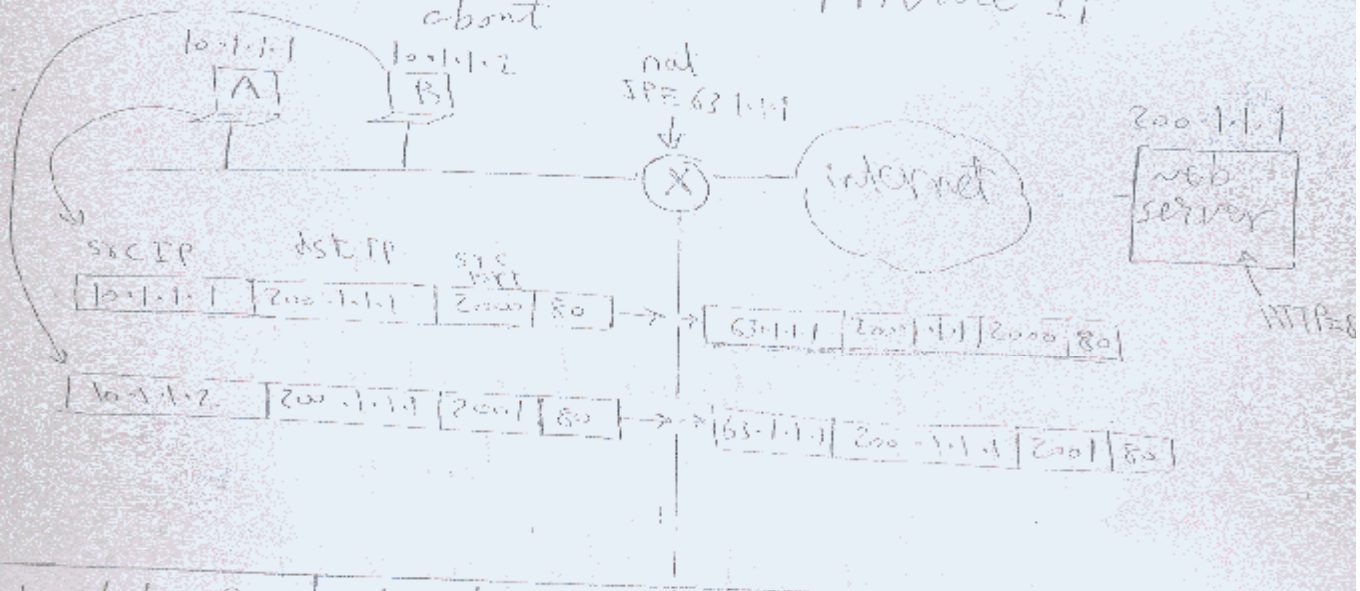
B. Dynamic NAT

- automatic translation, router is given a pool of IP's that contains global IP address, so every user tries to access a public N.W will be given IP from the pool



[3] PAT "Port address translation"

- Static & Dynamic NAT problem is that it's provide one to one address translation
- PAT ← use one or more public IP's using port number called "over load"
- used when ← inside users wants to access outside resources
- 1 public IP serve about → 64000 private IP

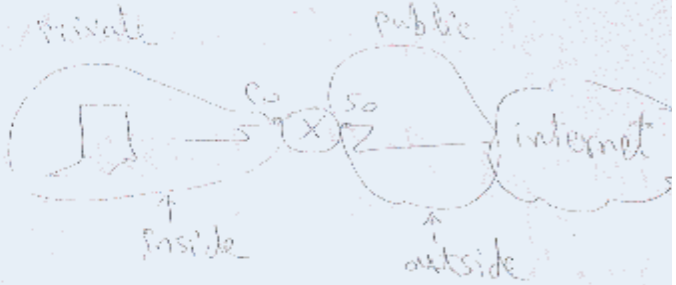


inside local IP	inside local port	inside global IP	inside global Port
10.1.1.1	2000	63.1.1.1	2000
10.1.1.2	2001	63.1.1.1	2001
10.1.1.2	2000	63.1.1.1	2002

10.1.1.2 & 10.1.1.1 من 2002 ← 2000 من port لـ الـ هنا الـ router هاد بتغيير رقم الـ
collision صار ما (ليش) (63.1.1.1 = public IP) الـ على بحيث بالـ

NAT configuration

1) Static NAT



(config)# IP nat inside source static inside_local / src IP ↑ private IP inside_global / src IP ↑ public IP

(config)# int e0
(config-if)# IP nat inside
(config-if)# int s0
(config-if)# IP nat outside

[2] Dynamic NAT

a) define allowed inside IP address, "standard ACL"

(config) # access-list ___ # - permit ___ srcIP ___ [wcm] ← optional

b) define pool "public addresses"

(config) # IP nat pool ___ pool name ___ beginning inside global ___ ending inside global IP ___

netmask 255.255...

c) (config) # IP nat inside source list ACL # ___

pool ___ pool name ___ [overload] ← optional

-PAT

d) assign configuration to interfaces

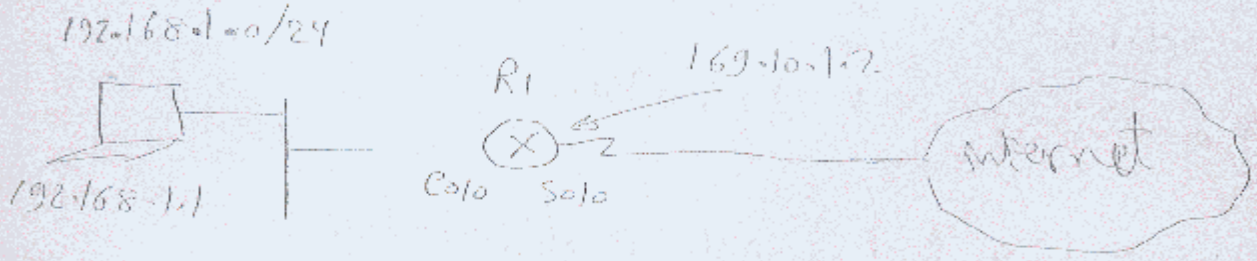
Trouble shooting

show IP nat translations
↳ natting ده اللي بيعرض الـ IP's اللي بتتحول

#sh IP nat statistics → to see → inside nat int
→ outside nat int

---

ex:



① assign a public IP 169.10.1.2 to 192.168.1.1
↳ static NAT

(config)# IP nat inside source static 192.168.1.1 169.10.1.2

(config)# int fa0/0
(config-if)# IP nat inside
(config-if)# int se0/0/0
(config-if)# IP nat outside

② assign the ethernetwork address to adynamic assigned address pool public range

169.10.1.50/24 ~ 169.10.1.100/24

:- Dynamic

ⓐ (config)# access-list 1 permit 192.168.1.0 0.0.0.255

ⓑ

(config)# IP nat pool aaa 169.10.1.50 169.10.1.100 netmask 255.255.255.0

ⓒ #(config)# IP nat inside source list 1 pool aaa

ⓓ T

---

③ configure NAT over load on R1

:- PAT

ⓐ ~ like ②

ⓑ ~ like ②

ⓒ like ② + overload

ⓓ T like ②

DAY 12

CCNA Track
Prepared by-
ENG: Ahmed Abdallah

Switching

- switch is a layer 2 device
- switch is single B.C domain & multiple C.D domain
- Forwarding in switch depends on hardware using ASIC's
- types of errors that sw can't overcome it.
  - CRC
  - Runt frame error
  - giant frame error
- switching methods

1- store & forward → check all the frame
2- cut Through → check 1st 14 byte
3- modified cut Through [fragement free] → check 1st 64 byte

- Transparancy :

1- no host aware that there is a switch
2- no switch aware that there is another switch
3- switch don't change in the frame

- switch functions :

[1] learning : Forming MAC table Through learning the src in the Frame

[2] Forwarding :

a) Flooding Forwarding → B.C
→ multi unicast
→ unknown unicast

b) dedicated forwarding by microsegmentation to a known unicast

5 Remove Layer 2 loops:

switch remove L2 loops using STP

Day 2 2:1

- STP: Spanning tree protocol (STP) : IEEE 802.1d

→ to avoid loops we can remove one of switches but we need it for redundancy

- loop occures when we have 2 pathes to dst so we will use STP to make a logical Block for one path & when the used path fails, STP will open the Blocked one

STP operation:

- 1 Flooding & collecting "BPDUs":

- First its sw consider it self a root & send "BPDU" = "Bride protocol data unit" to other switches on multicast MAC

- every sw will take a copy of the "BPDU" & resend it to other switches after changing the accumulative cost

- each sw will form BPDU data base

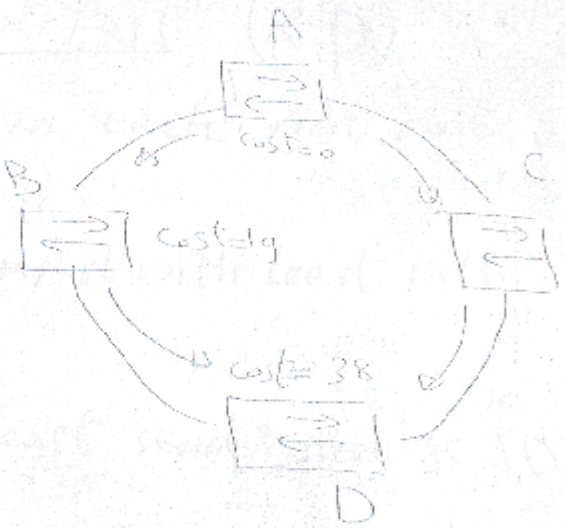
BPDU: is a msg have some information

	Bridge ID
	sender Bridge ID
	Port ID
	accumulative cost

Bridge ID → Priority | Bridge MAC address
sender Bridge ID → Priority | Port MAC address
Port ID → Priority | Physical Port No.

→ accumulative cost: initially = 0

Then cost increase according BW



[2] electing The root Bridge (RB)

- it is The sw with lowest Bridge ID
- choice according to → lowest priority → if equal → lowest sw MAC
- after electing The root, The root Bridge only send BPDU's every 2 sec
- other non root switches stop sending BPDU's

[3] electing The root Port (RP)

- RP → best Port in each non root sw to reach The root
- choice → Port with least path "low accumulative cost" → if equal → least sender Bridge ID → if equal → least port ID

[4] electing The Designated port "DP"

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

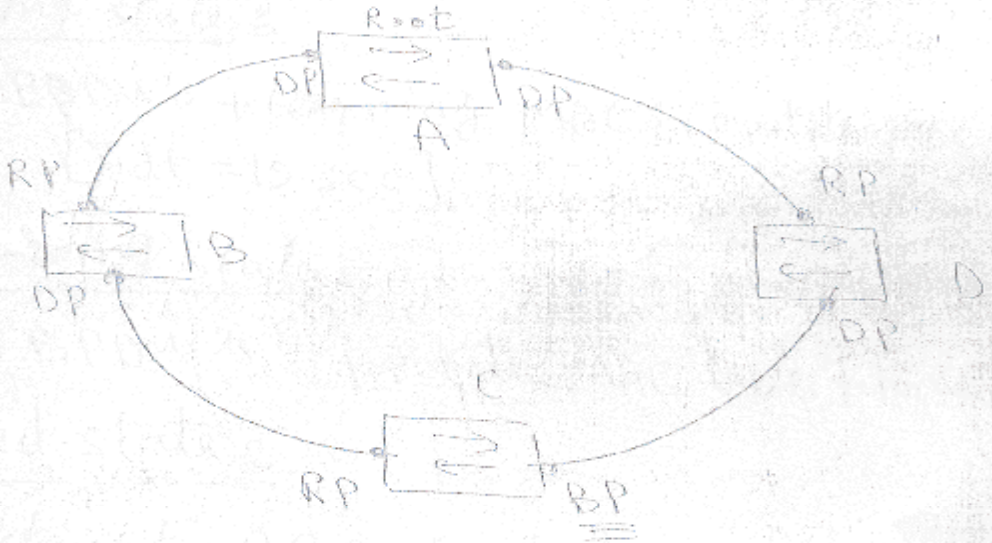
choice → > port with least accumulative cost → if equal → least sender Bridge ID

5) Determine Blocked port:

neither RP nor DP is the BP (Blocked port)

EX: assume that Bridge ID of

A < B < C < D



Notes:

- If 2 port's on same SW as shown The RP will be the port with least port ID
- one root Bridge / n.w
- one root port per non root sw's
- one designated port per segment
- neither RP nor DP is BP

STP operation states

① listening state:
Process only BPDU's, to elect root sw, RP, DP
→ Forward delay time = fdt = 15 sec

② learning state:
Process BPDU's + learning MAC's (Populate MAC table)
[Fdt = 15 sec]

③ forwarding state:
Process BPDU's + Populate MAC table + forward data

④ Blocked state:
only listen to BPDU's & drop any data
max aging time = 20 sec [to BPDU's]

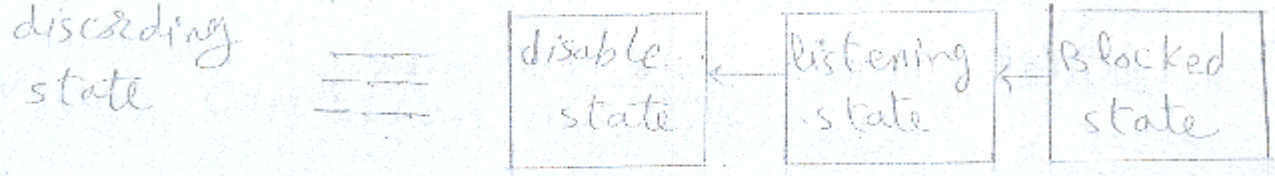
⑤ disable state:
Physical Blocking → disconnected cable
OR
→ port shut down

at change: The sw that sense a change send "BPDU-TCN" topology change notification to all sw's so all sw's erase BPDU data base & repeat The election process.

∴ convergence time = 30 → 50 sec $^{20+15+15}$

RSTP : "Rapid spanning tree protocol"

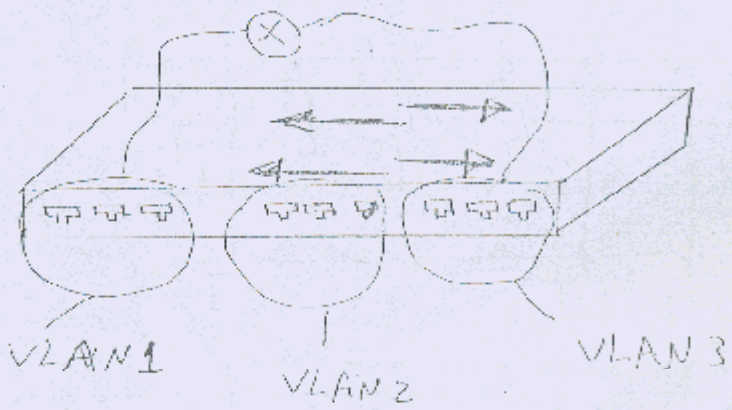
- RSTP speed the recalculations of spanning tree when N.W topology change
- for stp convergence time 30 → 50 sec
so it enhance the convergence time
- RSTP elects a back up port for each RP & DP
- RSTP merges the "blocked state + listening state + disable state" into one state called "discarding state"



DAY 13

CCNA track
Prepared by..
Eng: Ahmed Abdallah

"Virtual local area network" [VLAN]



VLAN's :

- The basic dic's of VLAN is to make multiple B.C domain by logically devide the sw into multiple independent sw's at L2
- VLAN Provide segmentation, flexability & security
- VLANS can span multiple sw's

VLAN membership

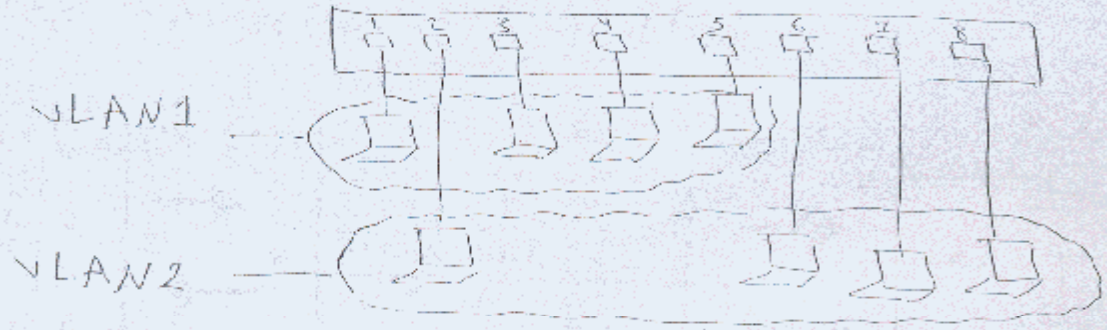
How make a PC member in a VLAN?

we have 2 ways

1 static membership:

- assign a certain port to a certain VLAN

"Port Based"

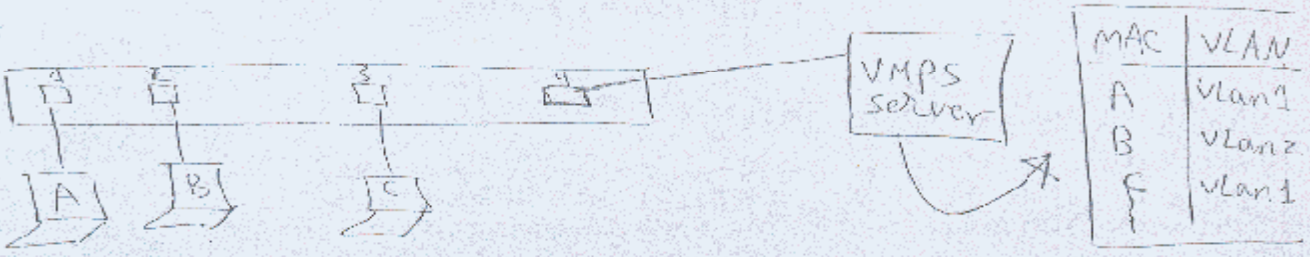


2 Dynamic membership:

assign a certain MAC to a certain VLAN

"MAC based"

By using VMPS "VLAN membership server"



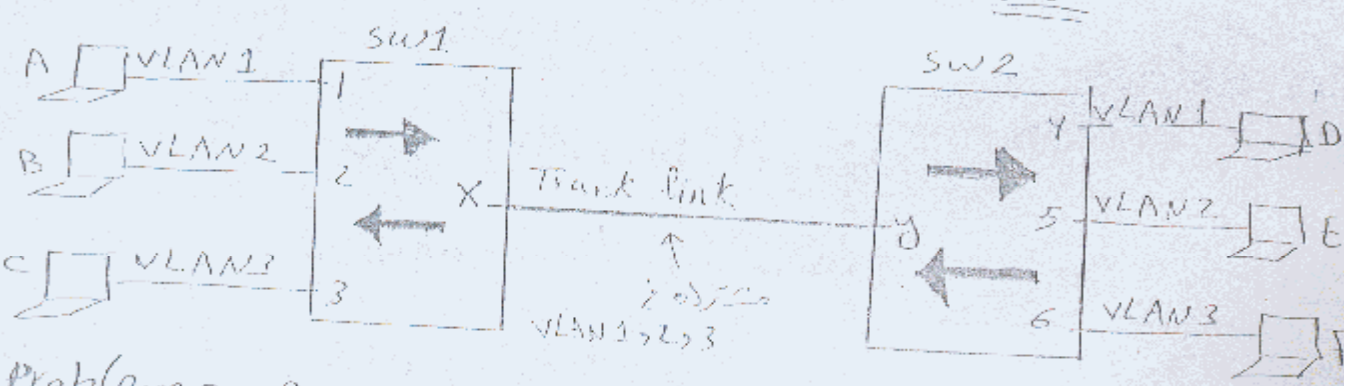
VLAN Port Connection type:

1) access Port: member in one VLAN

ex PC connected with sw

2) trunk Port: member in all VLANs

ex sw connected with another sw



Problem: if A send a broad cast frame from Port 1 sw1 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 PCs (to all VLANs in sw2)

solution: "Tagging" --> trunk add a field that identify the src VLAN ID to the frame

VLAN trunking methods

1- ISL "cisco proprietary"

2- IEEE 802.1q

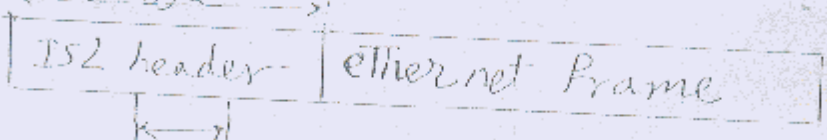
3- LANE → for ATM

4- IEEE 802.10 → for FDDI

---

1) ISL "inter switching link"

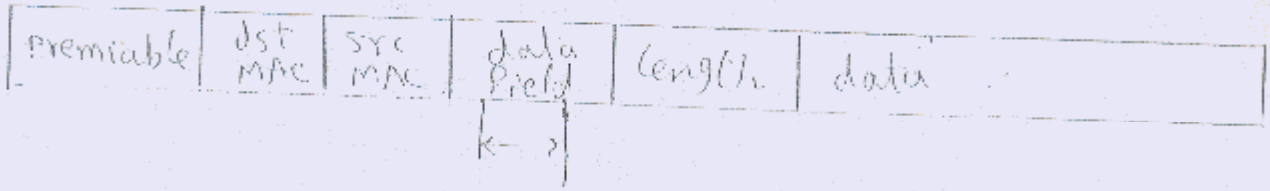
- tagging by 30 byte



---

2) IEEE 802.1q "dot1q"

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



VLAN1 is default ... [illegible] ...

VLAN & spanning tree

[1] CST "Common spanning tree"
one spanning tree for all VLANs

[2] PVST "Per VLAN spanning tree" "cisco proprietary"
one spanning for each VLAN

VLAN trunking protocol "VTP"

- overview: in large organizations managing VLANs on large number of switches is difficult
- VTP: cisco proprietary
  ↳ it is an easy administration method to transfer information about VLANs between switches in the same domain.
- VTP domains:
  - it is an area with common VLAN requirements
    "all sw's support same f° & policy"
  - sw can member in only one VTP domain
  - default VTP domain name is = "NULL"

VTP Ens : add, remove & modify for VLANs

note : steps to configure VLAN

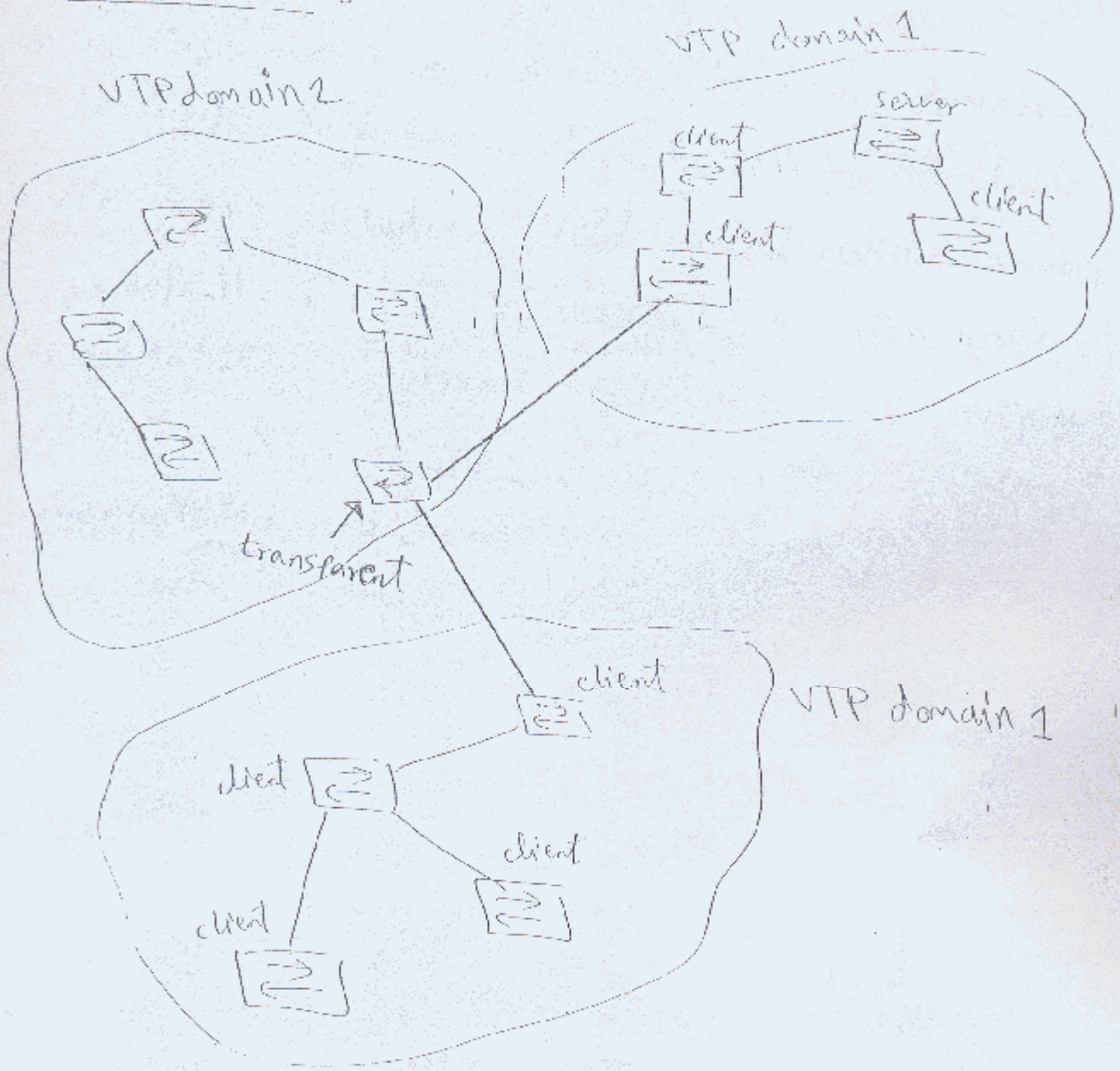
1- create VLAN
2- name VLAN [optional] → can be advertised by VTP msgs
3- assign ports to VLAN

switch in VTP domain can be one of 3 modes

1- server
2- client
3- transparent

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 msgs	✓ if server domain	✓	✗
• default VTP mode	✓	✗	✗
• save configuration	✓ save in NVRAM	✗ save in RAM	✓ in NVRAM

transparent :

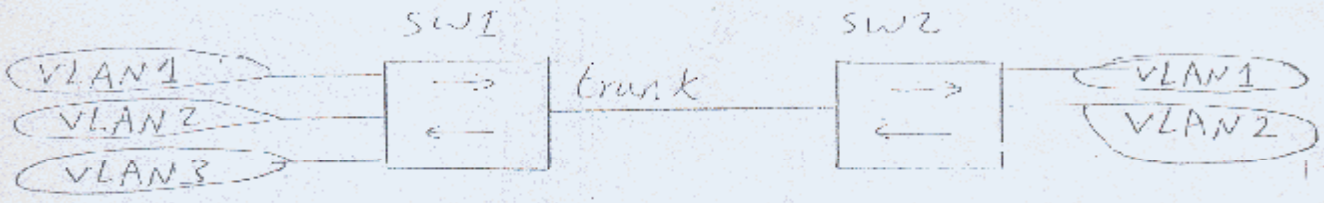


transparent sw :- هو sw مش بيعمل VTP (VTP domain) بس بيمشي الفلوس اللي جاية عليه عشان يوصل ما بين الـ 2 parts of VTP domain 1

hints

- in case we have 2 servers in same domain, VTP msgs go between them & will be affectable
- VTP msgs include a field called revision number "by default = 0" & it increases by 1 with each configuration command so, if any msg reach a sw with revision number < that on it, it will be forwarded with out being affected by it

* VTP Pruning *



Problem :

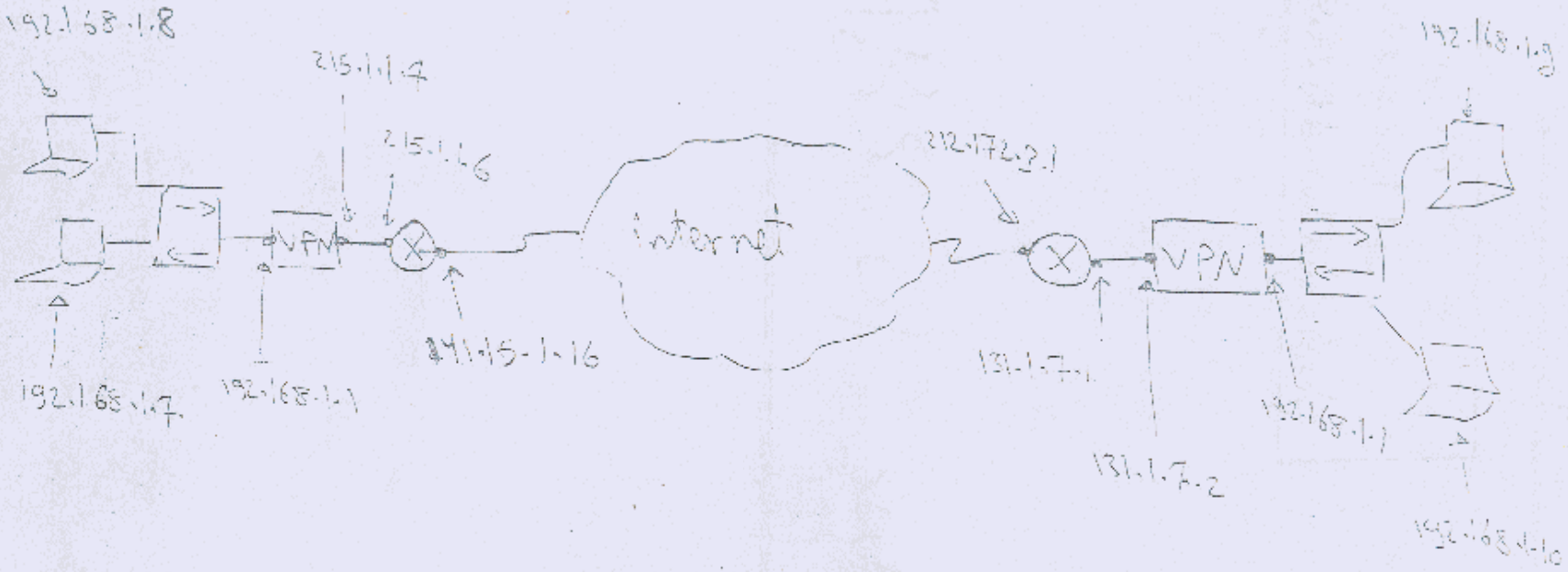
Although SW2 not contain VLAN3 so, if VLAN3 send broadcast, it will Path through trunk link to SW2 " link over head + tagging process"

Solution : => Pruning Process

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

↝ in This case all switches must be in server mode

VPN (virtual private network)



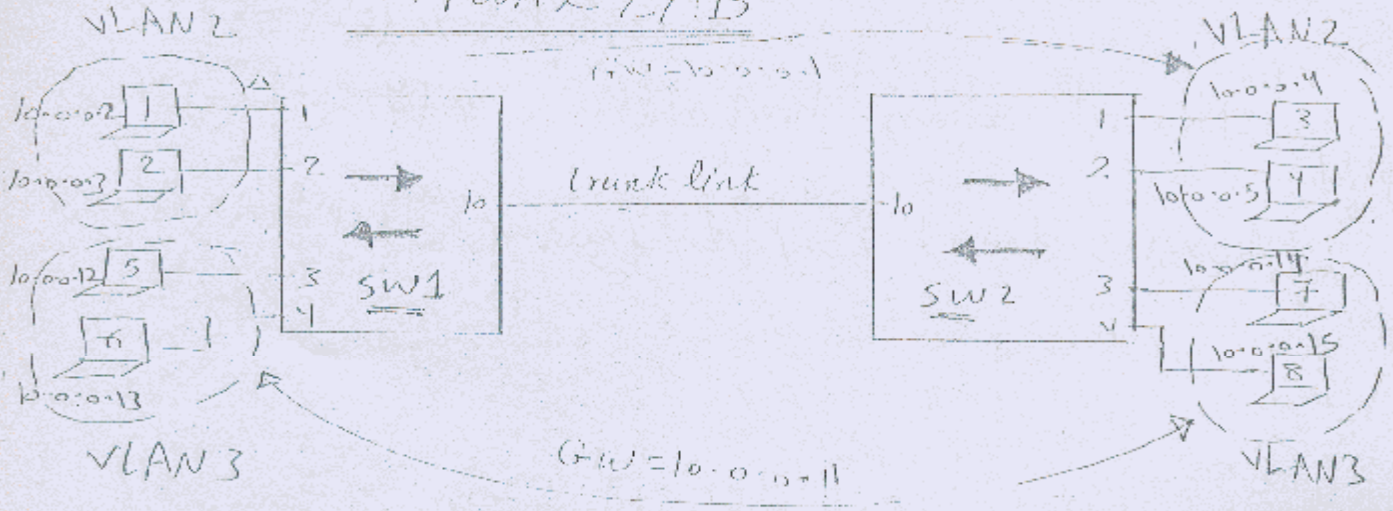
134

DAY 14

CCNA track
Prepared by
ENG: Ahmed Abdallah

LABS of switching

Trunk LAB




```
sw1(config)# VLAN 2
sw1(config)#VLAN 3        } to create vlan ② & ③
sw1(config)#int e1
sw1(config-if)# switch port mode ACCESS
sw1(config-if)# switch port access VLAN 2
```

int e2 كرر نفس الأوامر على

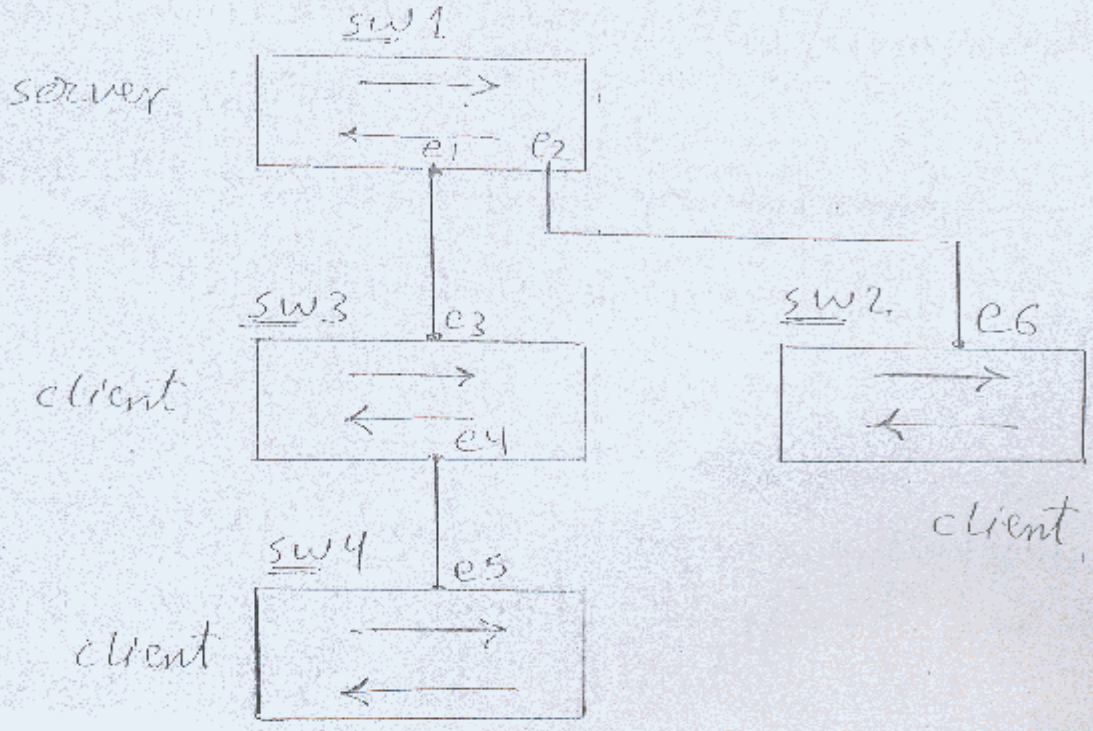
```
sw1(config-if)# int e3
if)# switch port mode ACCESS
if)# switch port access VLAN-3
```

int e4 كرر نفس الأوامر على

sw1(config)# int e1o
sw1(config-if)# switch port mode trunk
sw1(config-if)# switch port trunk encapsulation dot1q
ISL

كرر كل الخطوات السابقة على sw2 ثم
جرب ping على جميع PC4 & PC3 & PC2 & PC1
وستجد أيضاً PC8 & PC7 & PC6 & PC5

VTP LAB



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

٢- إذا أردنا إنشاء أكثر من VLAN غير الطبيعي أو نقل أي سويتش لـ

وأعرف بـ هذه الـ VLANs وتقلع في سويتشات Cisco الوضع تلقائي

٣- يجعل أحد هذه السويتشات في (server mode) والباقي في (client mode)

٤- إذا أردت عمل create أو delete أو modify لأي VLAN

على (server sw) وأوتوماتيك حتى يتم إرسال VTP msg إلى clients

فتقوم هي الأخرى بإضافة أي هذه الـ VLANs عندها

```
sw1(config)# VTP domain cisco
sw1(config)# VTP password 91
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 الأوامر السابقة على int e2

```
sw2(config)# VTP domain cisco
sw2(config)# VTP password 91
sw2(config)# VTP mode client
sw2(config)# int e6
sw2(config-if)# switch port mode trunk
sw2(config-if)# switch port encapsulation dot1q
```

وكذلك مع باقي السويتشات

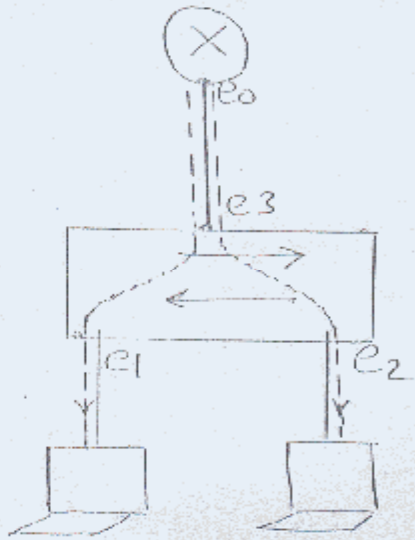
وننشئ أول VLAN على السيرفر (server) ونعطيها أي اسم

```
sw1(config)# VLAN 5 name SCC
```

ثم ندخل الأمر ← #show VLAN

على أي سويتش - وفي أي server أو client - وشوف عمل creation للـ VLAN 5 ذات الاسم SCC

Inter VLAN Routing



switch configuration

```
SW(config)# VLAN 10
SW(config)# VLAN 20
SW(config)# int e1
SW(config-if)# switchport mode access
```

trunk port(e3) بقية التعريفات لـ e2 و

Router configuration

```
R(config)# int e0.10
R(config-subif)# ip add 10.0.0.1 255.0.0.0
R(config-subif)# encapsulation dot1q 10   ← VLAN رقم
R(config-subif)# int e0.20
R(config-subif)# ip add 11.0.0.1 255.0.0.0
R(config-subif)# encapsulation dot1q 20   ← Vlan 20
```

الآن يجب أن يعمل Ping بين 10.0.0.2 و 11.0.0.2

نريد عمل telnet على السويتش من الراوتر

(config)# int VLAN 1
(config)# ip address ___IP___ ___sm___ ← هنا بكون الـ network اللي بدي اعمل telnet عليه

-to make Port security

(config)#switchport Port-security
-if)#switchport Port-security MAC-address ____
if)#switchport Port-security violation {shutdown / restrict / protect}

shutdown → if unknown MAC shutdown the port
restrict → if unknown MAC don't shutdown but (track) عدد الـ MAC اللي جاية
protect → if unknown MAC.
don't shut down & don't track

Trouble shooting

#show spanning-tree → to see spanning tree parameters

#show VLAN → show VLAN data base

#show VTP status → display VTP information on sw

#sh int switchport → يكتب اذا ما بدي ints كم بروتين access او trunk

#sh int fe0/3 switch port

access او trunk بدي اعرف (int fe0/3) البروتين الـ

DAY 15

CCNA track
Prepared by
ENG: Ahmed Abdollah

IPV.6 + wireless technology

IPV.6 :

- Longer address space "128 bit" → give 2^{128} IP's

+ IP V.6 Format:

- colored (:) hexa decimal form "8 X 4 hexa"

X : X : X : X : X : X : X : X

X = 4 hexa = 4 x 4 = 16 bit

- leading zero in a field is optional

FE10:0001:0005:BC23:X:X:X:X

= FE10:1:5:BC23:X:X:X:X

- successive zeros in a field are represented by :0:

ex

FE10:0000:0000:B22C:0000:X:X:X

↓

=FE10:0:0:B22C:0:X:X:X

- successive fields of zeros are represented by "::" & can be used once.

ex

F2BC:0000:0000:E456:0000:0000:0000:B22A

F2BC:0:0:E456:0:0:0:B22A

F2BC::E456:0:0:0:B22A → ①

F2BC:0:0:E456::B22A → ②

F2BC::E456::B22A → X

(2) ما ① ليش

IPV.6 Forms :

1- unicast address
- → "link local" : used with direct connected devices start with [FE80]
- → "site local" : Private address used in same site
- → "aggregate global" : "public IP"
- → "loop back" : "::1" (like 127.0.0.1 in IPV.4)

2- multicast address :
- start with "FF"
- From [FF00:: /8] → [FFFF:: /8]

3- Any cast : group of devices that have the same fns take same IP

4- Broad cast : ⇒ Not supported by IPV.6

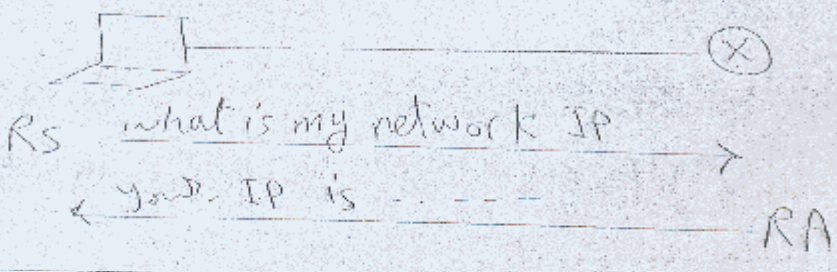
IPV6 Features:

[1] Auto configuration:

- we don't have DHCP, in this case the router can give the PC an IP address using:

1- Rs msg "Router solicitation"

2- RA msg "Router advertisment"



[2] Plug & Play:

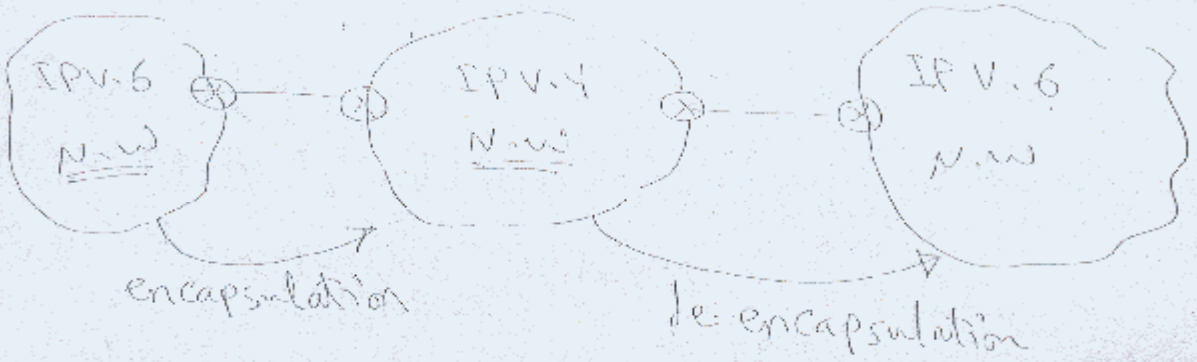
because we don't need DHCP server

[3] Renumbering & mobility: ability of changing the n.w devices IP's without manual reconfiguration

[4] Integrated security: use IPsec "encryption method" provide end to end security

[5] simple header than IPv4 "no fragmentation or CRC fields in the header"

IPV.6 to IPV.4 tunneling.



- tunneling is automatic with out configuration
- if the start of IPV.6 address = [2002: /16]
  make it tunnel through IPV.4 N.W

NATing:

cisco Routers can made natting on IPV.6

Routing: cisco Routers support Routing using IPV.6

ex (config) # int e0/1
if) # IPV6 ospf 1 area 0
if) # int solo
if) # IPV6 ospf 1 area 0

Dual stack

- Router understand both IPV.4 & IPV.6 / interface

(config) # int e0

(config-if) # IP address IPV.4 SM

(config-if) # IP V.6 address

(config) # IP V.6 unicast-routing

↳ enable router to support IPV.6 Routing

[2] wireless technologies

- Cisco buy linksys company to introduce wireless technology
- They use WI-FI technology to transmit the data in the air

Hint: Wi-Fi = IEEE 802.11 standered

There is many types of 802.11 standered

1- IEEE 802.11g

* freq. range = 2.4 GHz
* non overlapping channels = 3
* max data = 54 Mbps
* max distance with max data rate = 90-100 feet
* max distance running with lowest data rate = 300 feet

2- IEEE 802.11a

* freq. range ≈ 5 GHz
* non over lapping channels = 12
* max data rate = 54 Mbps
* max distance with max data rate ≈ 65-75 Feet
* max distance running with lowest data rate = 175 Feet

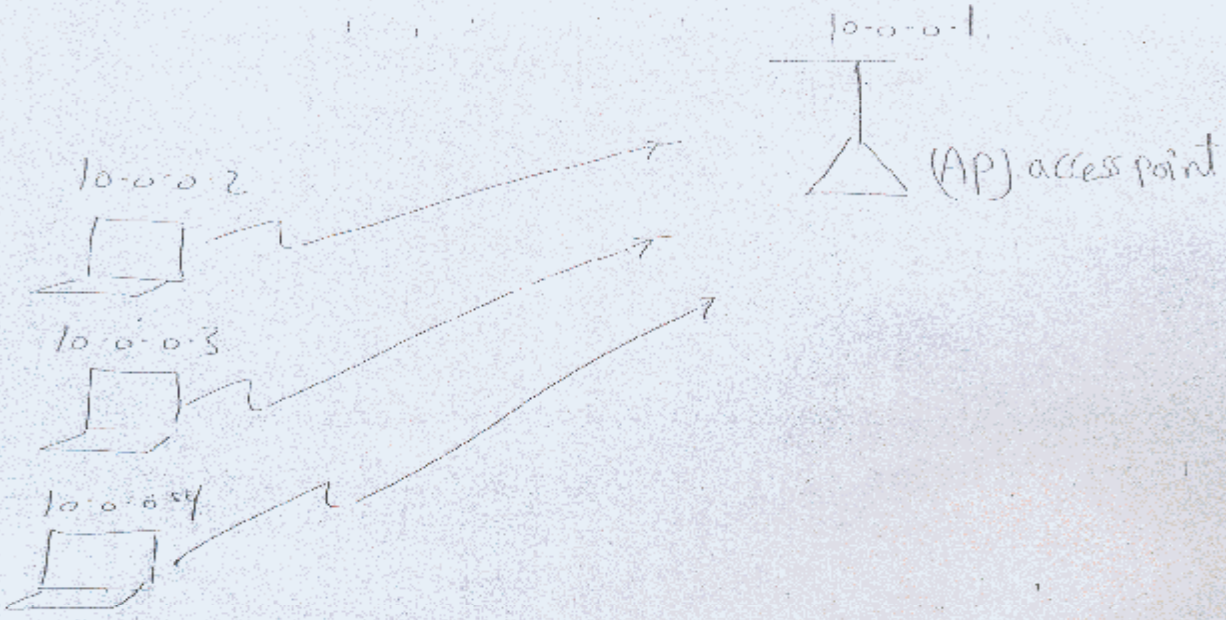
3- IEEE 802.11b

* freq. range = 2.4 GHz
* non over lapping chs = 3
* max data rate = 11 Mbps
* max distance with max data rate ≈ 150 feet
* max distance running the lowest data rate = 350 Feet

ملحوظة: كل التقنيات اللاحقة تدعم spread spectrum technology

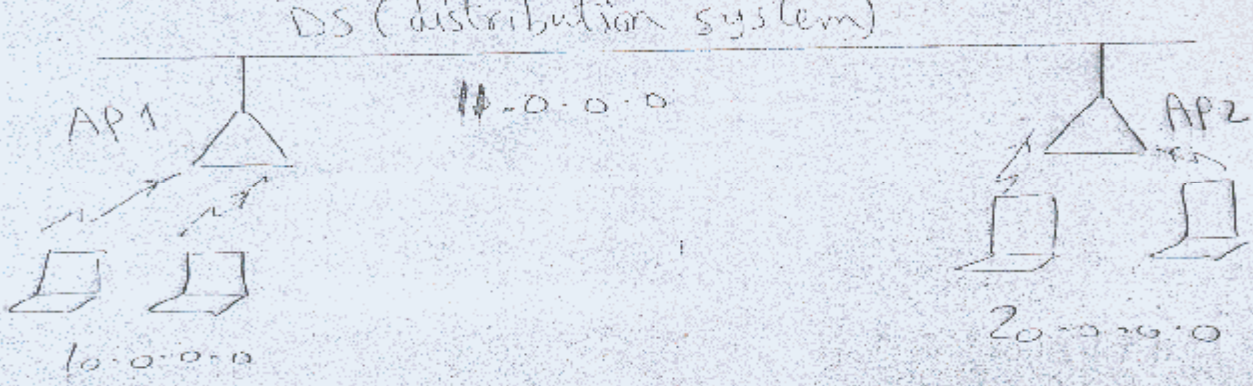
wireless transmission

① BSS (Basic service set)



- to connect more than one wireless network we use

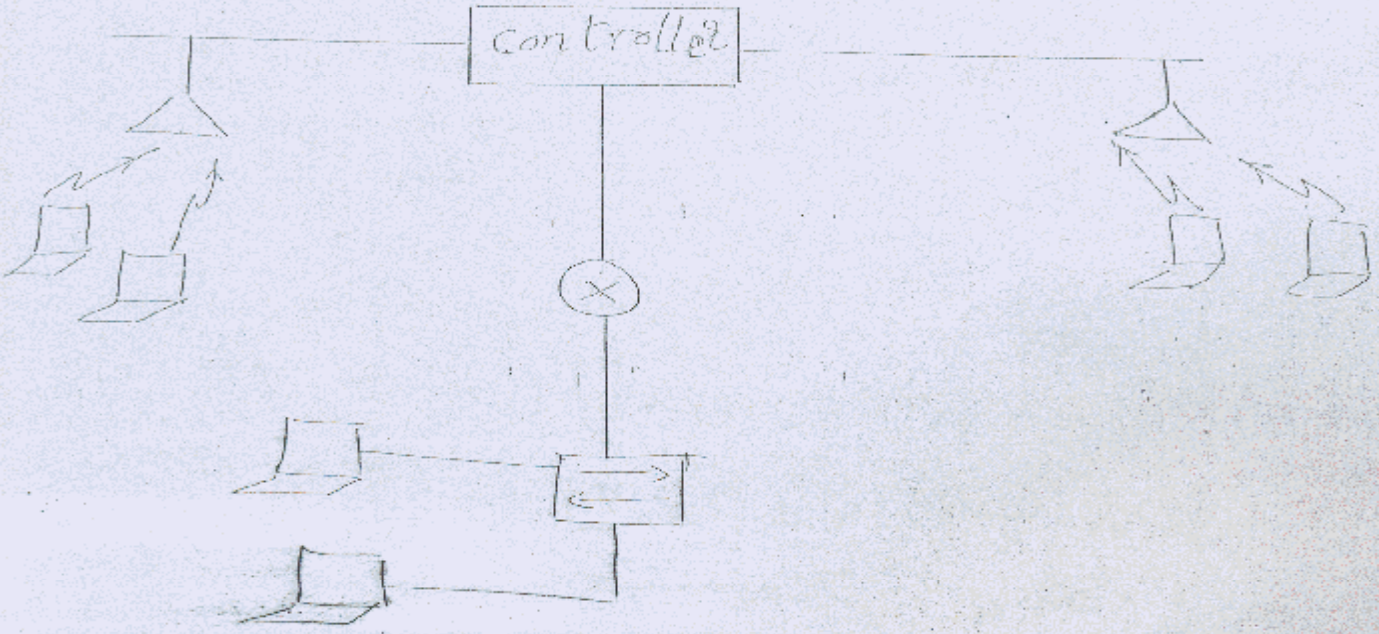
② ESS (extended service set)



AP1 & AP2 are configured to work on 2 different channels.

split MAC architecture

it use controller to connect between wire & wireless networks



wireless security :

① open Access :

No security & any one can access the Access point

(2) SSID [service set identifier]

SSID: is a common network name for the devices in WLAN system

- if any one want to connect to AP he should know the SSID

مشكلة الـ SSID : clear text على شكل

وبالتالي لو حد هاكر بيحب للعبث فعندما يأتي يحاول

يدخل الشبكة فلما الـ AP تكتشف الـ SSID

فرسل لـ الـ SSID كلمة واضح فيقوم الهاكر بترجمة الـ SSID

(3) Shared-Key authentication

text "Ahmed" → [WEP] → (in 128 bit) > encrypted code "oE1173HM3716"

challange text

WEP: wired equivalency protocol

- يتم أخذ الـ "challange text" وتشفيرة بمفتاح مشترك بين الجهاز والـ AP (access point)

- وتم عادت الشبكة مرة أخرى بالكود (clear text) يتشكل

4) client MAC addresses

(MAC addresses) وفيها نقوم بوضع الـ AP في الـ (MAC table) بتوبيز

الراد دخوله بـ AP

- وهذه الطريقة تعتبر أكثر وأقوى من الطرق السابقة

5) PSK (Pre-shared key)

- generate an encryption key for each packet of transmission data

- وهذه الطريقة تعتبر من "أكثر الطرق أماناً"

وهي الحالية بتستخدم في wi-fi

PSK + wi-Fi ⟶ WPA (wi-fi protected access)

WPA : (IEEE.11i)

DAY 16

CCNA track
Prepared by
ENG: Ahmed Abdallah

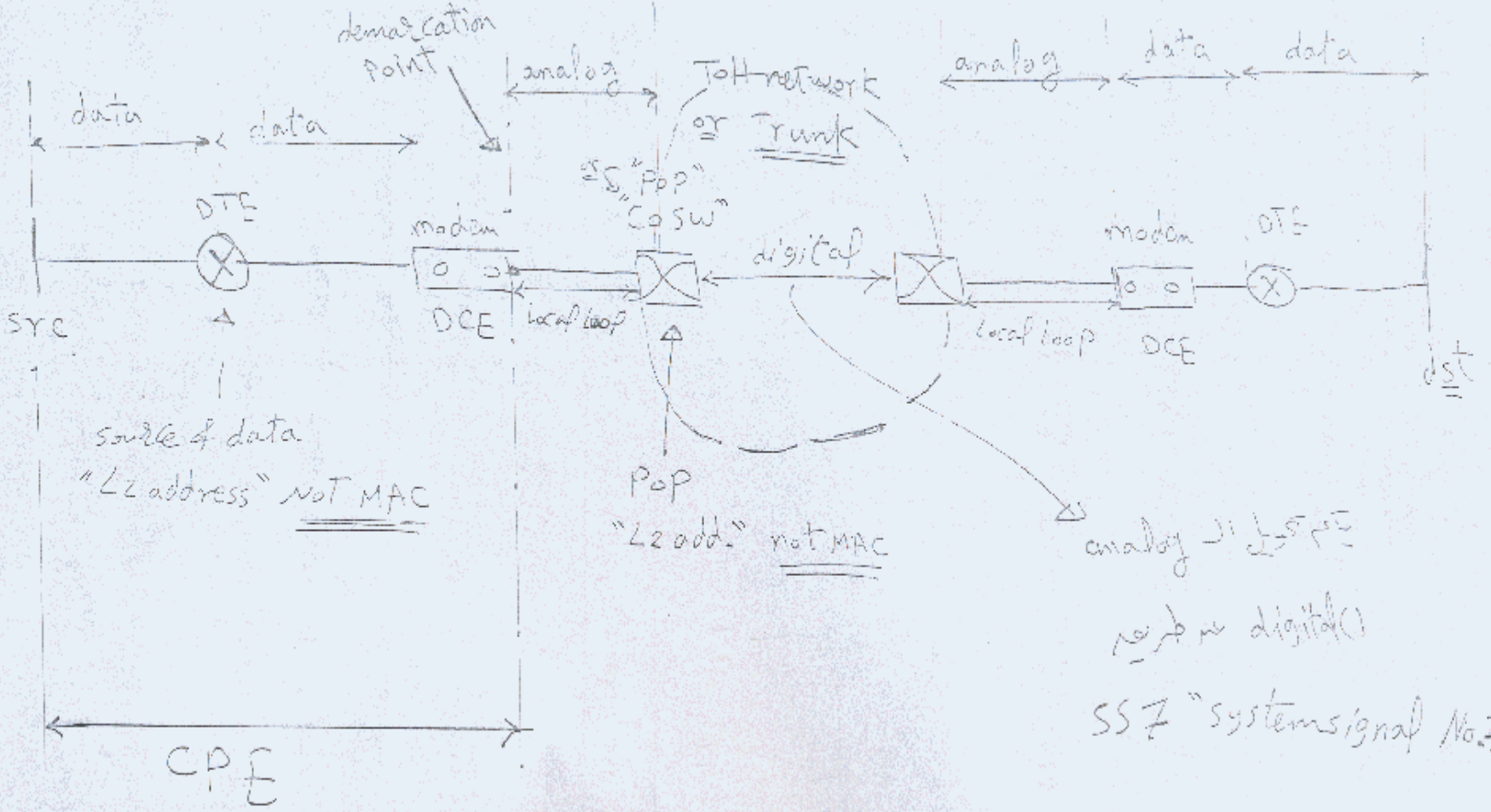
Introduction to wide Area network [WAN]

overview:

- WAN is a layer 2 technology works together with L3 protocols [Routing protocols]
- You don't own the WAN infrastructure
  "service provider (SP) & telephone company own it"
- WAN selection depends on: availability, BW & cost
- WAN connect remote sites extend your LAN over large geographical area
- WAN Thinking: L2 addressing + Hop to Hop data delivary
  ↑
  NOT MAC address

WAN connection termenologies:

- CPE → Customer Prices equipment
  "Your new equipment include DTE & DCE"
- DTE → data teminal equipment
  "end user device" or "src of data"
  ex [PC & Router]
- DCE → data communicating equipment
  Provide L1 framing, clocking, syncronization & connection termination
  ex: modem
- Demarcation point → logical boundary where responsibility of the carrier is passed to you
- Loocal loop → connection from Central office C.O.SW to demarcation point
- Central office switch "C.O.SW" → carrier SW that forward traffic based on L2 addressing "NOT MAC" [ex: PoP → Point of presense]
- TOLL network → trunk lines "infrastructure"


demarcation point
analog
ToH network or Trunk
analog
data
data
data
data
"5" "pop" Co SW
DTE
modem
digital
modem
DTE
SYC
DCE
local loop
local loop
DCE
dst
source of data
"L2 address" not MAC
PoP
"L2 add." not MAC
analog
digital
SS7 "system signal No.7"
CPE

154

WAN layer standards

- WAN is a layer 2 technology.

a) Layer 1 standards:

- Cisco routers serial ports are either → DB60 / → DB25 & connected to EIA/TIA232 & EIA/TIA449 & EIA530 and X.21 V.35

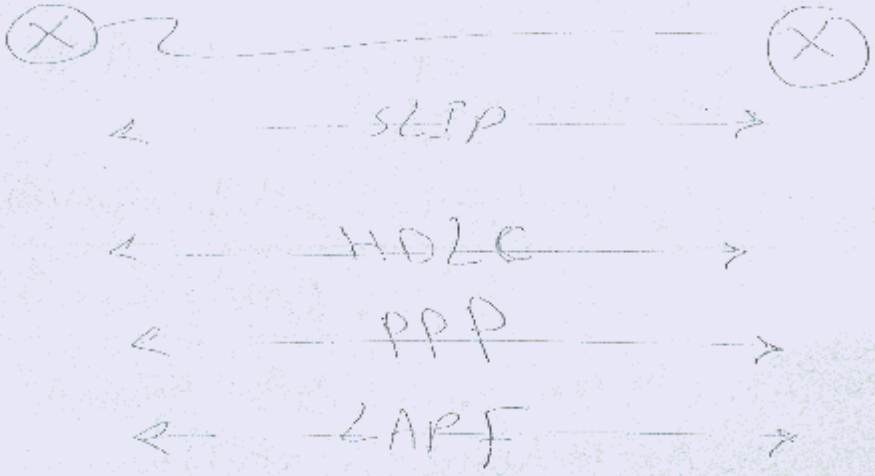
b) data link "L2" encapsulation standards:

- SLIP → "serial link internet protocol"
  - → Pt_to_Pt connection support only TCP/IP
  - → "earlier version"

- HDLC → "high level data link control"
  - → used for serial sync. connection

- PPP → "Pt_to_Pt protocol"
  - → support multiple protocol & link monitoring

- LAPF ⇒ "link access Procedure Frame relay"
  ↳ ⇒ used for Frame relay



---

* WAN Connection and related technologies

(1) Dedicated connection:

- Pre-established the link, available all the time with guaranted B.W
- used when → small distance
  → constant amount of traffic
- dis advantages ⇒ cost ↑↑
- WAN technology ⇒ leased line "synchronous serial line"
  - T1 — 1.54 M
  - T3 — 45 M

- WAN encapsulation ⇒ PPP, HDLC, SLIP

[2] Circuit switching:

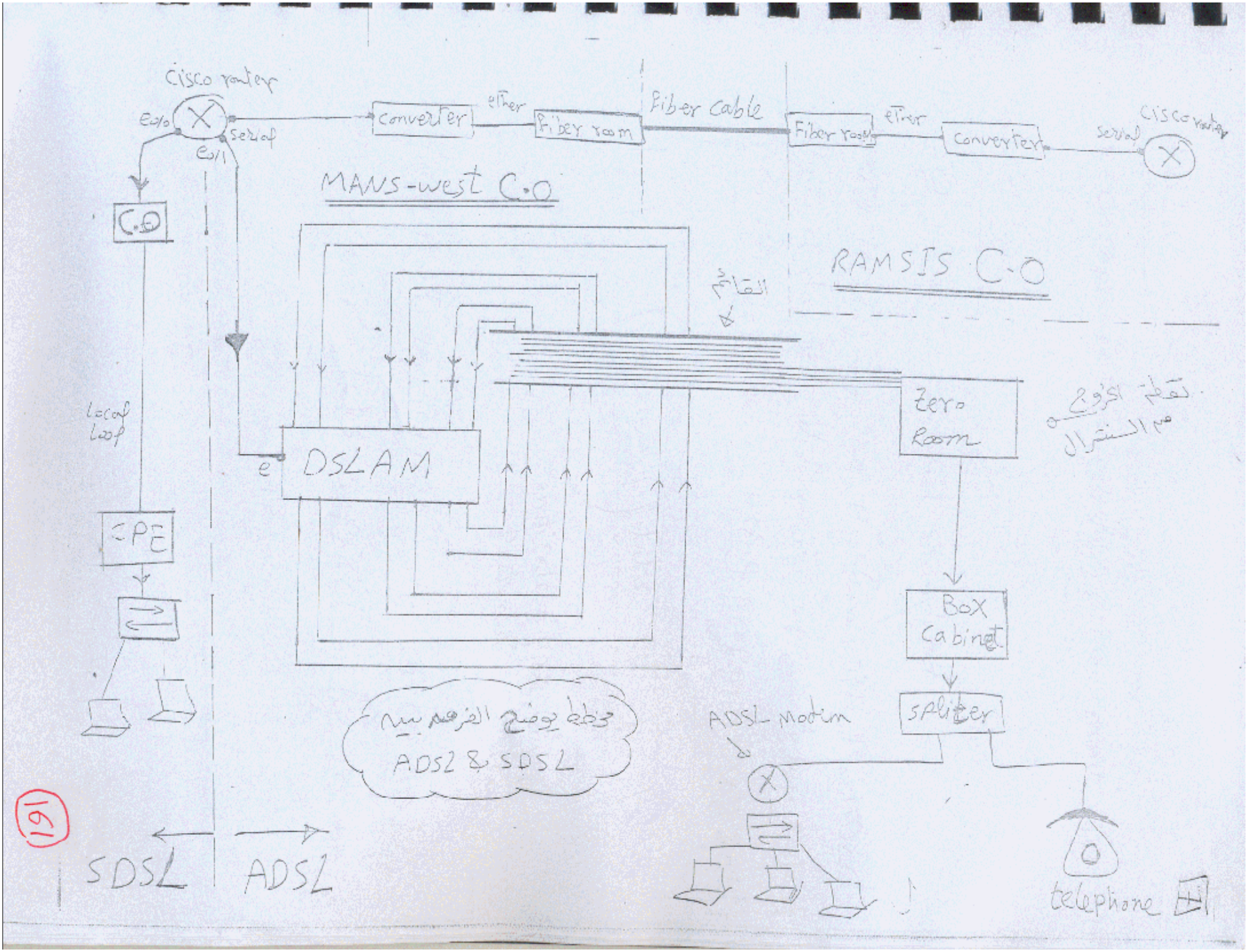
- link phone call must establish the connection before data transfer.
- WAN technologies → analog dialup "analog modem"
  → digital dialup "ISDN"
- WAN encapsulation → PPP, SLIP, HDLC, LAPD

[3] Packet switching:

- allow sharing of BW, use one physical connection to connect to multiple sites using VC "virtual circuits"
- WAN technologies → X.25
  → FR
  → ATM
- WAN Encapsulation → LAPB, LAPF, ATM

[4] Broad band connection:

- L1 technology use FDM [Freq. division multiplexing] which is convert Base band to Pass band
- technologies → satellite
  → wireless
  → cable modem
  → DSL
    - SDSL
      upload speed = download speed
    - ADSL
      - upload = ¼ or ½ download


Cisco router
Eth0
Serial
Eth1
converter
ether
Fiber room
Fiber cable
Fiber room
ether
converter
Cisco router
Serial
MANS-west C.O
RAMSIS C.O
C.O
local loop
DSLAM
Zero Room
CPE
Box Cabinet
Splitter
ADSL Modem
telephone
SDSL
ADSL
ADSL & SDSL

191

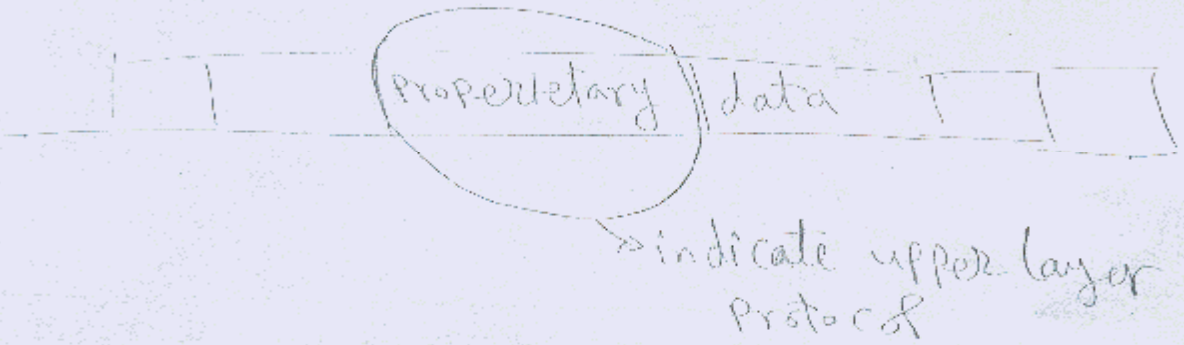
HDLC

- L2 encapsulation defines the frame type

HDLC types

① ISO HDLC → open standard

② Cisco HDLC - ▷ The problem with ISO HDLC is that it dosn't define the upper layer protocol [Cisco HDLC define it using proprietary field]



- Cisco Routers support only Cisco HDLC
- Non Cisco Routers support only ISO HDLC

configuration

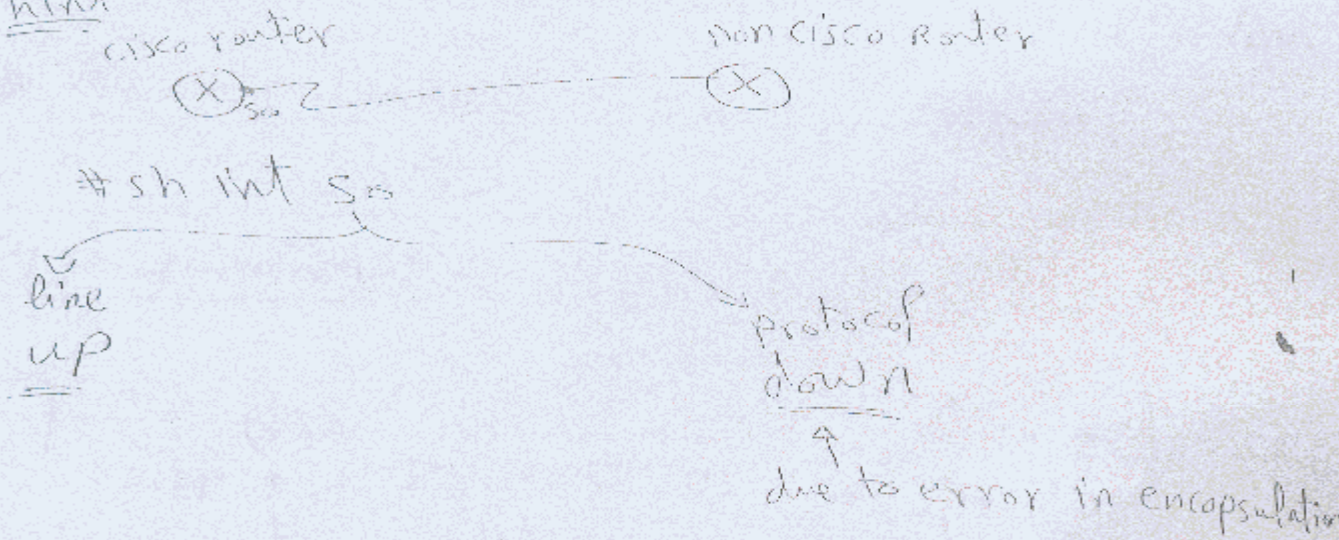
(config) # int s0

(config if) # encapsulation HDLC

Trouble shooting

show int s0

hint



Point to Point Protocol

- works with serial connection
- support multi vendor & multi protocol

- PPP main components

① LCP "link control protocol"

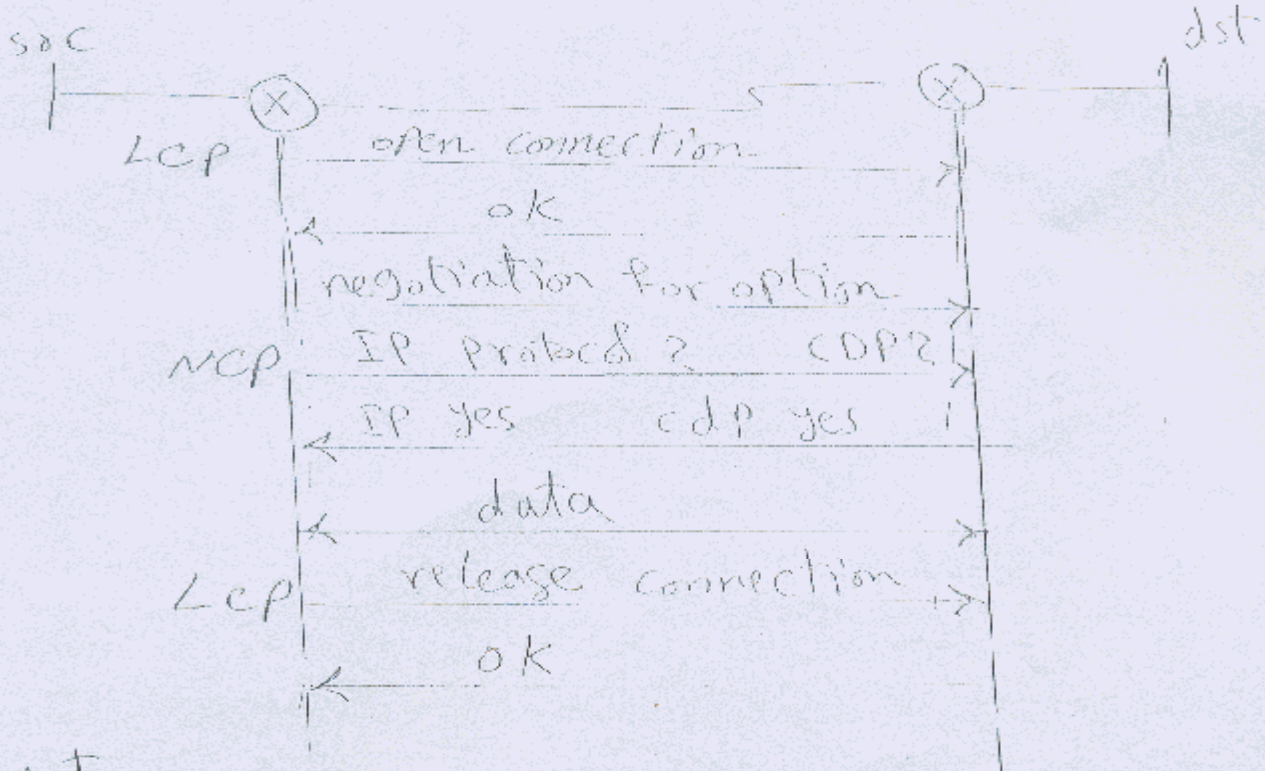
- Responsable for establish, close & maintain a PPP connection.

② NCP "network control protocol"

- Negotiate the upper layer protocol "IP, IPX, ..." & CDP that will be transmitted across PPP link

➪ The main difference between PPP & HDLC is the negotiation.

- PPP operation :



hint : NCP = IPCP If you work on IP protocol

PPP options

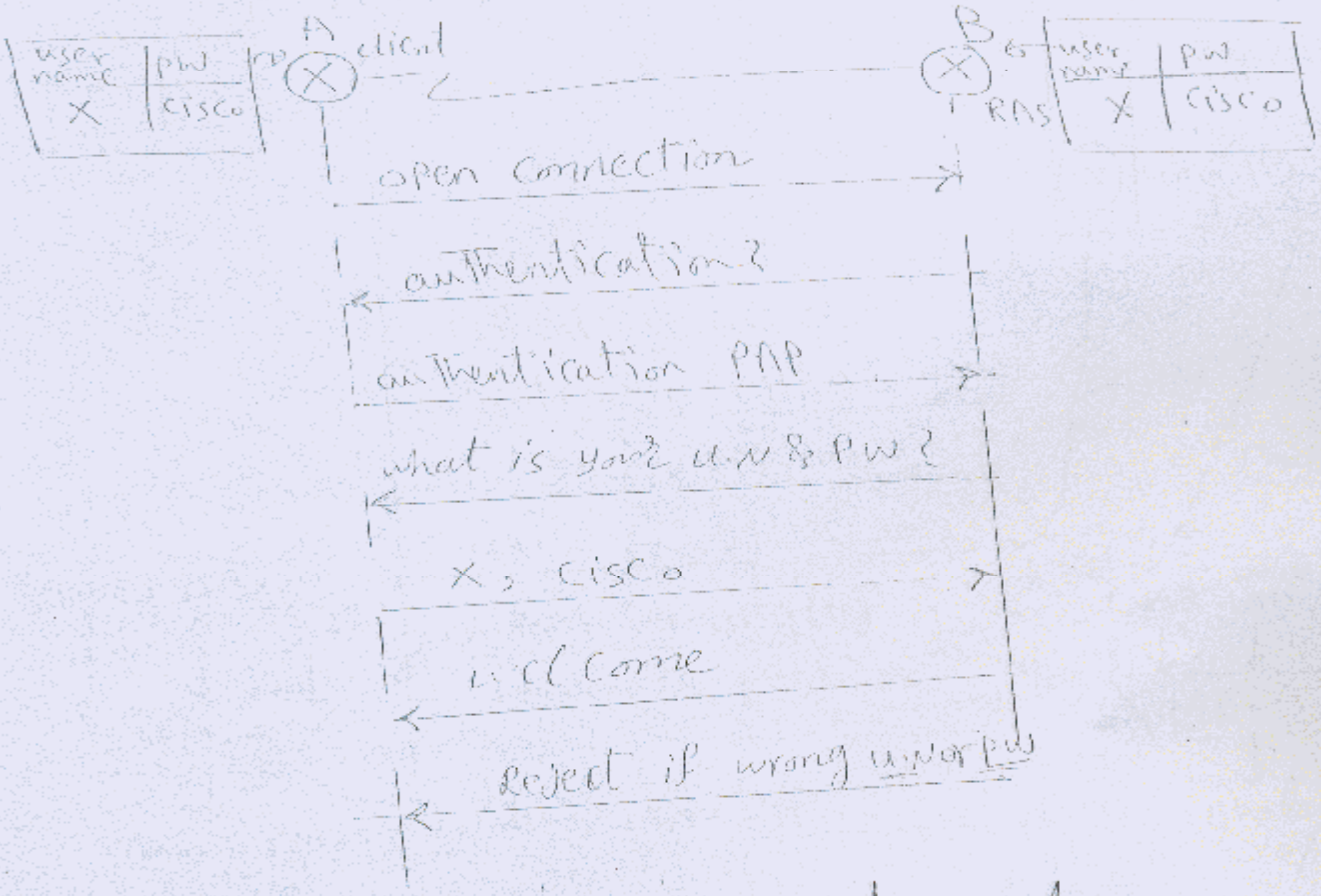
① Compression: to improve Throughput on slower-speed link, PPP support "STAC, Predictor, MPPC & TCP header" compression algorithms

② multi link: BW aggregation combine multi physical interfaces into 1 logical interface

③ authentication: using PAP or CHAP
↳ "user name + pw"

PAP : "PPP authentication Protocol"

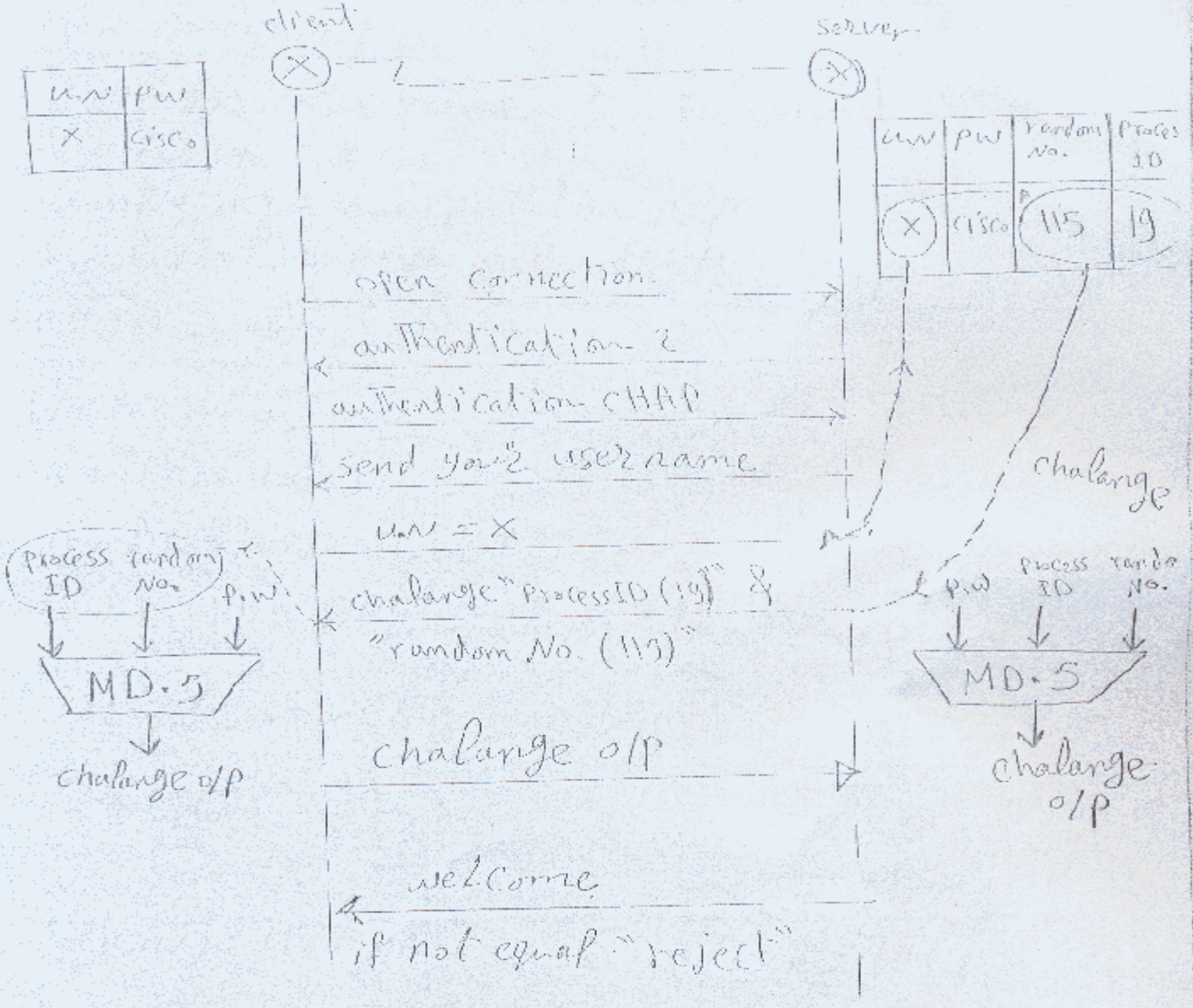
- 2 way hand shake = one way authentication between users (client & Router access server (RAS))



dis advantages : Password sent as a clear text

CHAP = challenge hand shake authentication protocol

- 3 way hand shake = 2 way authentication



MD-5 = message digest

PPP Configuration

R(config)# int S0
R(config-if)# encapsulation PPP

PAP configuration

(config)# username x password cisco
(config)# int S0
(config-if)# encapsulation PPP
(config-if)# PPP authentication PAP

CHAP configuration

(config)# username x password cisco
(config)# int S0
(config-if)# encapsulation PPP
(config-if)# PPP authentication chap

Trouble shooting

show int S0

opened: IPCP

protocol up

closed: IPCP

protocol down

DAY 17 [last day]

CCNA track
prepared by
ENG: Ahmed Abdallah

FRAME RELAT [FR]

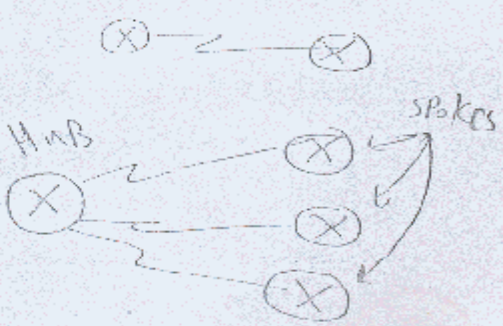
overview: it is a packet switching support multiple channels per one physical path using V.C "virtual circuit" ≡ "permit virtual circuit" (PVC)

⇒ Fast speed than VPN it can reach to 45 & 48 Mbps

- FR is connection oriented
- FR is L2 wan technology perform error detection & leave error correction to L4
- FR is NBMA "non broad cast multiple access"

topologies ⇒ PT_to_PT

⇒ Hub & spoke



note

NBMA → not support B.C & to make B.C

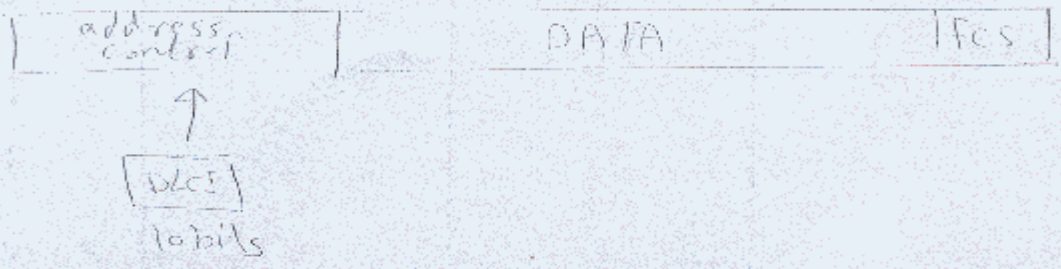
we can make multi unicast = replicated uni cast

unicast مثل ما بعمل مع الـ B.C بس بعمل لكل واحد

Frame relay components

1. LAPF

- represent the encapsulation "frame format" between 2 FR routers
- there are 2 types of LAPF { → cisco, → ietf



[2] DLCI No. "data link connection identifier" [3]

- used to identify virtual circuit ID [VCID]
- it is a unique local address "10 bits = 1024 DLCI address"

[3] FR Mapping's

making table between N.W address & DLCI No.

a) static FR Mapping : manually using configuration

b) Dynamic FR Mapping : using "inverse ARP"

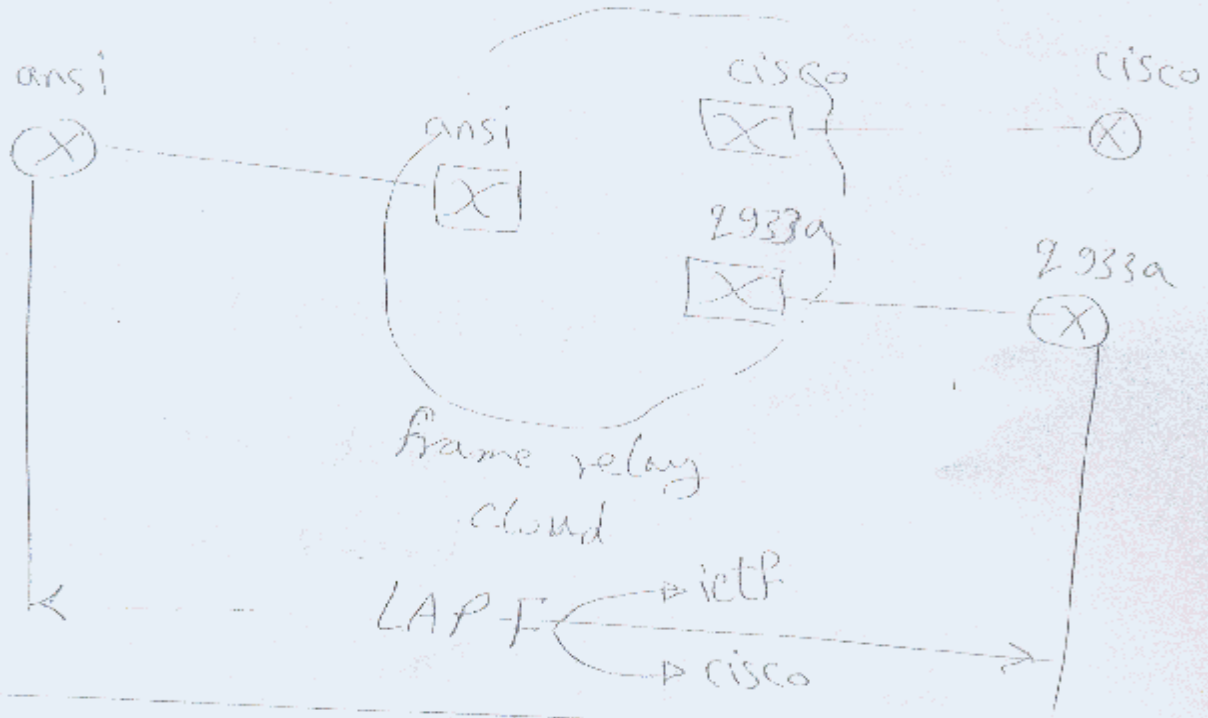
we have DLCI & we want IP

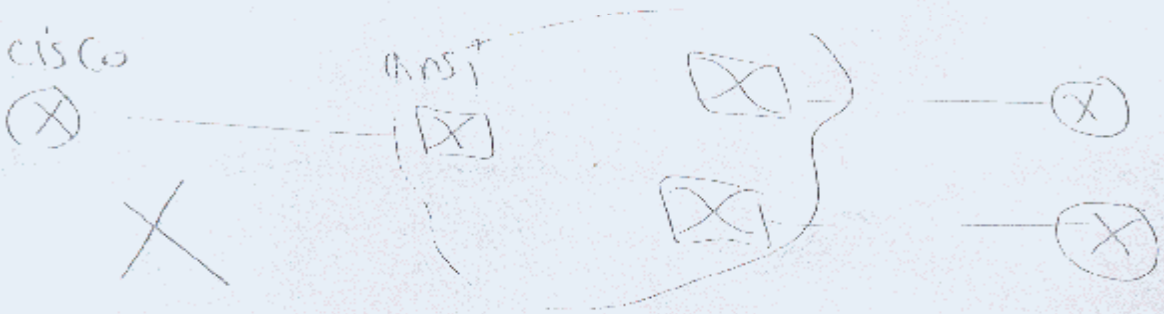
I/P port	I/P DLCI	O/P port	O/P DLCI	
1	100	2	20	11.0.0.0
1	200	3	30	12.0.0.0
3	30	1	200	10.0.0.0
2	20	1	100	10.0.0.0

1) LMI "Local management interface"

- describe & manage the interaction "language" between Routers & F.R sw

Types of LMI → ANSI
→ Q933a
→ CISCO





PVC status

- 1-active → PVC is up & ppl is normal

2-deleted → LMI not exchanged or misconfigured DLCI on local sw

- active → PVC is up

if ansi ↔ q933a

- status deleted

FR configuration

(config) # int s0

(config-if) # encapsulation frame-relay [ietf/cisco]

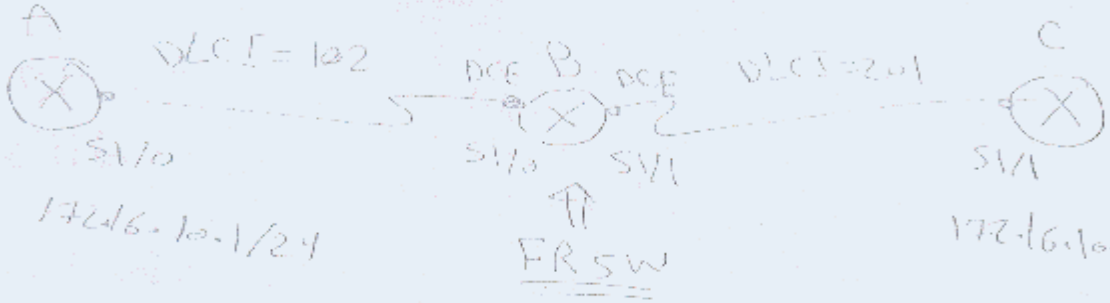
(config-if) # frame-relay LMI-type {ansi/cisco/q933a}

---

we have 2 LAB's on Frame relay

look at the next pages

LAB 1



FR sw على Router B الكلوب

FR ← تاخد DCE من B والوجه الثاني DCE. ليه؟

① Solution

```
B(config)# frame-relay switching
B(config)# int S1/0
B(config-if)# encapsulation frame-relay
B(config-if)# frame-relay intf-type dce
B(config-if)# int S1/1
B(config-if)# encapsulation frame-relay
B(config-if)# frame-relay intf-type dce
```

(2) route making + putting DLCI

```
B(config)# int s1/0
B(config-if)# frame-relay route 102 int s1/1 201
B(config-if)# int s1/1
B(config-if)# frame-relay route 201 int s1/0 102
```

(3) Router A

```
A(config)# int s1/0
A(config-if)# encapsulation frame-relay
A(config-if)# ip address 172.16.10.1 255.255.255.0
A(config-if)# no shut
A(config-if)# frame-relay interface-dlci 102
```

(4) Router C

```
C((config)# int s1/1
C(config-if)# encapsulation frame-relay
C(config-if)# frame-relay interface-dlci 201
C(config-if)# no shut
C((config-if)#IP address 172.16.10.2 255.255.255.0
```

⑨ تحكم تغيير LMI

(config-if) # frame-relay lmi-type ansi / cisco / q933a

Trouble Shooting

sh frame-relay lmi ← لرؤية نوع LMI المستخدم

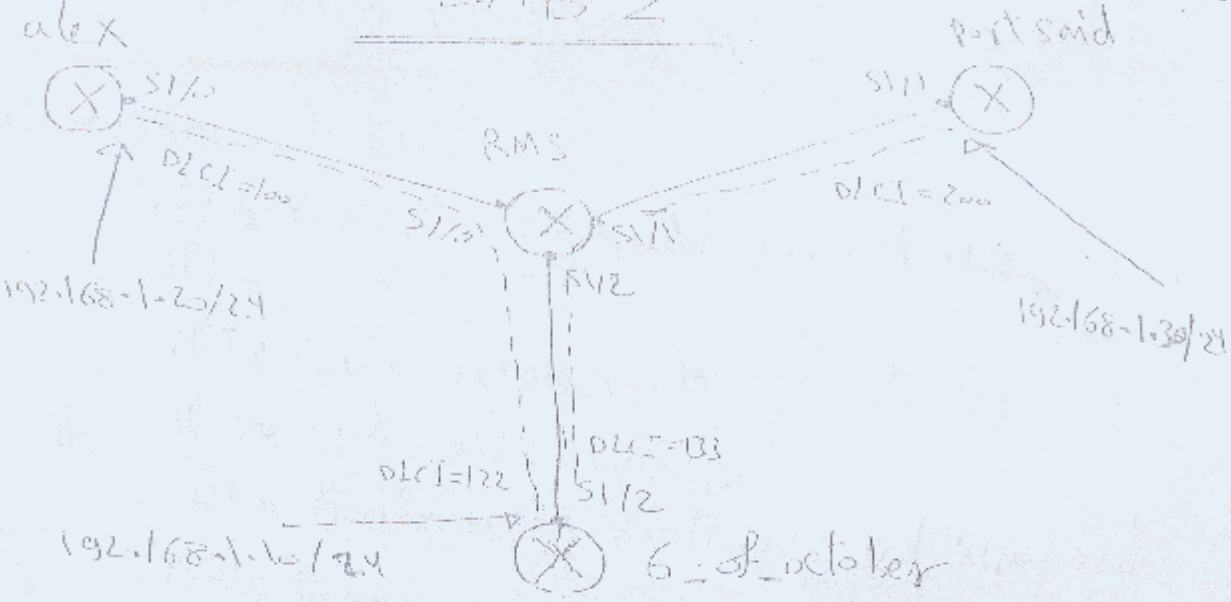
sh frame relay pvc ← لرؤية الـ (DLCI No.) الموجودة في الـ Ints

sh frame-relay route ← لرؤية

① i/p interface & I/p dlci

② O/p interface & o/p dlci

LAB 2



we want to make RMS Router act as FRSW

soh

```
RMS(config)# frame-relay switching
RMS(config)# int S1/0
 -if)# encapsulation frame-relay
 -if)# frame-relay intf-type dce
 -if)# int S1/1
 -if)# encapsulation frame-relay
 -if)# frame-relay intf-type dce
 -if)# int S1/2
 -if)# encapsulation frame-relay
 -if)# frame-relay intf-type dce
```

5) 6_of_october Router

6_of_october(config)# int s1/2

-if) # encapsulation frame-relay

-if) # IP address 192.168.1.10 255.255.255.0

-if) # no shut

-if) # frame-relay interface-dlci 122

if) # frame relay interface-dlci 133

عشان وضح أكثر ممكن dlci لأ مختلف لكل

وأيضاً لازم تحدد الـ LMT

(config)# frame-relay lmi-type {ansi/cisco/q933a}

& you can make trouple shooting

look at Page [91]

مع تمنياتي لكم بالتوفيق والنجاح والسداد

م/ عبد الله