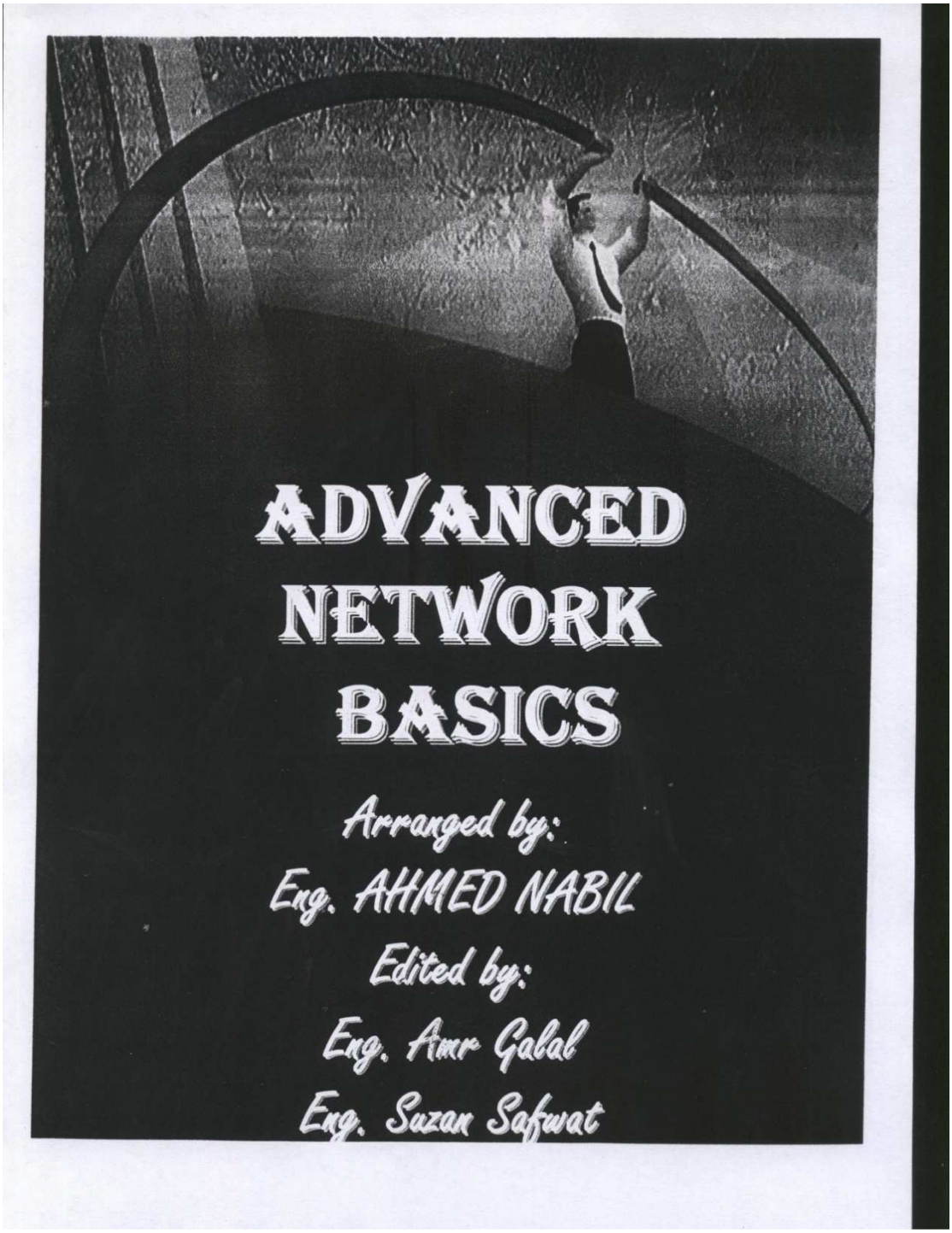


ADVANCED NETWORK BASICS

Arranged by:

Eng. AHMED NABIL

Edited by:

Eng. Amr Galal

Eng. Suzan Safwat

(I)

Acquaintance

What is Cisco? Cisco is from San Francisco & it was founded in 1984 by a small group of computer scientists from Stanford university.

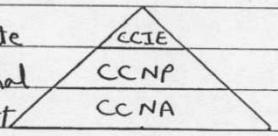
- Cisco
  - → H/w (Network devices) ⇒ very complex
  - → S/w

Introduction to Cisco Certificates

Standard Model

Network Implementation

CCNA : Cisco Certified Network Associate
CCNP : Cisco Certified Network professional
CCIE : Cisco Certified InterNetwork Expert
(between)



CCNP → 4 Certificates ≡ 4 Exams to be CCNP Certified

- → Routing
- → Switching
- → Remote Access
- → Trouble Shooting

(II)

DATE
DAY

Network design : Not famous in egypt

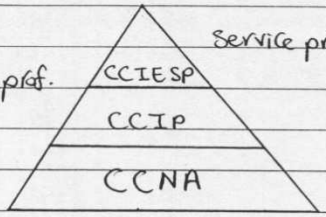
CCDA : Cisco Certified Design Associate

CCDP : Cisco Certified Design professional

Service provider

CCIP : Cisco Certified InterNetwork prof.

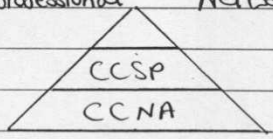
- BGP
- MPLS
- QoS



Network Security

CCSP : Cisco Certified Security professional

- h/w firewall
- VPN
- IDS



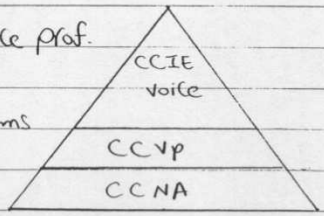
VPN : Virtual Private Networks

IDS : Intrusion Detection Systems

Voice :

CCVP : Cisco Certified Voice prof.

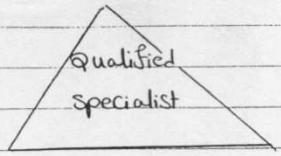
- 6 Certificates = 6 Exams



(III)

Qualified Specialist

In ATM / wireless LANs



How to be Certified ?

CCNA

take exam 640 - 801
60 → 70 questions
- → MCQ (55 → 60 Q)
- → drag & drop
- → Simulation (1 → 2 Q)

75 → 100 marks
max-score : 1000 marks
passing score : 850 marks
Solve "pass4sure" first = 370 Q
exam duration : 2 hours
fees : 84 English pounds
or 165 dollars
or 1000 L.E

take 2 Exams

Introduction + ICND
(640-821) (640-811)
50 → 55 Q the same as
1.5 hours
passing score 850
fees : 750 L.E

ICND : Inter connecting Cisco Network Devices

List of contents

PAGE
DATE

CCNA Course Content

1 - Network Introduction
2 - TCP/IP Model
3 - Data link layer
4 - Internet layer → IP Addressing
5 - Transport & Application layer
6 - Routers & Switches (S/w & H/w)
7 - Routing protocols
8 - Security (Access control lists)
9 - Switching
10 - Remote Access (WAN technologies : ISDN, FR, DSL)

Session 1
17/4/2006

CCNA Course

Topics — Introduction to Networks

- Network
- Importance of Network
- Network Components
- Network topologies
- logical vs physical topologies
- Network types

Network : Group of components or devices connected together to give the user a certain service (Application)

Importance of Network : (1) Easy sharing of files & Information.
(2) Sharing of expensive devices ex:- Servers – printers
(3) Modern tech. (VoIP – Video conferencing – Netmeetings)

Network components :

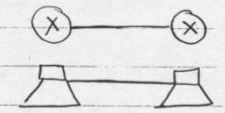
(1) PC : Source of Network aware Applications ex:- browsing – downloading files – sending & receiving mails
⇒ we use some sfws loaded on PCs & Servers to make these Network aware applications ex:- HTTP (HyperText Transfere Protocol) ⇒ browsing
FTP (file Transfere Protocol), SMTP (Simple Mail Transfere Protocol) ⇒ to send mails, POP3 (post office Protocol 3) ⇒ to receive mails,
Telnet Application :- for remote login certain device for setup & configure some sfws on it (equnt)

(2) Network Devices :
Hub ⟷, modem ○○, Switch ⇄, Router ⊗, Repeater ☰
NIC (Network Interface Card), bridge

(3) Connectivity : Cables – wireless

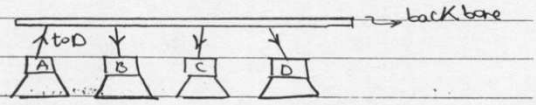
Network Topologies

(1) Point-to-point



ex:- leased lines, ISDN
Analog dial-up

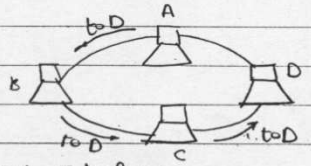
(2) Bus Topology



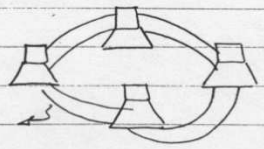
⇒ if A wants to send a msg to D then this msg will be sent to All PCs but D only will accept it

ex:- Ethernet 10Base5 → 500m, 10Base2, 10BaseT → twisted pair
10 Mbps, Baseband (no modulation & data will remain digital from $T^x \rightarrow R^d$)
way of comm. between devices close to each other.

(3) Token Ring

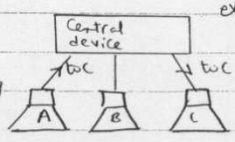


⇒ Sending only in 1 direction
⇒ very Slow
ex:- Token Ring
FDDI (fiber distributed Data Interface)
↳ use 2 Rings



one is used as backup

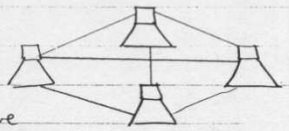
(4) Star topology



ex:- Ethernet
Token Ring

⇒ 1 smart central device will receive msg from src & directs it to the proper dst.

(5) Mesh Topology -



each PC is connected to all other PCs, there is redundancy due to Multi backups

ex:- ATM, FR, Ethernet

physical vs logical topology -

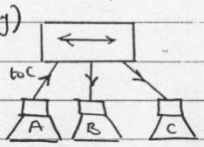
physical topology : How the devices are physically cabled or wired.

logical topology : How the devices communicate internally OR How the internal circuits behave or think.

(ex 1) Ethernet 10Base T Hub (Dummy)

physically → Star

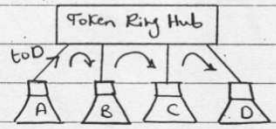
logically → Bus



(ex 2) Token Ring Hub (data from port n $\xrightarrow[\text{to}]{\text{sent}}$ port n+1 if it's not the port's msg)

physically → star

logically → Token Ring

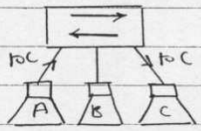


(ex 3) Ethernet switch (Smart)

physically → Star

logically → Star, Mesh

p-p

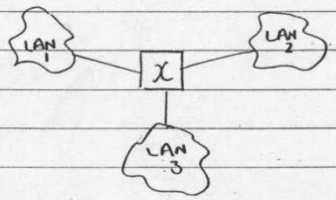


Network Types

(1) LAN (Local Area Network) : connection between devices near to each other without using central office

ex : Token Ring – FDDI – ATM (Asynchronous Transfere mode) (upto 40 Gbps)
Ethernet 10Mbps
Fast Ethernet 100Mbps
Giga Ethernet 1Gbps
10 Giga Ethernet 10Gbps (used in core Network)

(2) MAN (Metropliton Area Network) : connection between groups of LANs over a small area within city like Cairo



ex :- ATM (using fiber cables) ≤ 40 Gbps

(3) WAN (wide Area Network) : connection between groups of LANs over a large Area (continets - countries)

ex :- FR – ISDN – X.25 – Analog dialup – ATM (155Mbps – 622Mbps)

session (2)
13/4/2006

Topics

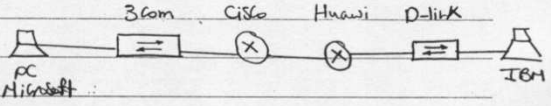
- Network Models (OSI Model - TCP/IP Model)
- Typical Network Topology

Model : Set of Rules & Regulations .

Why Model is layered : Because Any layer can't perform its fn unless it uses All the down Stream layers

Importance of the Model :

(1) Vendors Interoperability
« Standardaization »



(2) Better under standing of data transfere

OSI Model (open System Interconnection Model)

⇒ Educational Model developed by ISO & No longer used as the Sws on PCs & Sws on Network devices (Routers/Switches) used TCP/IP Model .

⇒ In Incoming discussion for OSI Model we'll use examples from TCP/IP Model

L7 Application layer

It is the S/w on our PCs that is used to represent a user interface to the Network & so aids the user to make Applications like browsing, Telnet, FTP

L7	Application layer	S/w
L6	presentation layer	S/w
L5	session layer	S/w
L4	Transport layer	S/w & H/w
L3	Network layer	S/w & H/w
L2	Data link layer	S/w & H/w
L1	physical layer	S/w & H/w

L6 presentation layer

- used to represent the data in aproper format .

ASCII → Text , Avi, mpg → vide , JPG → pictures

Internet explorer , Netscape → make some fn's of the presentation layer .

N·B Layer 6 & layer 7 are highly contingent to each other, because if there is a user interface this means that L6 represents the data in the proper format

L5 session layer : It is responsible for

(1) To be sure that all information required for opening a session (connection) is available this inf. like : src/dest. addresses, filesize, filename, ...

(2) Give orders for : Establishment of session
Management of session
Termination of session

session ⇒ may be browsing, downloading files

L4 Transport layer : It is responsible for actual Mechanics

(1) Establishment of connection

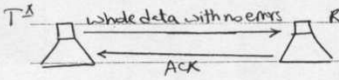
(2) Termination of connection

(3) Management of connection

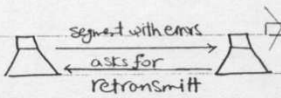
(3·1) Segmentation : The whole data is divided into small segments sent one by one & so if one segment has an error, we will resend this segment only & not the whole data

(3·2) Sequencing : Each segment is given a sequence no. so that we can reassemble our data in a proper way at the dest.

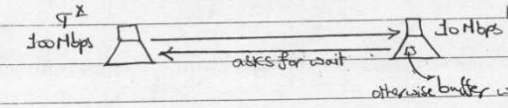
(3·3) End-to-End check : If the whole data is received correctly the dest. will send an Acknowlegment to the src.



(3·4) Error detection & correction : If one segment is received with errors the dest. will discard it & asks the src to retransmit it.



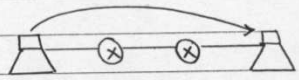
(3-5) Flow control : dest. controls the src transmission.
If the src transmits @ a higher rate than that the dst can receive, the dest. will ask the src to wait, otherwise the buffer of the dest. will be overloaded & all other segments will be discarded.



examples from TCP/IP Model for this layer
- TCP (Transfere control protocol)
- UDP (user data gram protocol) ⇒ used with voice & video

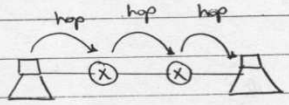
⇒ The whole mission of this layer is to make « End-to-End QoS »

L3 Network layer : It is responsible for



(1) End-to-End delivery.
(2) logical Addressing (unique Address for each device) (final End Addressing)
ex:- IP Address ⇒ IP_{v4} Protocol, IPX
Appletalk add. → Appletalk protocol in some private networks.
(3) Routing (Chossing best path to destination) ex: OSPF, Eigrp

L2 Data link layer : It is responsible for

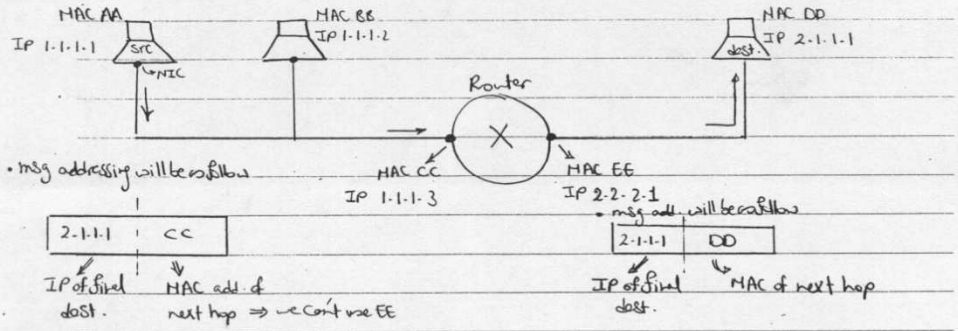


(1) Hop-to-hop data delivery.
(2) MAC Addressing (hop-to-hop Addressing)
(3) Hop-to-hop error detection
(4) Hop-to-hop flow control

hop → hop (rear) → Ethernet, FDDI
hop → hop (for Router → Router)
WAN tech : FR, ATM, X.25, ISDN

L1 physical layer : It is responsible for all physical properties of the network
(1) Cable lenght (2) Cable type (3) bit rate (4) voltage levels
(5) H/w Interface types : RJ45 (Ethernet), DB-21 / RS 232 / RS 449 (WAN)

example to show difference between IP & MAC Addresses



N.B : - Each Interface in the Router has a MAC & IP

- Data in the Router will travel from 1 interface to another without Addressing
- for telnet Applications to configure the router, the scr will use dst MAC CC & IP either 1.1.1.3 or 2.2.2.1

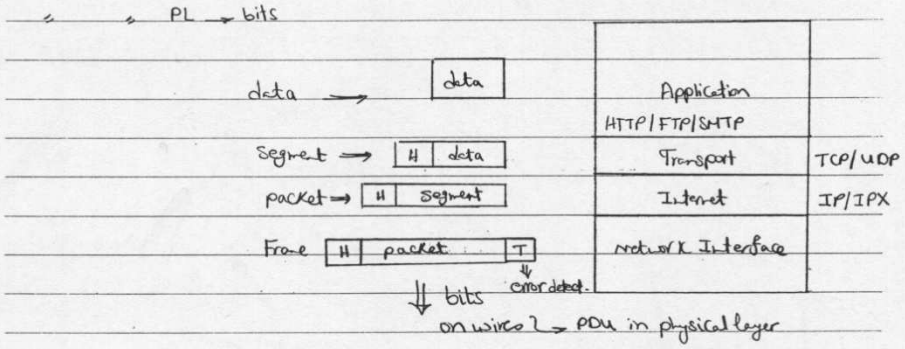
TCP/IP Model DoD Model (Department of Defense Model) ⇒ وزارة الدفاع الأمريكية

Application			
presentation		Application layer	
Session			4-layer Model
Transport		Transport layer	
Network		Internet layer	
Datalink		Network Interface layer	→ DLL & PL in some books
Physical			
OSI Model		TCP/IP Model	
7-layer Model			

Encapsulation process

PDU (protocol data unit) ≡ The unit of data with which the s/w (protocol) in each layer will deal with.

PDU In Application layer is called → data
" " Transport " " " → segment = data + header
" " Internet " " " → packet = segment + header
" " Datalink " " " → Frame = packet + header + Tail
" " PL → bits



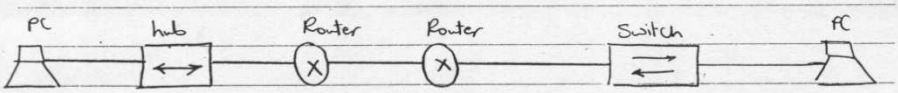
Header in Transport layer contains indications of
(1) upper layer protocol (to submit the data to the proper protocol @ the dest.) ex: HTTP, FTP, ...
(2) A contain Add. called service add:/ s/w port no.
(3) Transport layer indications like : sequence no., ...

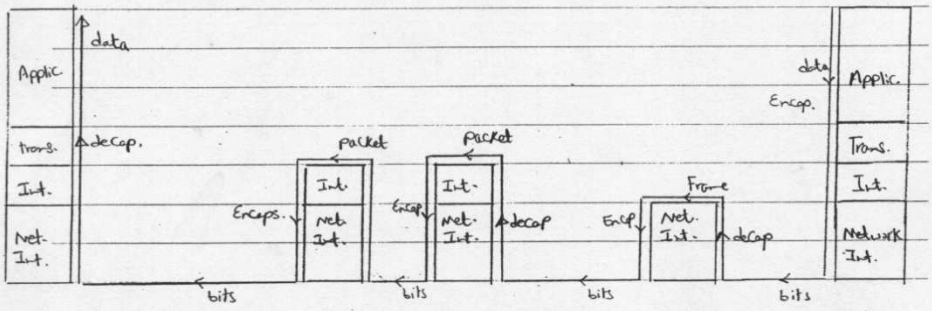
Header in Internet layer contains indications of
(1) upper layer protocol (TCP/UDP)
(2) IP - address of src & final dest.

Header in Network Interface layer contains indications of
(1) upper layer protocol (IP, IPX, Appletalk)
(2) src & next hop MAC addresses

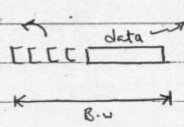
De-Encapsulation This is the reverse operation & will be made at the dest.

Router (L3 → L1) PC (L7 → L1)
Hub (L1) Switch (L_2 → L1)





* Difference bet. B.w & through put → what is useful in B.w (real data)



Ideal B.w > through put

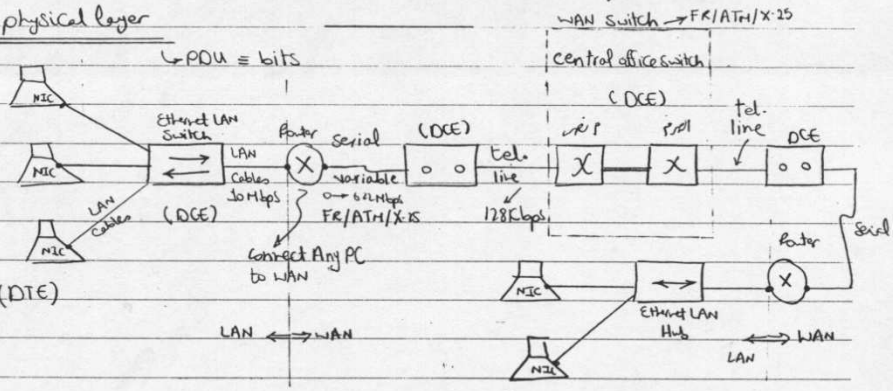
Session 3
26/4/06

Topics

TCP/IP
↳ Network Interface layer
↳ physical layer
↳ WAN Standards, Cables & Connections

physical layer

↳ PDU ≡ bits

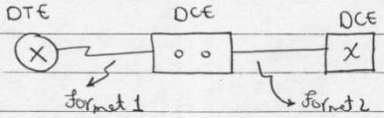


DTE ≡ Data Terminal Equipment, Can be src or dest. of data (Brain)

DCE ≡ Data Control Equipment, used to adjust Clking & Synchronization (tongue)

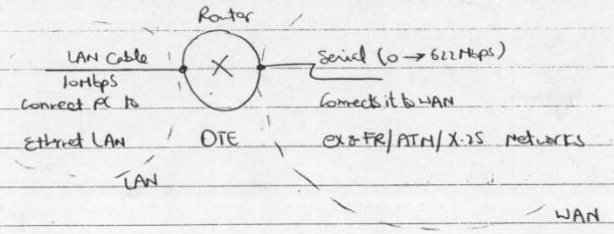
↳ clocking & Synchronization : If we reserve a B-w from central device at rate 128 Kbps but serial cable is variable rate so to adjust it to transmitt & receive at this rate we use a DCE device ex: Modem.

- we may use a DCE device to change from 1 format to another i.e line coding



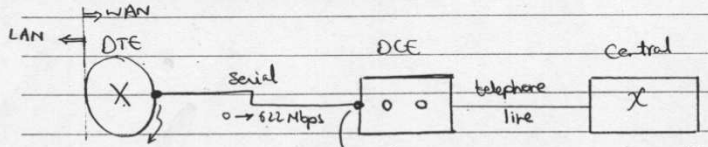
N.B :- DCE is called Modem only when we convert from Analog → digital & vice versa

Router : At least has 2 interfaces & used to connect any PC to WAN



DCE device by configuration can be used for FR/ATM/ISDN

(I) WAN Standards, Cables, Connectors



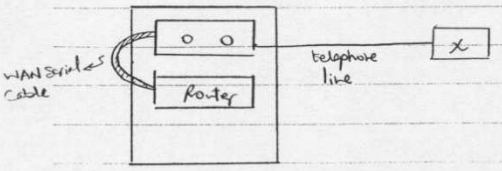
DB-60 (60 pins)

Smart Serial ↔ DB-21 (21 pins)

ex: V.35, X.21, EIA/TIA 232 (RS 232)
EIA/TIA 449, EIA/TIA 530

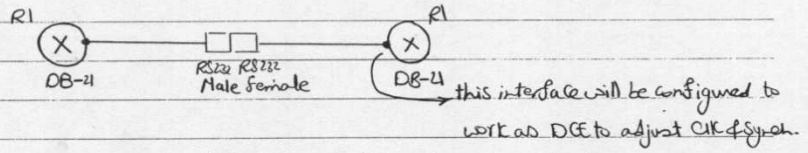
⇒ each of these standards will use certain cable length, cable type, certain connectors, certain Pin assignment & certain bit rate

We may find (DB-60) ↔ RS 232 Cable (DB-21) ↔ V.35 Cable
(DB-21) ↔ RS 232 Cable



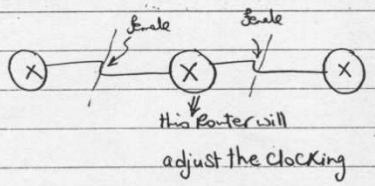
How to connect two Routers ? ⇒ we'll use null - Modem Method

- 2 Routers are 2 DTEs, can't be connected to each other unless we use a DCE device to adjust Clk & Synch., but now we'll use another Method
- 2 Routers will be connected back-to-back & we'll use 2 Cables
  DB-21 ↔ RS232 Male & DB-21 ↔ RS232 female
  & the Router to the side of the female port will be configured to work as DCE i.e it'll adjust Clk & Synch. i.e it'll be the master & the other will be slave.



⇒ Cisco made one Cable 1 terminal to be connected to the DTE device & the other terminal will be connected to the device that will be configured as DCE

⇒ for 3 Routers



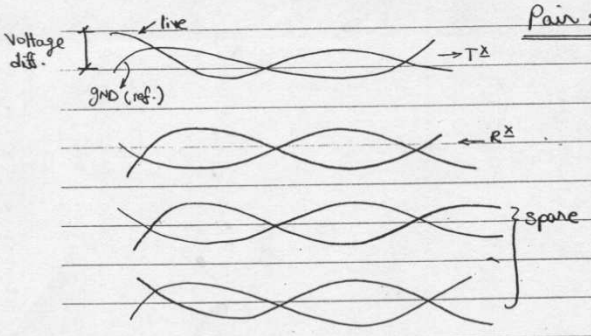
session 4
29/4/06

II - LAN Cables, Standards & Connectors

1- Twisted pairs :- (1.1) Cables

(1.1.1) UTP (unshielded Twisted pair)

It is an 8-wires cable as follow

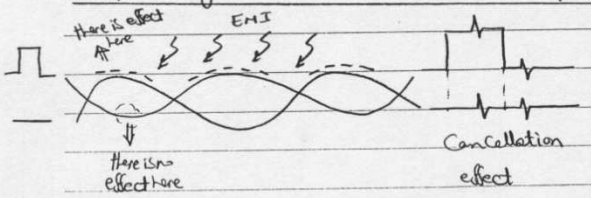


Pair :- we've no common ground for each pair 1 wire is live & the other is ground or Ref.

unshielded : the outer cover is not shielder, it is just a cover & it can't prevent noise.

Twisted : for noise immunity against EMI/RFI & cross talk

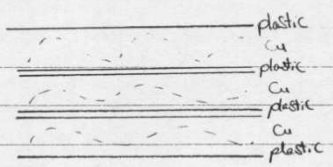
EMI (Electromagnetic Interference) & RFI (Radio Frequency Interference) rejection

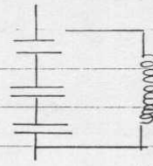


EMI occurs if our cable travels beside ancon lamp, motors.

Cross talk rejection

effective ct ⇒ Capacitors



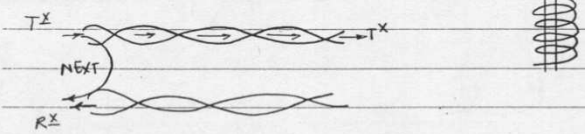


→ in order to cancel capacitive effect, we should use a coil which is accomplished using the twisting of wires.

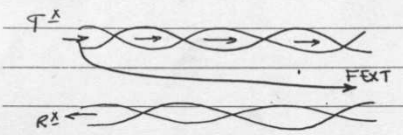
الملفوف على شكل coil وهو ده الـ twisting بتاع الـ wires

Types of cross-talk

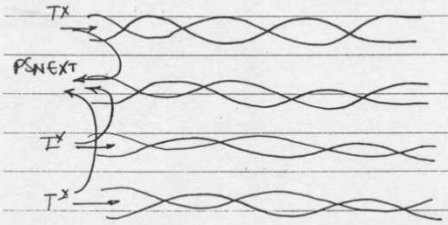
(1) NEXT : Near End Cross-talk



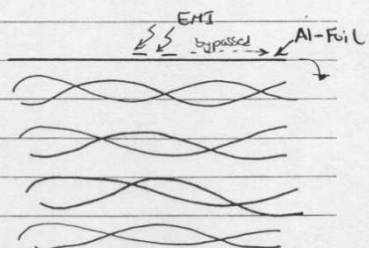
(2) FEXT : Far End cross-talk ⇒ has less effect bec. the signal will be attenuated until it reaches the other end.



(3) PSNEXT : power Sum NEXT ⇒ Sum of effects of no of cables at one cable



(1.1.2) STP (Shielded Twisted pair)

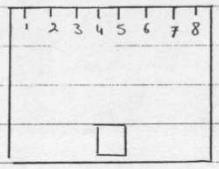


- Aluminium Foil is used to bypass charges & so prevent EMI effect.
- each pair may be shielded to prevent cross-talk

for STP 1m wire costs ≅ 7 L.E

(1.2) Connectors for Twisted pairs in LANs

RJ 45 (Registed Jack no. 45) is used ⇒ It has 8 pins



pin 1 → orange X white
pin 2 → orage
pin 3 → green X white
pin 6 → green
pin 4 → blue
pin 5 → b X w
pin 7 → w X brown
pin 8 → brown

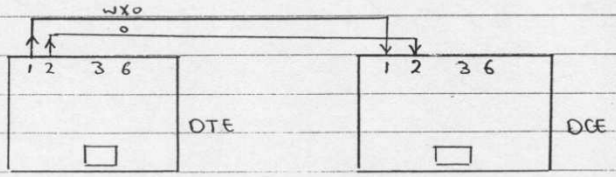
pins (1 & 2) → T^{X} from DTE & R^{X} to DCE
(1: GND, 2: live)

pins (3 & 6) → R^{X} to DTE & T^{X} from DCE
(3: GND, 6: live)

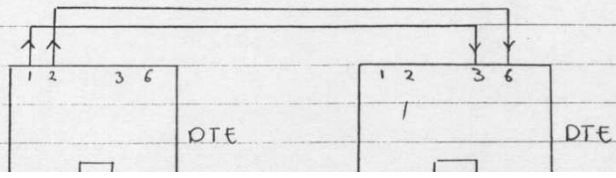
(1.3) Connections of twisted pairs

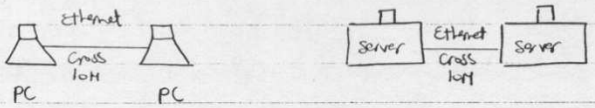
(1.3.1) Straight connection :- Between LAN DTE & LAN DCE ex:- PC & Switch

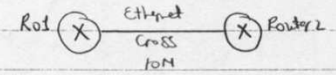
pin 1 T^{X} → pin 1 R^{X} pin 3 T^{X} → pin 3 R^{X}
pin 2 T^{X} → pin 2 R^{X} pin 6 T^{X} → pin 6 R^{X}



(1.3.2) Cross over connection : Bet. 2 DTEs or 2 DCEs ex:- 2 Routers, 2 PCs, 2 Switches

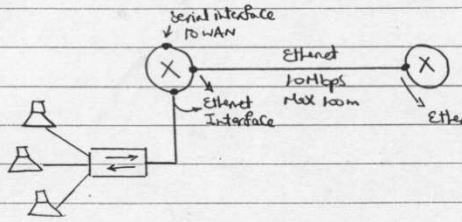






N.B:- when we connect 2 Routers through serial connection as before, we may use a DCE device between them or configure one of them as a DCE inorder to adjust CLK & Synchronization.

But through Ethernet interface we can connect 2 DTEs or 2 Routers without a need to a DCE device ?? bec. in Ethernet we've fixed standard speed = 10 Mbps & both R1 & R2 work with Ethernet & so CLK & Synch. is adjusted



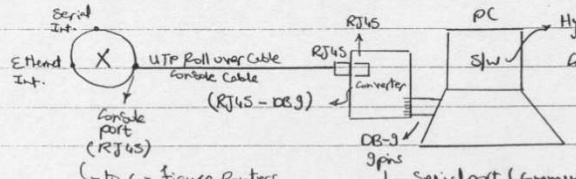
- Clking & synch. are integrated technology.
- both Routers should work with the same technology; if R1 works with Ethernet & R2 's 's fast 's they won't communicate with each other

(1.3.3) Rollover Cable (see cables ⇒ different colors are used

↳ to configure the Router for the 1st time

(Pin1 ↔ Pin 8, Pin2 ↔ Pin 7, Pin 3 ↔ Pin 6, Pin4 ↔ Pin5)

⇒ Now Routers come with it a cable has an internal converter this cable RJ45 (Router) ↔ DB-9 (PC)



↳ to configure Routers for 1st time

↳ Serial port (communication port) DB-9 / DB-25

(1-4) LAN Standards with Twisted pairs

Ethernet ⇒ 10 Base T (IEEE 802.3) (1980 ~ February) ⇒ (Exam)
↳ (uTP/STP ≅ 100m max)

Fast Ethernet ⇒ 100 Base T

1 Giga Ethernet ⇒ 1000 Base T (IEEE 802.3ab gigabit over Copper)
↳ (Exam)

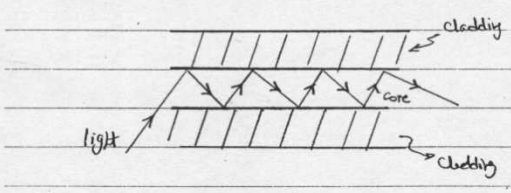
(1-5) Twisted pairs Cables Standards

- Cat 5 (Category 5)
- Cat 5e (Category 5 enhanced) up to 1 Gbps
- Cat 6 (Category 6) up to 1 Gbps

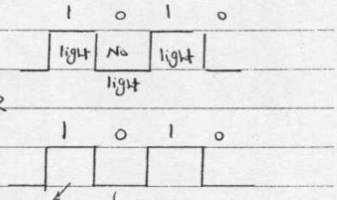
→ this classification is according to att., speed, noise immunity, --- point of view

(2) Fiber Cables used for long distances.

AS diameter ↓ it is better



OR



high light intensity ↳ low light intensity

(2-1) Cables SMF & MMF

SMF (Single mode)	MMF (Multi Mode Fiber)
- up to 100 Km	- up to 4 Km
- Core diameter = 9 Mm	- Core diameter = 50 Mm / 62.5 Mm
- Cladding ↓ = 125 Mm	- Cladding ↓ = 125 Mm
(9/125)	(50/125) or (62.5/125)
	- used mainly in LANs

(2.2) Fiber Connectors

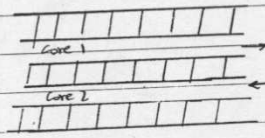
SC (Square Connector) □
ST (Straight Tip)
MTRJ → most popular

} we use the connector according to the Routers & Switches used
⇒ there're Cables SC ↔ ST

(2.3) LAN standards with Fiber

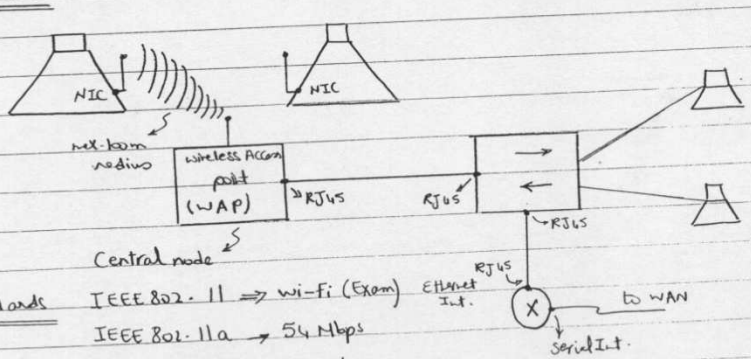
10 Base F
100 Base F
1000 Base LX (long wavelength ≡ long dist. (SM))
1000 Base SX (short " " ≡ short dist. (MM))
} IEEE 802.3z (Exam) — Gigabyte over fiber

N.B : for each fiber cable we're at least 2 cores 1 T^x & 1 R^x



(3) wireless

Wi-Fi → wireless Fidelity



Central node

standards
IEEE 802.11 ⇒ wi-Fi (Exam)
IEEE 802.11a → 54 Mbps
IEEE 802.11 b → 11 Mbps
IEEE 802.11 g → 54 Mbps

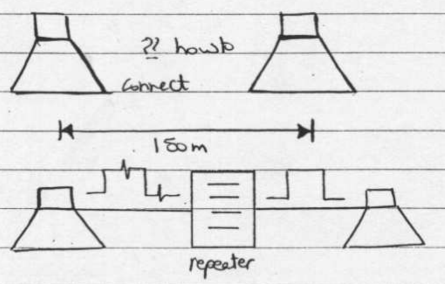
physical layer devices : Devices work in physical layer ⇒ deal with bits

physical layer WAN devices ⇒ only Modem

physical layer LAN devices ⇒ Repeater & hub

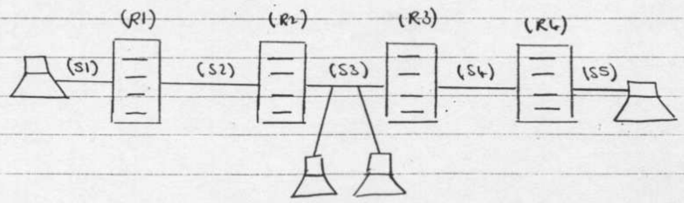
(1) Repeater : used for signal Regeneration , it may use a level detector to regenerate the old signal.

N.B :- Regeneration ⇒ Amplify desired signal only
Amplification ⇒ Amplify both the signal & noise.



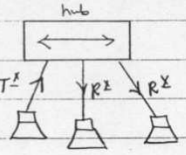
5 - 4 - 3 Rule : This Rule is used to manage max. no. of repeaters that may be used without collision occurrence.

5 : max. no. of segments = 5 , 4 : max. no. of repeaters = 4
3 : max. no. of populated segments. ٣ segm بس ينفع توصيلهم ب PCs



(2) Hub ⇒ physical layer device, i.e deal with bits

(a) Multiport Repeater : regenerate the signal bit by bit.



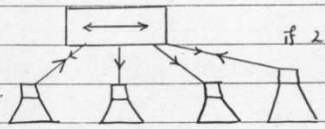
- signal transmitted from one port will be received by all other ports (logically ⇒ bus)
- 5-4-3 Rule is applicable & we can use 4 hubs as max. otherwise collision will occur.

(b) All devices connected to a hub are members in a single collision domain

domain ⇒ group of PCs 

collision domain ⇒ group of PCs if they talk at the same time, collision will occur & affects all other PCs

i.e group of devices that're affected by each others collision.



if 2 PCs try to transmit at the same time, collision will occur.

(c) All devices connected to a hub are members in a single Broadcast domain.

- A broad cast msg from 1 PC will reach all other PCs & they will accept it.

(d) Devices connected to a hub operate half duplex (either T^X or R^X at a time) not full duplex (T^X & R^X at the same time)

- 10 Base T ⇒ this means that the port speed @ half duplex = 10 Mbps
- If we've hub 4 port ∴ hub speed = 10 Mbps because we're allowed to T^X from only 1 port at a time.

Sessions
1/5/06

Topics : TCP/IP
↳ Network Interface layer
↳ DLL (1) MAC Addressing
(2) Hop to hop delivery – MAC Method
– Frame format & Error detection
– flow control

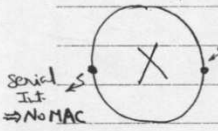
In DLL ⇒ PDu ≡ Frame (3) DLL devices

"Data link layer"

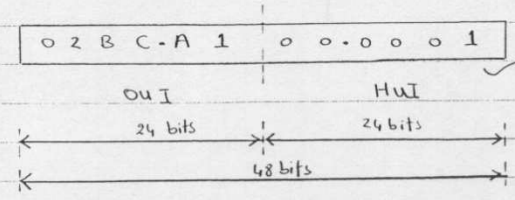
(1) MAC Addressing :

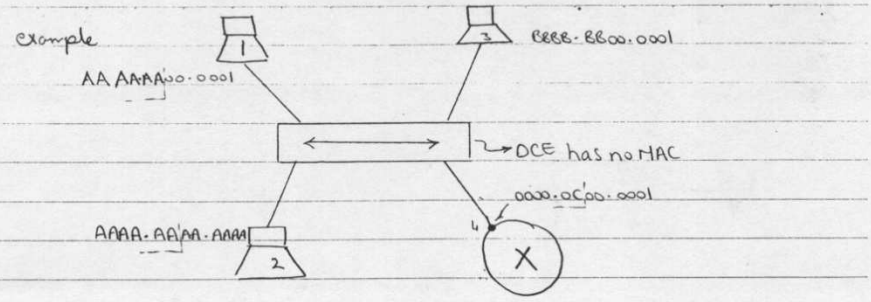
– Medium Access control addressing
– Each device needs an address to access the media which is the MAC address
– It is called next hop addressing, we will deal with LANs Ethernet & so this next hop is bet. near devices.
– It is a H/w unique address

MAC Address for Ethernet – 48 bit address burnt on the ROM of the NIC of the DTE ≡ physical or H/w address
– Serial interface of the Router has No MAC Add.
– Ethernet " " " " " MAC Add.



– 48 bits ≡ 12 hexadecimals (0,1, ... 9,A,B,C,D,E,F)
– 48 bits are divided into two parts each of 24 bits
↳ OUI (organization unique Identifier) ≡ unique ID/vendor ⇒ manufacturer
↳ HUI (Host unique Identifier) ≡ unique ID/host ⇒ host specific part

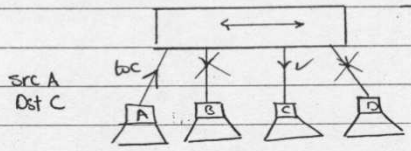




NIC for PC1 & NIC for PC2 were produced by the same Vendor.

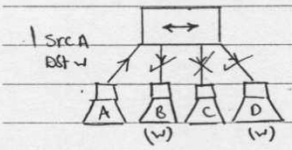
Next Hop Destination MAC Add. may be

(1) Unicast MAC Add. :- msg to only 1 destination



- The msg will be sent to all PCs, but only C will accept it

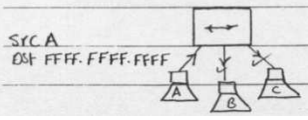
(2) Multicast MAC Add. : msg to 2 or more destinations.



- This will be useful in some Applications like video conference when someone needs to send to many PCs
- using a SW setupped on these PCs, we teach each PC a virtual MAC Add. ex : W & the Src will use this MAC AS the dest. MAC

W may be like 00.000C

(3) Broadcast MAC Add. :-



- msg sent to All the PCs & they will accept it.
- The Src uses a MAC Add. consists of 48 ones
- B.C MAC FFFF.FFFF.FFFF

⇒ In reality the NIC make AND operation with the incoming MAC & if the result is its MAC then it'll accept the msg

(ex1) . T^A R^B (MAC Add 10101)

Src MAC A

dst MAC 10101 ⇒ unicast msg

AND operation 10101
10101

10101 ✓ My MAC

(ex2) T^A R^X (MAC Add 10101)

Src MAC A

dst MAC 11111 ⇒ broadcast msg

AND 10101
11111

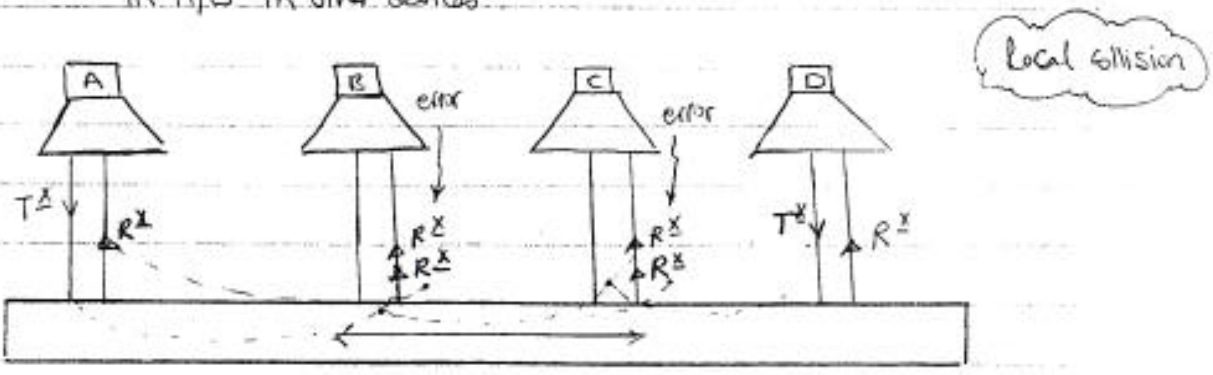
10101 ✓ My MAC

(2) Hop to Hop delivery with Ethernet LANs

(2.1) Ethernet MAC Method : It is the method used to access a shared media without collision

CSMA/CD (Carrier Sense Multiple Access with Collision detection)

↳ This is also on the ROM of the NIC or It may be implemented in H/w in other devices.

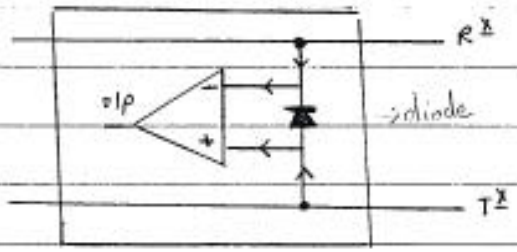


A & D send at the same time, B & C'll receive 2 msgs 1 from A & 1 from D & they'll think that it is 1 msg which is wrong.

NIC will perform the following operation

(1) Carrier Sense : Sensing electricaly in the wire through the receiving pair by the mean of a loop back circuit inside NIC inorder to know wheather the line is busy or not.

(2) Multiple Access : A & D sense No Carrier & transmit at the Sametime.



loop back circuit (detects collision)

if o/p is Zero volt
↳ either T^X or R^X has a signal on it
if o/p is 5 volt
↳ both T^X & R^X have signals.

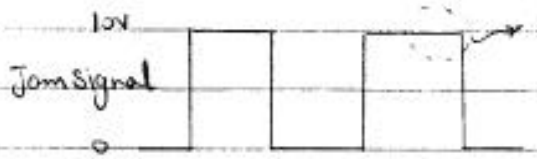
(3) Collision detection : - A & D will detect collision due to they found themselves T^X & R^X at the Same time (using loop back ct.)

- A & D will perform backoff algorithm & Stop transmitting of the frame.

Even if A & D are very far from each other the Sent part of the frame won't exceed 64 byte before A & D Sense collision

↳ for this reason we use 5-4-3 rule i.e we use 4 hubs as max. otherwise A may Send a whole frame & Can't Sense that any other PC is transmitting

- After that A & D will Send a Jam Signal (0 → 10v) & not an ordinary signal (-5v → 5v) so B & C will know that there is collision & they will discard the part of the frame they received (this part is < 64 byte)

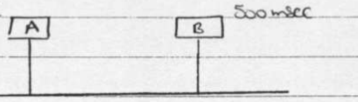


→ this high voltage makes B & C feel that there is Something wrong

(4) A & D will start a Random counter :

- The device that finishes its count down will start the operation again by transmitting the last failed frame

N.B :- NIC saves the last frame until it is sent correctly.



- If 1 PC try to send the same frame 16 times & in each time he senses collision, he will ⇒ يفصل نفسه بعض الوقت ويبدأ بعد ذلك يبعث

---

local collision vs. late collision ⇒ In exam (drag & drop)

local collision

(1) occur befor 64 bytes of data are transmitted.

(2) occur in normal Network operation

(3) Jam signal is sent intentionally to corrupt the collided Frame

(4) Dagamed Frame is retransmitted

Late collision

(1) occur after 64 bytes of data are transmitted.

(2) occur in Abnormal Network operation

(3) occur due to excessive Network latency (delay)

(4) Damaged frame is not transmitted.

→ if we use more than 4 hubs.

→ wires 're not good & more delay

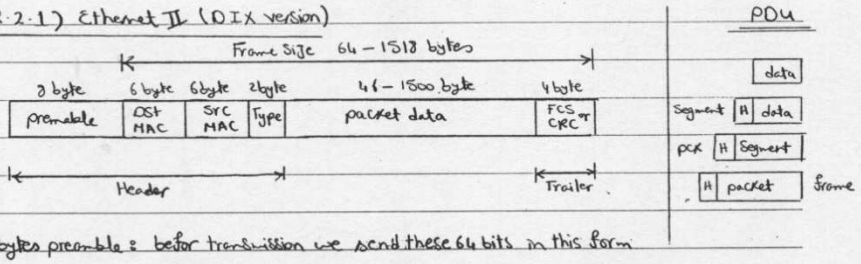
→ NICs 're not good & it senses the carrier so late after 64 bytes 're transmitted.

CSMA/CD ⇒ Restarts its operation each frame.

(2.2) Frame Format & Error detection

- Ethernet I — Huawii university
- Ethernet II — DIX version — Digital Intel Xerox (not frequently used)
- IEEE version — 802.2, 802.3

(2.2.1) Ethernet II (DIX version)



8 bytes preamble : befor transmission we send these 64 bits in this form
1010101 ... to synchronize the CLK & thats why 2 DTEs in LANs can be connected to each other without need to a DCE device.

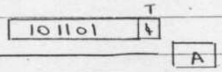
6 bytes Dst MAC : It is sent first bec. if it is not my msg i won't perform any un need processing

6 bytes Src MAC : we should know the src add. so the dst can reply with ACK.

2 bytes Type : Type of the upper layer protocol (IPv_4, IP_x, Appletalk)

46 – 1500 bytes data : Ethernet packet 46 – 1500 bytes where MTU (Max. Transmission unit) equals 1500 bytes.

4 bytes trailer : for Error detection



→ FCS (FCS check sum)
In the trailer field we send no of 1s in our msg
& B will make CHECK to know wheather msg is correct or not . but if B receives 01110 4 ⇒ msg is wrong but B will accept it !!

→ CRC (Cyclic Redundancy Check) : more smart method

⇒ Min Frame size = 64 bytes , if one receives < 64 byte .. this means that this frame is wrong

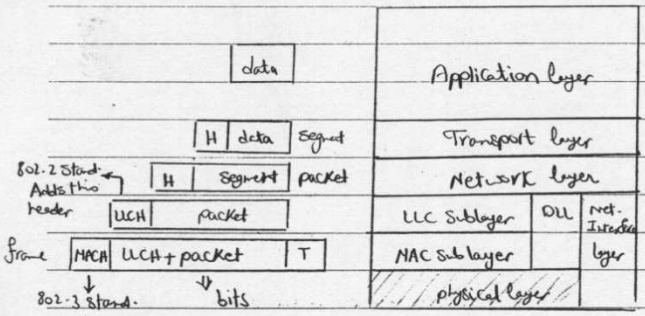
Session 6
3/5/06

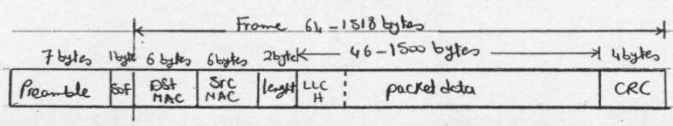
(2.2.2) IEEE version

Datalink layer

IEEE 802.3
MAC Sublayer
(Interact with PL)

IEEE 802.2
LogicalLink Sublayer (LLC)
(Interact with upper layer)





7 bytes preamble : 10101010 ⎍⎍⎍⎍ to adjust synchronization & clking

1 byte SoF : Start of frame byte tekethis form 10101011 → to inform the dst. that this is the start of the frame

6 bytes dst. MAC

6 bytes src MAC

2 bytes lenght : 64 bytes → 1518 bytes (MTU) ⇒ lenght of the frame

↳ aids the RX to calculate CRC bit by bit until the End of the frame.

⇒ If we're no lenght field [ ] idletime [ ] idletime [ ]
but lenght field saves time

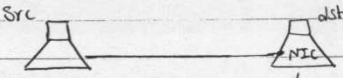
N.B :-(1) MAC Header ≡ Dst MAC + Src MAC + lenght + CRC

(2) Even if the transport layer sends an ACK with no data is just headers = 64 bytes

(2·3) Flow control ⇒ from hop to hop

- here in layer 2 we've no wait; i.e dst can't control src transmission.
- dst has a buffer ≡ RAM of NIC if it is over loaded ⇒ all incoming frames will be discarded

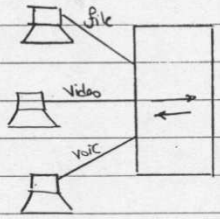
(2·3·1) Buffering :



Transmits at very high rate

↳ NIC buffer/memory will store the data but to a certain limit.

(2·3·2) Congestion avoidance : NIC will choose some contents of the buffer of less priority & discard it & this happens only ⇒ في حالة



voice/video ⇒ highest priority
file/browsing ⇒ can be discarded
priority ⇒ class of service

(3) Data link layer devices (layer 2 devices)

These're devices that understand MAC
- MAC Add.
- MAC Method (CSMA/CD) of delivery hop-hop
- MAC frame formate

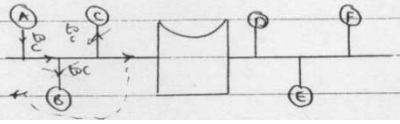
(3·1) NIC (Network Interface Card)

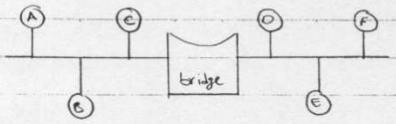
↳ has MAC add. — has the CSMA/CD s/w on its Rom — transmits bits on the wires frame by frame

(3·2) Bridge

collision isolator ⇐

device that is used to segment the network into multiple collision domains & it also regenerates the signal.



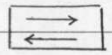


bridge Make table for those at left & those at right segment

Collision domain(1) (LAN segment1)

Collision domain(2) (LAN segment2)

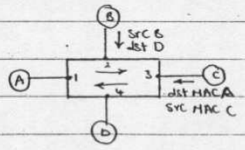
- Bridge performs its fn in S/w this means that it has → processor & memory
- using S/w bridge can decide that A & B share the same collision domain & A & D don't share the same collision domain
- Bridge has max. 16 ports because as no of ports ↑ ∴ processing ↑
- Bridge is now obsolete & not used.

(3.3) Switch  upto 576 ports

- It is a multiport bridge, regenerates the signal & segments the Network into multiple collision domains.
- Switch performs its fn (learning & forwarding) both in H/w using ASIC (Application specific IC) i.e All cases are implemented
- The switch has 3 fns : learning – forwarding – Remove layer 2 loops

(3.3.1) learning : form MAC Table by checking the SRC MAC in an incoming frame

- At power on, the MAC table is empty, i.e there is no automatic learning
- MAC table will now be as follow

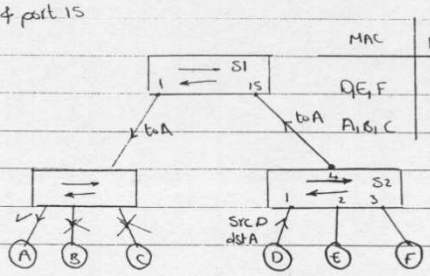


MAC	port no.
B	2
C	3

2 → switch learns that B is on port 2 from the SRC MAC

- The switch learns the entry for only 300 secs (5 min) of non activity & then removes it inorder to free space in the memory

Rule 1 : Single switch can learn existence of multiple devices like port 1 & port 15



MAC table S1

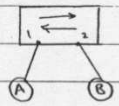
MAC	port
D,E,F	15
A,B,C	1

MAC Table (S2)

MAC	port
D	1
A,B,C	4

Rule 2 : A single device can never exist on two switch ports at the same time

MAC	port
A	1

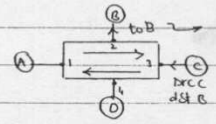


MAC	port
~~A~~	1 → deleted
A	2

i.e The switch adapted himself to any change.

(3-3-2) Forwarding : Switching frames to dst. by checking dst MAC in an incoming frame.

assume that the switch learned All the entries & perform his table as follows

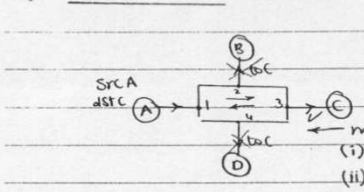


MAC	port
A	1
B	2
C	3
D	4

- Now assume that our switch is not teached, what will he do??

⇒ The switch will F.w.D by flooding (multicast sw) in these cases :-
act as a Hub (send msg to all ports)

(1) unknown unicast (the switch didn't learn this entry before)

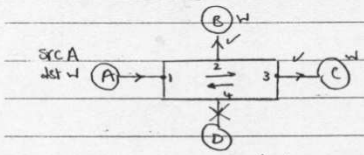


MAC	port
A	1
C	3

using (i)

now C reply with ACK
(i) the switch knows that C → port 3
(ii) " " F.w.D ACK to A

(2) Multicast msg (msg to some PCs only i.e video conference)



A, B, C can recieve with MAC w, but send with thier original MACs A, B & C

- now A, B & C use a S/w called Telnet, each of them will have an additional logical MAC ex: w to which anyone can send on, but none of them can make ACK with w

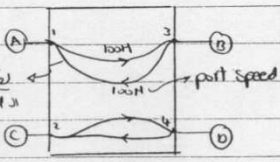
(3) Broadcast msg — flooding to all PCs & they all accept the msg

Note A : Devices connected to switch are members in single Broadcast domain.

- The switch forwarding is done by MicroSegmentation
↳ part of LAN

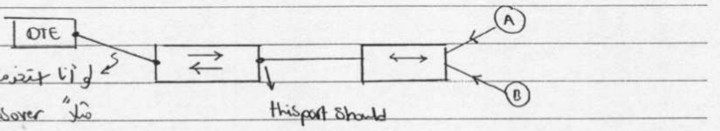
(1) Dedicated connection bet. src & dst.
(2) Full B.w is given to src & dst

Note B : devices connected to switch operate @ full duplex (i.e T^x & R^x @ same time)



- if Port 1 $\xrightarrow{T^x}$ to port 2 & port 4 @ same time
  ∴ it will $\xrightarrow{T^x}$ port 2 with 50 Mbps } bec. port speed = 100 Mbps
  └ $\xrightarrow{T^x}$ port 4 " " "

<u>Note C</u> : Every port on the switch is considered single collision domain
& this appears clearly if 1 port of the switch is connected to a hub



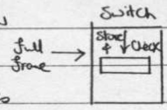
و أنا فترضت كابل غلط
مثلاً " crossover

this port should operate with CSMA/CD → ميقدرش أرجاب A و B) يبعت في نفس الوقت

- If port 1, port 2 & port 3 T^x @ same time to port 4 each with 100 Mbps
  ⇒ port 4 won't bear 300 Mbps & so it will make Queing & apply FIFO technology.
  (FIFO = First In First Out)

<u>The switch forwarding Modes</u> ⇒ ordinary switches operate by one of them but smart ones can use 2 of these modes & switch bet. them.

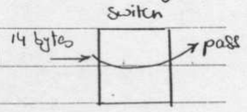
(1) <u>store & FWD</u> : save the whole frame till end of the CRC & then check for errors, then begin to FWD ⇒ check is made in H/W



frame error may be → (a) CRC error
(b) giant frame ⇒ frame > 1518 bytes
(c) Runt frame ⇒ frame < 64 bytes
↳ the switch is connected to a hub makes many collisions

Adv → error free   Disadv. → slow

(2) <u>Cut through</u> : the switch waits for 14 bytes (preamble + dst MAC) then begins to FWD it after knowing the dst. MAC



Adv. → very fast , Disadv. → no error check & PC will make the check.

<u>N.B :-</u> Cisco switches are smart, they operate with cut through mode & every no. of frames forwarded they check a frame for error & If the percentage of damaged frames in the checked frames is large then they switch to store & FWD mode ⇒ but Cisco routers are expensive.

(3) <u>fragmentation free</u> ⇒ the switch waits for the first 64 byte & then begins to FWD.

يعني لو ال frame > 64byte ← يبقى أكيد هو مش Runt

ولكنه ممكن أن تكون ← giant

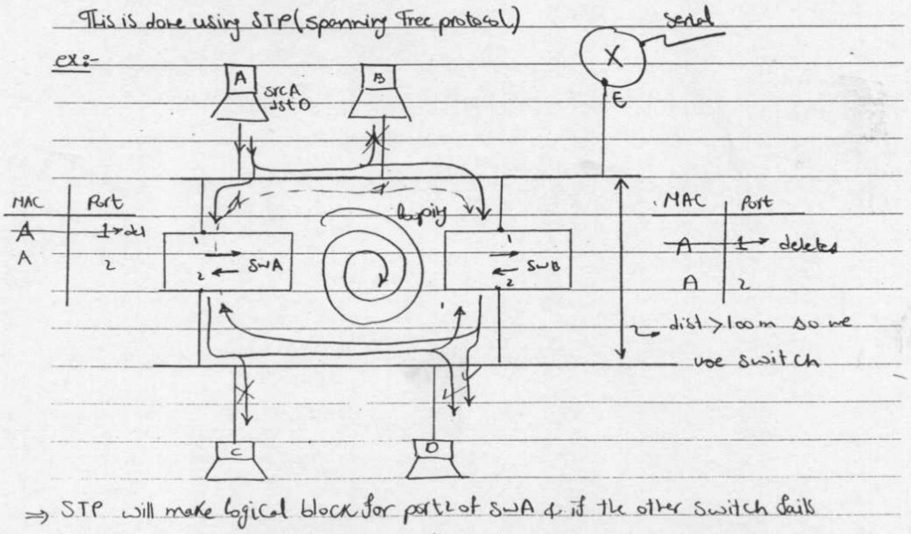
↙ CRC error

Adv. moderate speed

<u>(3.3.3) Remove layer 2 Looping</u>

This is done using STP (spanning Tree protocol)

<u>ex:-</u>



⇒ STP will make logical block for port 2 of SWA & if the other switch fails the STP will make port 2 of SWA available again.

⇒ The 1st frame is always Broadcast, with no STP we'll have a B.C storm.

Session 7
5/7/06

Topics

Internet layer
- → logical Addressing } IP_{v4} _ IP_{v6} _ ICMP _ ARP _ RARP
- → End-to-End data delivery }
- → Routing (finding the best device) } OSPF _ IGRP _ EIGRP
- → layer 3 devices

PDU ≡ packet

logical addressing:

(1) giving each device a unique IP globally
↳ no 2 devices will have the same IP (up till now!)

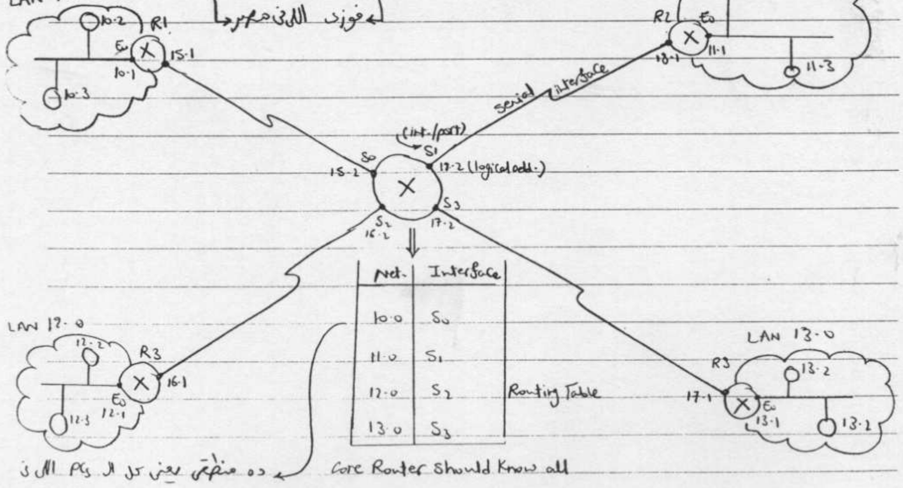
(2) consists of 2 parts

Network ID	Host ID

logical address

Network part (Network ID) | Host part (Host ID)

↳ فوزي اللي [illegible]



Net.	Interface
10.0	S_0
11.0	S_1
12.0	S_2
13.0	S_3

Routing Table

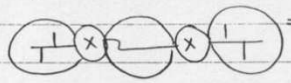
ده منطقي يعني كل ال PCs اللي ف
ال LAN 10.0 يمكنه الوصول لها عن طريق S0

Core Router should know all LANs in the network

Notes

(1) 0,1,2,3,... ← Routers ترقيم الـ ، 1,2,3,... ← Switches ترقيم الـ

(2) Each point on the Router is considered a different network



⇒ 3 Networks

(3) 10.0, 11.0, 12.0, 13.0 ⇒ are Network names, but we can't send to this a certain msg.

(4) Routers try to know how to arrive to all other Routers

⇒ Routing Table of R1

10.0	E0
11.0	S0
12.0	S0
13.0	S0

but the Short Routing Table will be configured

Net.	Int.
10.0	E0
0.0	S0

عنوان الى ملوش عنوان ←

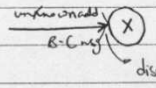
- يعني أي حاجة على هذا العنوان تخرج من S0 وهذا معناه انه هذه الـ msg تكون لـ LAN بعيد

(5) Each LAN will have a unique Add. If 2 LANs have the same Add. ⇒ therefore network will think like that

10.0	S0
10.0	S4

i.e the Router can reach the LAN 10.0 from 2 paths & so it will send ½ of the data through S0 & ½ of the data through S4 ⇒ وهذه بيتشاد

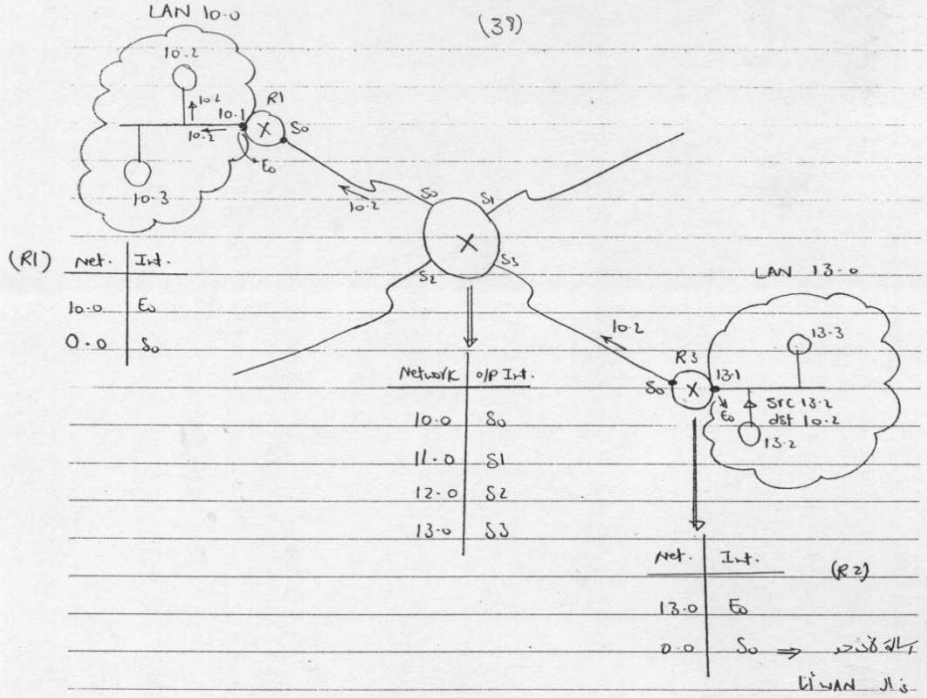
(6) Router will discard the B.C msg & make no flooding ⇒ because all LANs in the world will fail



(7) WAN Switches are not like LAN Switches i.e they make no flooding

(8) Routers can learn & construct the Routing table using Routing protocols (by configuration)

(9) Every port on the Router is considered a diff B.C domain & a diff collision domain.



logical Address protocols : IP_{V4}, IP_{V6}, ARP, RARP

IP_{V4} : (1) Support logical addressing (IP Address)
(2) Support End-to-End delivery

IP address : ⇒ 32 bit

XXXX XXXX . XXXX XXXX . XXXX XXXX . XXXX XXXX

1 octet = 8 bits

⇒ IP add. is represented in dotted decimal notation

1111 1111 . 1111 1110 . 1111 1111 . 1111 1111

255 . 254 . 255 . 255

IP Classes

IP Class A :

N	H	H	H

⇒ first octet begins with 0 i.e 1st octet 0xxx xxxx

i.e 1st octet ranges from 0000 0000 → 0111 1111 (decimal)

0 → 127

(0.0.0.0) reserved → default route all ones

ex:- R1 Routing table

10.0	E0
0.0	S0

reserved (127.0.0.0) for some purposes

127.0.0.1 → loop back test on DOS

ping 127.0.0.1 ⇒ test TCP/IP S/W on our PC

ex:-

check 1st octet = 57 i.e bet. 0 & 127

⇒ this is class A 57.1.5.5 (N H)

Network ID = 57.0.0.0

host. ID = 57.1.5.5

IP Class B

N	N	H	H

⇒ first octet begins with 10 i.e 1st octet 10xx xxxx → class B

i.e 1st octet ranges from 1000 0000 → 1011 1111 (decimal)

128 → 191

ex:-

this is class B 172.1.5.6 (N N H H)

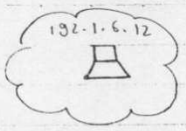
Network ID = 172.1.0.0

IP Class C

N	N	N	H

⇒ first octet begins with 110 i.e 1st octet 110x xxxx → class C

192 → 223

ex :- 

192 bet. 191 & 223 ⇒ class C i.e $\frac{192.1.6.12}{N \quad H}$

Network Add 192.1.6.0

IP class D Its first octet starts with 1110 XXXX

224 → 239

↳ reserved for multicasting

⇒ Any PC must have class A or class B or class C IP add. & it can also have a class D multicast add. if Any PC setup a Telnet/video conference program on his PC

IP Class E Reserved for experiments of new protocols.

Its first octet starts with 1111 XXXX

240 → 255

↳ reserved (255.255.255.255)

local Broadcast ↲

(Inside the LAN ≡ All host Add.)

The Router doesn't B.C msg outside the LAN

Reserved IP Addresses

- 0.0.0.0 ⇒ Add. of All Networks
- 127.0.0.1 ⇒ loop back test
- 255.255.255.255 ⇒ local Broadcast

IANA (Internet Addressing Network Association) ⇒ IPs ... All ...

Types of IP Addresses Rules

(1) Network Address All host bits = 0

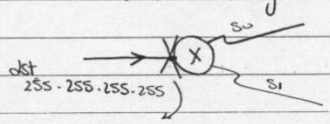
(2) Broadcast Address (Direct Broadcast ⇒ to All hosts in certain network)
All host bits = 1

(3) Host Address All host bits ≠ 0 & All host bits ≠ 1

What is the difference bet. local B.C & direct B.C

255.255.255.255

If I'm in certain LAN & I want to send a B.C msg to All hosts in my LAN

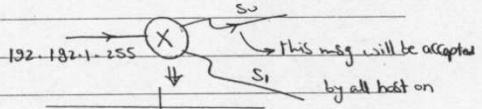


Router will discard it & doesn't pass it

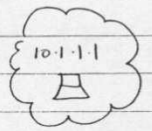
ex: 192.192.1.5

Network ID = 192.192.1.0

direct Broadcast ID = 192.192.1.255



192.192.1.0	S0	192.192.1.0
192.192.2.0	S1	

(ex1) 

class A 10.1.1.1 (N H) Net ID 10.0.0.0

B.C ID 10.255.255.255

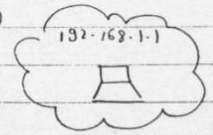
no. of valid hosts $(2^{24} - 2)$

(ex2) 

class B 172.16.5.5 (N N H H) Net ID 172.16.0.0

B.C ID 172.16.255.255

no. of valid hosts $(2^{16} - 2)$

(ex3) 

class C 192.168.1.1 (N N N H) Net ID 192.168.1.0

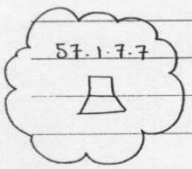
B.C ID 192.162.1.255

no. of valid hosts $(2^8 - 2) = 254$ PCs

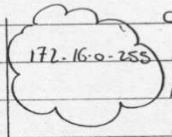
Session(8)
8/5/06

Topics
- Internet layer
  - logical Addressing
    - IP Addressing
    - Shortage of IPs
      1 - Subnetting
      2 - private addressing
      3 - IP_{v6}

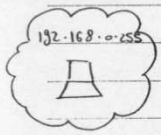
ex: for the following find
(a) Type of address (Host Add. / Network Add. / Broadcast Add.)
(b) If it is a host Add. find Net. & B.C addresses
(c) for each Network find no of IPs that is valid to be used by hosts



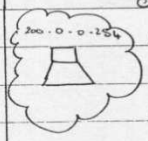
Class A 57.1.7.7 (N / H)
Host Add.
Net. Add. 57.0.0.0
B.C Add. 57.255.255.255
no. of valid hosts = $2^{24} - 2$



Class B 172.16.0.255 (N / H)
Host Add
Net. Add 172.16.0.0
B.C Add 172.16.255.255
no. of valid hosts = $2^{16} - 2$



Class C 192.168.0.255 (N / H)
Broadcast Add.
Net. Add = 192.168.0.0
no. of valid hosts = $2^8 - 2 = 254$ hosts



Class C 200.0.0.254 (N / H)
Host Add.
Net. Add 200.0.0.0
B.C Add 200.0.0.255
no. of valid hosts = $2^8 - 2 = 254$ hosts

Notes
- Direct B.C can be considered unicast until it reaches certain Network & then broadcasted inside it
- by default the router doesn't allow direct B.C but the router can learn by configuration
- The Router doesn't allow the local B.C & it can't learn by config. to allow it.

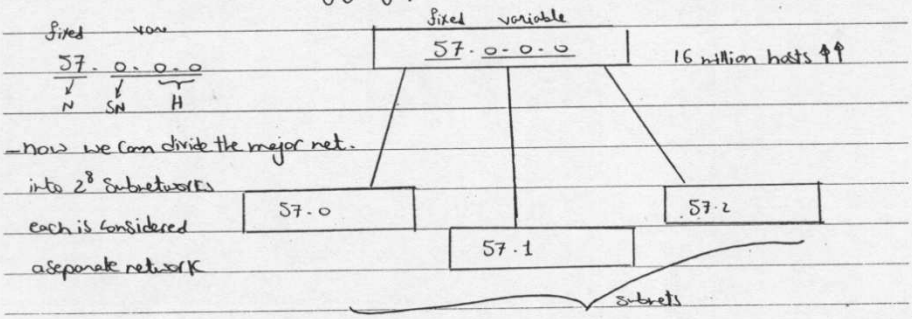
Shortage of IPs

∵ The IP add. is 32 bit So we've net. 2^{32} IPs ≈ 4 million ↓↓

So to solve this Prb. we've 3 solutions Subnetting 3 private networks & IP_{16}

I- Subnetting :

- dividing a major Network into multiple subnetworks, where each subnet is treated as if it is a seperate Network.
- This can be achieved by giving part of host bits to Network bits



Subnet mask :- Should exist beside the IP Add. & used to differentiate bet. Net. & host parts

- It is 32-bit Mask ? because our IP = 32 bit
- I contains 1s followed by continous 0s
- 1 indicates in IP ⇒ Network part
- 0 " " " ⇒ host part

Default Mask : for class A / class B & class C i.e default classes

Class A $\frac{10.0.0.0}{N \quad H}$ ⇒ Default mask : 1111 1111 . 0000 0000 . 0000 0000 . 0000 0000

The default mask is given in two ways

10.0.0.0 / 8 ← (8 ↓ 1st 8 bits are Net. part)

→ 10.0.0.0 (IP) 255.0.0.0 (default mask)

Class B : 172 (N) . 16 (N) . 0 (H) . 0 (H)

172.16.0.0/16 — 172.16.0.0 — 255.255.0.0 ⇓ default mask

Class C : 192 (N) . 168 (N) . 1 (N) . 0 (H)

192.168.1.0/24 — 192.168.1.0 — 255.255.255.0 ⇓ default mask

Now let's see how to deal with Subnets

(Ex1) we've a major Network 192.168.168.0/24
& we need to divide that network into 6 subnets each containing 30 hosts.

fixed ⇐ N H ⇒ Variable

Sol^n : 192.168.168.0/24

Default mask 255.255.255.0

for this major network we've only 8 Variable host bits that we can deal with

192.168.168. (SN) XXX (host) XXXXX

now b'ze 6 subnets we need 3 bits → 8 combinations

& & & 30 hosts & & 5 bits → 32

⇒ 192.168.168.0/27

Subnet mask 255.255.255.1110 0000

255.255.255.224

+ 32
+ 64
128
224

no. of valid subnets = $2^3 - 2 = 6$ subnets

& & & hosts = $2^5 - 2 = 30$ host

Net (fixed) Hst (var.)

(ex 2) 192 . 168 . 168 . 0 /24

we need 14 subnets & 14 hosts/subnet

Sol^n 14 subnets → needs 4 bits

14 hosts → needs 4 bits

192 . 168 . 168 . 0 /28

255 . 255 . 255 . 1111 0000 ← subnet mask

255 . 255 . 255 . 240 ←

(ex 3) we've major Network 192 . 168 . 168 . 0 /24 (N . N . N . H)

using mask /29 find no. of subnets & no. of hosts

new subnet mask 255 . 255 . 255 . 248

this means that the subnet mask is as follows 192 . 168 . 168 . 11111 000 (N . N . N . SN H)

no. of valid subnets = $2^5 - 2 = 30$ subnet

no. of valid hosts = $2^3 - 2 = 6$ hosts/subnet

(ex 4) we've major net. 192 . 168 . 168 . 0 /24 (N . N . N . H)

using mask /30 find no. of subnets & no. of hosts

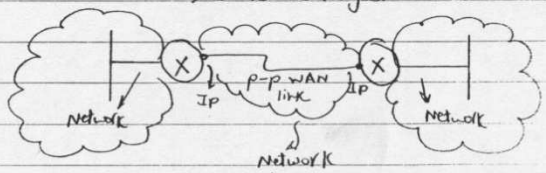
⇒ no. of valid subnets = $2^6 - 2 = 62$ subnets

" " " hosts = $2^2 - 2 = 2$ hosts

Net ID, B.C ID

NB:- mask /30 is used in p-p connections as it will results in only 2 hosts

↳ It is the longest subnet mask that can be used.



here we use mask /30

or 255 . 255 . 255 . 252

N.B :- Mask / 31 ⇒ Is not valid mask, why?

only 1 host bits

∴ no of valid hosts = $2^1 - 2 = 0$ hosts

(ex5) 192.168.1.0 / 24 , new mask /26

⇒ no of valid subnets = $2^2 - 2 = 2$ subnets

no. of hosts = $2^6 - 2 = 62$ hosts

subnet mask 255.255.255.192

(ex6) we've the network 172.16.0.0 & we need to divide it into 100 subnets containing 500 hosts

find (a) default subnet mask (b) new subnet mask to fulfill these requirements

Sol^n (a) default subnet mask, ∵ 1st octet = 172 ⇒ class B

→ 172.16.0.0/16

→ 255.255.0.0

(b) 100 subnet → at least 7 bits

500 subnet → at least 9 bits

new subnet mask | 172.16.0.0 / 23 |

or | 255.255.1111 1110.0000 0000 |

| 255.255.254.0 |

(ex7) for the host 192.168.16.17/29

find the subnet ID & Broad cast ID

Sol^n Subnet mask 255.255.255.1111 1000 ⇒ 255.255.255.248

to get subnet ID, make ANDing bet. host ID & subnet Mask

192.168.16.00010001

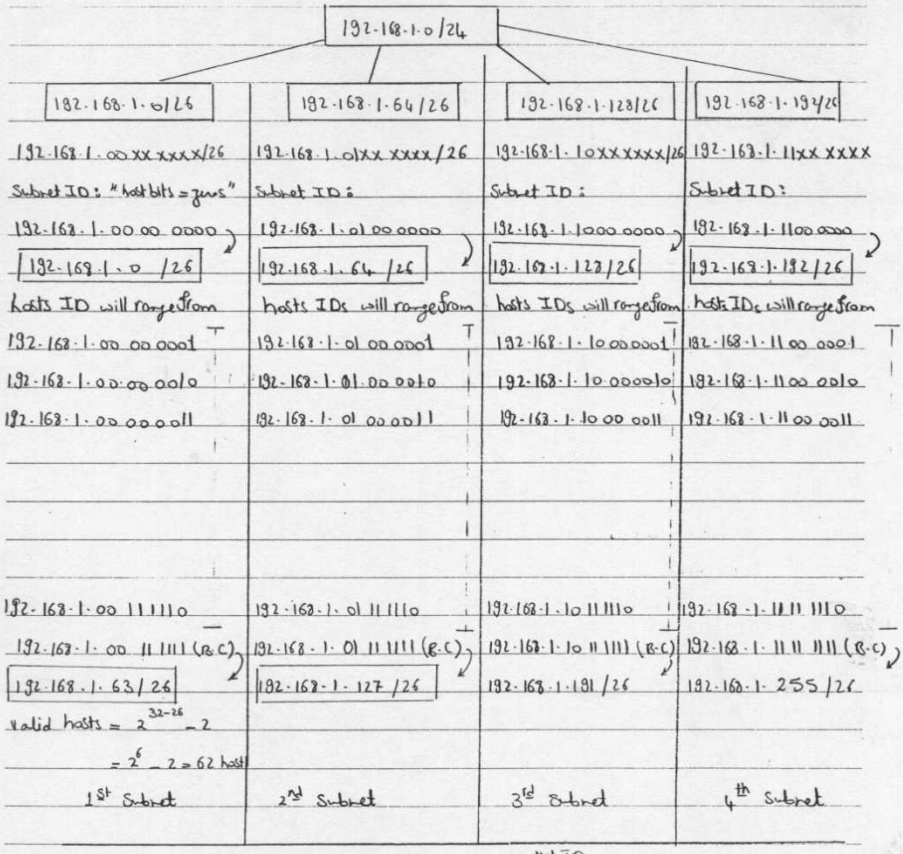
255.255.255.11111000 } AND

subnet ID = 192.168.16.00010000 = 192.168.16.16 / 29

OR Net. ID 192.168.16.00010 000 (N, SN, H), B.C ID 192.168.16.00010 111 (N, SN, H)

→ 192.168.16.16/29 → 192.167.16.23/29

ex(8) :- 192.168.1.0 | 24 , new mask /26



N.B: (1) When we count no of valid hosts = $2^6 - 2$ (Net ID, B.C ID)

(2) When we count no. of valid subnets = $2^2 - 2$ (1st Subnet, last Subnet) } both're not used

because (i) The 1st subnet has an ID = Net. ID of the major Network

(ii) The last subnet has a direct B.C ID = B.C ID of the major Network

(ex 9) What is the difference between 192.168.1.64/24 & 192.168.1.64/26

192.168.1.64/24
N H
192.168.1.0100 0000/24 } host ID

192.168.1.64/26
192.168.1.0100 0000
N host } Subnet ID

A procedure to solve this kind of problems

Subnet Mask
(1) get new subnet mask in dotted decimal
(2) get interesting octet value
(3) get hop = 256 − interesting octet value ⟹ Key 1

IP Add
(4) get 1st subnet = major network ⟹ Key 2
(5) get further subnets by adding hop (Key 1) to the interesting octet of previous subnet

(ex 10) 192.168.1.0/24 get new mask /26

(1) new subnet mask : 255.255.255.192
(2) Interesting octet value = 192
(3) hop = 256 − 192 = 64

1st Subnet	2nd Subnet	3rd Subnet	4th Subnet
ID: 192.168.1.0/26	ID: 192.168.1.64/26	ID: 192.168.1.128/26	ID: 192.168.1.192/26
B.CID: 192.168.1.63	B.CID: 192.168.1.127/26	B.CID: 192.168.1.191/26	BC: 192.168.1.255/26

no of valid hosts/Subnet = $2^{32-26} - 2$ = 62 hosts

ex(11) default ID 200.0.0.0/24 , new mask /27

(1) new subnet mask 255.255.255.224 , no of subnets = $2^3 = 8$

(2) value of interesting octet = 224 no of valid hosts = $2^5 - 2 = 30$ h/ subnet

(3) hop = 256 - 224 = 32

1st Subnet ID : 200.0.0.0/27 → unvalid		1st Subnet B.C ID : 200.0.0.31/27	
2nd " " : 200.0.0.32/27		2nd " " " : 200.0.0.63/27	
3rd " " : 200.0.0.64/27		3rd " " " : 200.0.0.95/27	
4th " " : 200.0.0.96/27		4th " " " : 200.0.0.127/27	
5th " " : 200.0.0.128/27		5th " " " : 200.0.0.159/27	
6th " " : 200.0.0.160/27		6th " " " : 200.0.0.191/27	
7th " " : 200.0.0.192/27		7th " " " : 200.0.0.223/27	
8th " " : 200.0.0.224/27 → unvalid		8th " " " : 200.0.0.255/27	

(ex12) determine wheather this is a host, network or B.C ID

192.168.168.167/27

192.168.168.1010 0111 ⇒ host ID

N host

Net ID 192.168.168.160/27

B.C ID 192.168.168.191/27

(ex13) find direct B.C ID for the network that contains host 192.200.1.77/27

host ID 192.200.1.0100 1101 ∴ Net ID 192.200.1.64/27

N H B.C ID 192.200.1.95/27

(ex14) What is the type of the IP 172.16.5.0/23

172.16.0000 0101.0000 0000 ⇒ host ID

N H ⇒ Net ID 172.16.4.0/23

⇒ B.C ID 172.16.5.255/23

Another Sol. ⇒ Subnet Mask = 255.255.254.0 , interesting octet value = 254

hop = 256 - 254 = 2 ⇒ 1st Subnet ID 172.16.0.0

172.16.2.0

B.C ID 172.16.5.255 ← 172.16.4.0

172.16.6.0

Session (9)
10/05/06

ex : for this address 192.168.1.137/24 use the new mask /27
to solve this problem we've 3 solns

method (1) : (Subnet mask) And (IP Add-) = Network ID

new Subnet mask = 255.255.255.1110 000 ⇒ /27
= 255.255.255.224

192.168.1.1000 1001 — 137
255.255.255.1110 0000 — −128
Net ID ⇒ 192.168.1.1000 0000 = 192.168.1.128/27 — 9

to get B.C ID Set All host bits = 1s

B.C ID ⇒ 192.168.1.1001 1111 = 192.168.1.159/27 — 128 + 31 = 159

method (2) 192.168.1.1000 1001 /27
N H

host bits = 0 , Net ID 192.168.1.1000 0000/27 = 192.168.1.128/27
host bits = 1 B.C ID 192.168.1.1001 1111/27 = 192.168.1.159/27

method (3) (1) new Subnet mask = 255.255.255.11100000
/27 = 255.255.255.224

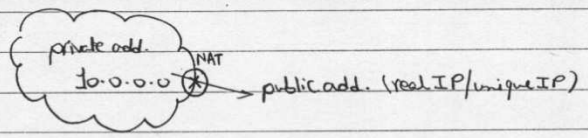
(2) value of Interesting oCtet = 224

(3) hop = 256 − 224 = 32

(4) 1st Subnet 192.168.1.0/27
2nd 192.168.1.32/27
3rd 192.168.1.64/27
4th 192.168.1.96/27
5th 192.168.1.128/27 ∴ Net ID = 192.168.1.128/27
6th 192.168.1.160/27 B.C ID = 192.168.1.159/27

Shortage of IPs "Cont'd" — II - private addressing

- private address ≠ public (real) address.
- The IANA assigned a range of private addresses, that can be given to devices in an internal network (LAN) & that add. can be repeated in any other LAN with no restrictions, ex: 10.0.0.0 .
- NAT is a certain protocol used to change private add. → public add. that can be used on the internet (NAT ≡ Network Address Translation)



Standard private addresses

Class A : $\underset{N}{10}.\underset{H}{0.0.0} \Longrightarrow \underset{N}{10}.\underset{H}{255.255.255}$

1 Network, $2^{24} - 2$ hosts/network

Class B : $\underset{N}{172.16}.\underset{H}{0.0} \Longrightarrow \underset{N}{172.31}.\underset{H}{255.255}$

16 Network, $2^{16} - 2$ hosts/network

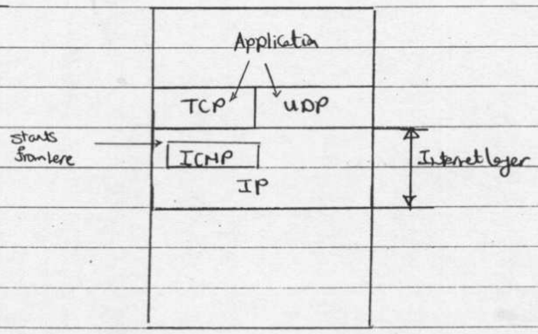
Class C : $\underset{N}{192.168.0}.\underset{H}{0} \Longrightarrow \underset{N}{192.168.255}.\underset{H}{255}$

256 Network, $2^{8} - 2 = 254$ hosts/network

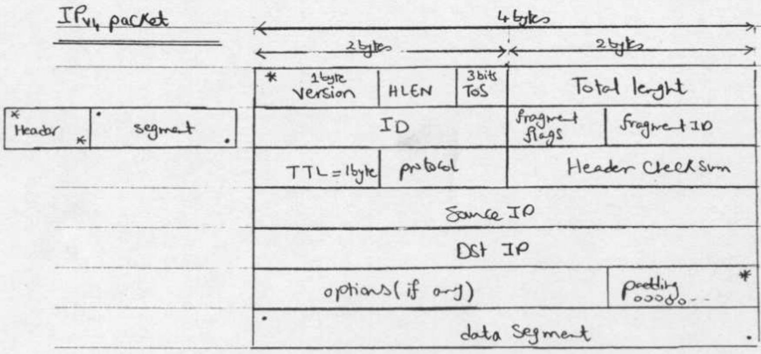
III IPv6 : consists of 128 bits i.e we'll have 2^{128} IPs (↑↑↑)
this will transfere us to what is called Internet II

Back to IP_{v4} :- (1) logical Addressing
(2) Support End – to – End delivery

- IP_{v4} is a connection less protocol i.e best effort delivery (it is ok as TCP will adjust every thing)
- Connectionless protocol ≠ connection oriented protocol
  ↳ ال protocol يفتح session قبل ال transmitting
  i.e يتأكد ان هنالك شبكة قبل ما يبعت ال data
  +
  يتأكد من وصول ال data صح



IP_{v4} packet

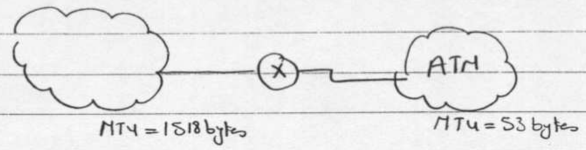


<u>Version</u> : IP_{v4} or IP_{v6} (with IP_{v4} it is equal 4 as follow : 0000 0100)

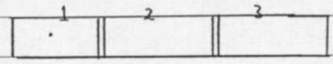
<u>HLEN</u> : Header lenght , header lenght min = 20 bytes

<u>ToS</u> (Type of service) : priority of our data it ranges from 0 → 7 (3 bits)

browsing (ToS = 3) , voice (ToS = 5) , (ToS = 6 & 7) → for protocols that adjust the network.



∴ data is fragmented to pass on networks with less MTU



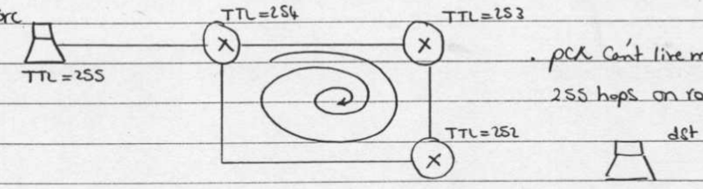
fragmentation

<u>ID</u> : Is the same for all fragments of the same pck & it is used to reassemble fragments of the pck

<u>fragment ID</u> : The sequence no. that the fragment takes

<u>fragment flag</u> : one of its bits states wheather there're other fragments in the pck left or not.

<u>TTL (Time To Live)</u> : It is a 1 byte header, used to remove L3 loops, TTL 0 → 255



. pck can't live more than 255 hops on routers.

if our pck enters a loop, its TTL will decrease until it reaches 0 & then been discarded.

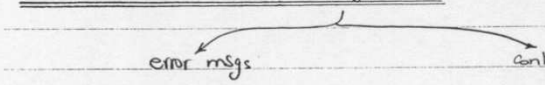
<u>protocol</u> : upper layer protocol (UDP, TCP, ICMP) ⇒ useful for dst.

<u>Header CheckSum</u> : It is the error detection on the whole header.

<u>padding (0's)</u> : padding bits are all zeros , added to make data in multiple of 4 bytes (يعني مثلا لكن ال 4bytes)

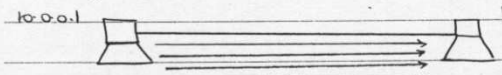
N.B:- In the Internet layer, we've some protocols work beside each others like IP & ICMP, but still IP protocol is the most famous one.

ICMP (Internet Control messeging protocol) : exists in Internet layer



(1) ICMP echo request (control msg)

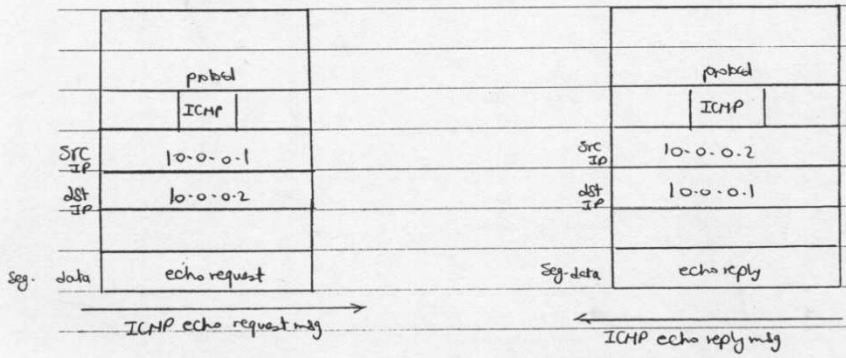
- Ping command initiates ICMP echo request msg.



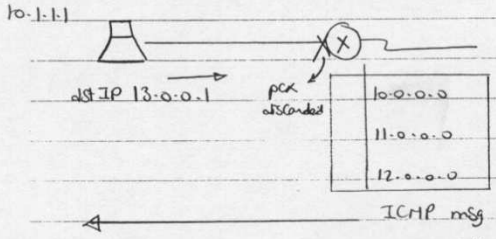
Ping 10.0.0.2 (i.e T^x a msg to a dst. & waits for reply)

(2) ICMP echo reply (control msg)

- Cisco 0.5 T^x 0.5 request msgs.
- window 0.5 T^x 4 request msgs



(3) ICMP Network unreachable msg (error msg)



ICMP msg is sent from the Router to the PC to tell it that this is unreachable Network.

Session (10)
13/3/06

lab(1)

Routers & Switches S/W components

(1) Cisco IOS (Internetwork operating System)

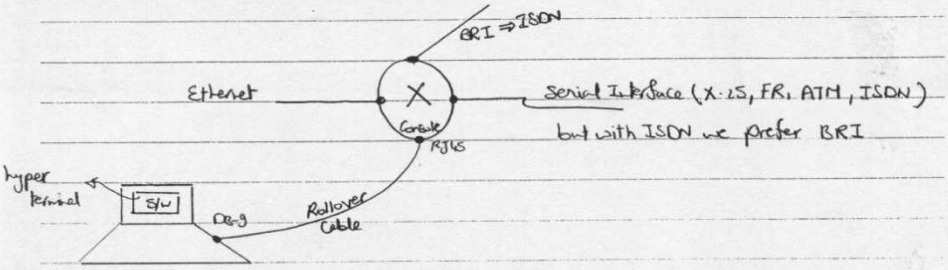
- It is the OS used to manage H/W devices like switches & Routers.
- It is stored in flash memory & excuted every time the router boots up.

(2) Configuration file

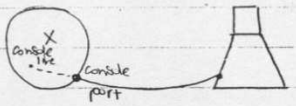
- It is the program file that contains commands, that tells the router how to react with the Network.
- It is stored in NVRAM & excuted every time the router boots up.

N.B :- switches make its action in H/W but its O.S ⇒ S/W

* How to perform configuration file



Interface ⇒ physical port (carry data traffic)
line ⇒ virtual port (carry config.)



to configure a Router we're 2 ways

(1) using console line : when the PC is directly connected to the Router through a rollover cable & we make configuration using the hyper terminal sw (config. for 1st time, giving IPs for the interfaces)

(2) using VTY (Virtual terminal lines) : VT0 → VT4 , used with remote configuration using Telnet application for example

to do this we need (1) IP add. of the interface
(2) no shut down for interfaces
(3) VTy password

VTys ≡ Remote consoles, each Router has at least 5 VTys

Configuration modes

(1) Setup modes : — It is a [Y/N] configuration dialogue, but it supports only simple configuration.
— It appears when Router boots up & there is no config. in the NVRAM
— It helps if you're pressed in time or you forgot config. commands
— 1st question : " Do you want to enter initial config. dialog? " [Y/N]
to exit that mode from the beginning use ⇒ N
" " " " at any time use ⇒ Ctlr + C

(2) Execution modes : CLI (Command Line Interface) ⇒ Sw interface to write commands that'll be executed line by line.

- (2-1) user mode
- (2-2) privilege mode
- (2-3) Global config. mode
- (2-4) Sub-Config. mode

(2.1) User mode : Router> ——
↳ name of the Router, may be Cairo, Alex, ——

- This mode only supports Simple monitoring & Simple trouble Shooting
(Some show commands, neighbours) ↳ (ping, telnet, traceroute)
- on this mode we can make no configuration

(2.2) priveledge mode (Enable mode) : Router ## ——
↳ name of the Router, may be Cairo

- It supports advanced monitoring & trouble Shooting
(all Show commands) ↳
- On this mode we can make no configuration

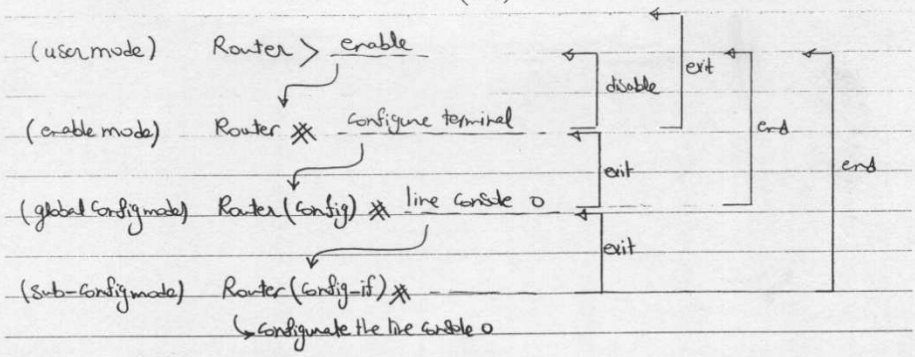
(2.3) Global config. mode : Router (config) ## ——

- It supports commands that affect the entire system
ex: putting a name or password for the Router
- on this mode we can make no Showing

(2.4) Sub-config mode : Router (config-if) ## ——

- It supports commands that affect a specific part of the router
ex: configure Interfaces, lines, routing protocols.
(Serial 0, Ethernet 0) ↳ (console line, VTy lines)
- On this mode we can make no Showing

N.B:- to Enter this modes we should enter them by order بالترتيب



IOS features :-

(1) context help :- `>?` `#?` } shows all the commands in that mode

(2) abbreviation feature :- `>en` → instead of writing enable
`# conf t er` → = configure terminal
`(config) # int s 0` ⇒ = interface serial 0
`(config) # li c 0` ⇒ = line console 0

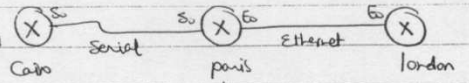
(3) Editing feature :- Ctlr + P → up arrow (previous command)
Ctlr + B → back letter (left arrow)
Ctlr + F → Fwd = (Right =)

(4) Ctlr + Z = end (return to enable mode)

(5) "Tab" button ⇒ auto complete for the command.

ex :- file → new net map

Router Model 2610
- Ethernet Interface fixed
& 2 Slots for WAN



paris ⇓

Router Model 2611
- Ethernet Interface fixed
& 2 Slots for WAN

* Back to our CLI ⇒ click on [cRouter ▼] to choose Router to config

Router > enable ↵

Router # show flash ⇒ information on flash Memory

→ IOS = c2600-js-mz.12.1-9.T.bin
→ version

Router # show version ↵

→ System Image file ( )

Router uptime 4 min → الوقت اللي الـ Router شغال فيه

32K NVRAM → RAM that save the config. file

8M flash memory

*Config register 0x2102 → controls the boot up

Router # config t ↵

Router (config) # hostname Cairo ↵ (to give a name to the Router)

Cairo (config) # banner motd $ ↵ (to put a welcome msg)
↓ msg of today

// Hello, I'm Amr" $ ↵ msg رسالة بتعرض أول ما حد يدخل

Cairo (config) # enable password cl ↵ (to put non-encrypted pass.)

Cairo (config) # exit ↵

Cairo # show run ↵ (to show the active config. file)

Cairo # show ▾ run ↵

name Cairo

password a1 → ممكن أى حد يعرف ال password لو سبت الجهاز شغال

Cairo #

Cairo(config) # enable ▾ secret ▾ a2 ↵ (to put secret encrypted password)

Cairo(config) # exit ↵

Cairo # show ▾ run ↵

name Cairo

password a1

secret xxxxxxxx → secret encrypted password

Cairo # exit ↵

" Hi my name is amr "

Cairo >

password : a2 ↵ → he will ask for the secret password to enter enable mode

Cairo # conf ▾ t ↵

Cairo(config) # no ▾ enable ▾ password ▾ a1 ↵ (to remove password)

Cairo(config) # no ▾ enable ▾ secret ▾ a2 ↵ (to remove secret password)

N.B :- we can also put a password on the console port or VTy lines so as to not permit anyone to alter the config. except with a password.

Cairo(config) # line ▾ console ▾ 0 ↵ (to conf. the console line)

Cairo(config-if) # password ▾ amr ↵

Cairo(config-if) # login ↵ (to activate the password)

Cairo(config-if) # exit ↵

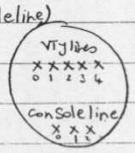
Cairo(config) # line ▾ vty ▾ 0 ▾ 4 ↵ (to config. the VTy lines)

Cairo(config-if) # password ▾ amr1 ↵

Cairo(config-if) # login ↵

Cairo(config-if) # end ↵

Cairo # exit ↵

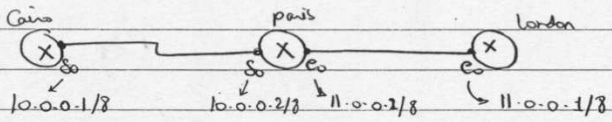


Direct connection (console)	No direct connection (Telnet)
(1) console password .	(1) Vty password .
(2) secret password .	(2) secret = .

Cairo (config) * service ▼ password ▼ encryption

---

let us take a numerical example



Cairo (config) * Int ▼ S0 ↵
Cairo (config_if) * IP ▼ address ▼ 10.0.0.1 ▼ 255.0.0.0 ↵
Cairo (config_if) * no ▼ Shut down ↵

& He done for paris & london
⇒ Cairo & paris are both DTEs & so one of them should act as DCE to adjust CLK
⇒ to know who is DTE & who is DCE use Cairo * Sh ▼ controller ▼ S0 ↵
paris * Sh ▼ controller ▼ S0 ↵
⇒ for example Paris ≡ DCE ∴ to adjust the CLK use :
paris (config-if) * clock ▼ rate ▼ 64000 ↵

Trouble Shooting on (L1 & L2)

Cairo # show ▾ interface ▾ S0 ↵

or

Cairo # show ▾ ip ▾ interface ▾ brief ↵

S0 is _____ , lin protocol is _____

(cables) status (L1)	protocol (L2)
(i) administratively down	down ⇒ you typed no shut down
no keepalives (ii) down → Cable failure → Interface → other side is shut down	down ⇒ " " "
(L1 is up) (iii) up	down → (L2 is down) missing clk / encapsulation mismatch (2 DTEs) (X) — (X) FR ATM default of Cisco Serial : HDLC
(iv) up	up ⇒ everything is OK till L2

Trouble Shooting on L3 : Cairo # Ping ▾ 11.0.0.1 ↵

. . . . . ← i.e pck sent & failed

Cairo # ping ▾ 10.0.0.2 ↵

! ! ! ! ! ← i.e pck sent & succeeded

Trouble Shooting on L3 (cont'd)

Cairo # Sh ↵ ip ↵ route ↵

C 10.0.0.0/8 is directly connected, Serial 0

i.e ping 11.0.0.0 ⇒ discarded

⇐ يعني كل Router شايف ال Routers الي directly connected ليه فقط ومش شايف ال Routers الي بعيده عنه ⇐ (L3 error)

∴ we should define a Routing protocol

Session (11)
16/5/06

Topics :
* Review
* Routers & switches H/w components
  - Routers boot up process
  - password recovery procedure
  - Saving IoS & config files

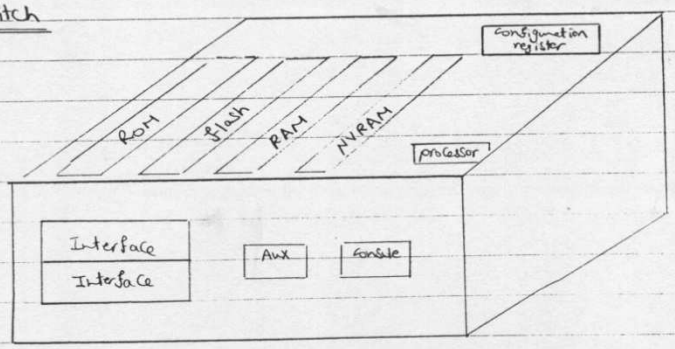
---

* Review :

Internet layer
- logical addressing
- End-to-end delivery
- L3 devices (H/w & S/w) → today

L3 devices (S/w) "Simulation"
- Cisco IoS
- Configuration
  - Console line (config. for the 1st time) ⇒ Setup mode
  - VTy line ⇒ Executive mode
  - Auxiliary line (in Routers only) ⇒ use RJ45 interface
    - Config. for 1st time (direct connection)
    - remote config (by connecting it to a telephone line)

Router or Switch



ROM (Read only)	flash (8M-16M)	RAM	NVRAM (Read write) (32K)	config register	
POST program	IOS file	Active running config files	Startup config file	16 bit mem. according to its value the Router will bootup in different ways 0x---- or hexa . to show the value use #Sh. ver	Interfaces
Boot Strap program	c2600-js-mz.121.bin ⇒ loaded from factory by default	IOS command executive (compiler) used to change comm. in To the log. the Router understand	bootup System commands		
mini-IOS (RX-boot)					
mini-os (low level os)		Routing, arp tables			
		Buffer			

What we need? ⇒ we need to locate IOS & config file & load them

Bootup process (what happens at power on?)

(1) Router will access the ROM

ROM	POST
	Boot Strap

POST (power ON Self Test) : A program that tests all h/w (memories & interfaces) at power on ⇒ يعني لو في mem. بايظة كده كده ال sys.
مش حيقوم , بالتالي لازم اعمل check في الأول

Boot Strap program :- search for valid IOS to boot the system from
↳ ده البرنامج اللي بيقوم ال system
like bios in PCs

(2) Boot Strap program will search for IOS following the next steps
Check the configuration register value (16-bit memory) to know how to bootup

(i) Config. register value is default (0X 2102 → 0X210F) (0X = hexa)

(ii) Config. register value is not default

(i) Configuration register value is default :-
bootstrap prog. will access NVRAM to check for boot system commands

(i.1) no boot system commands (config. for 1st time)

(i.2) There're boot system commands in the config. file
← ممكن نشوف هذا الجزء فقط من ال config file
علشان احنا لسه مجملناش ال IOS .

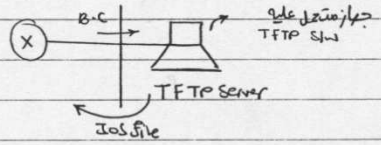
(i.1) No boot system commands exist in the NVRAM

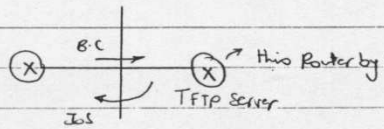
Bootstrap will follow the following sequence

(1) Flash		Search for IOS & load IOS
(2) TFTP Server		
(3) ROM	mini – IOS	
	mini-OS (ROMMON)	

(1) 1st the boot strap prg. will search in the Flash memory for an IOS file, if it didn't succeeded it will do the 2nd step.

(2) TFTP (Trivial file transfere protocol) Server : Bootstrap prg. will send a B.C msg to ask for a version of IOS on any PC/Router that is a TFTP server, if he failed he will jump to the 3rd step





(3) boot strap program will access the ROM to load either mini-IOS (exist in expensive routers only) or mini-OS (ROMMON) which exists in all Routers

mini-IOS : like Some mode on PCs, used to recover your IOS in Any way

min-OS (ROMMON) : like DOS on PCs, helps you to recover back your IOS

(low level OS) → used for → IOS recovery
→ password recovery

(i.2) If there are previous boot system commands in the config file in the NVRAM

Boot system commands may be

(1) Router(config) # boot system flash ↵
i.e boot up from the flash memory, if failed boot up from mini-OS (ROM MON)

(2) Router(config) # boot system TFTP ↵ i.e boot up from TFTP server & if failed
he will ask for path → IP boot up from mini-OS (ROM MON)
& file name → file name

(3) Router(config) # boot system ROM ↵ i.e boot up from mini-IOS & if failed boot up from mini-OS (ROM MON)

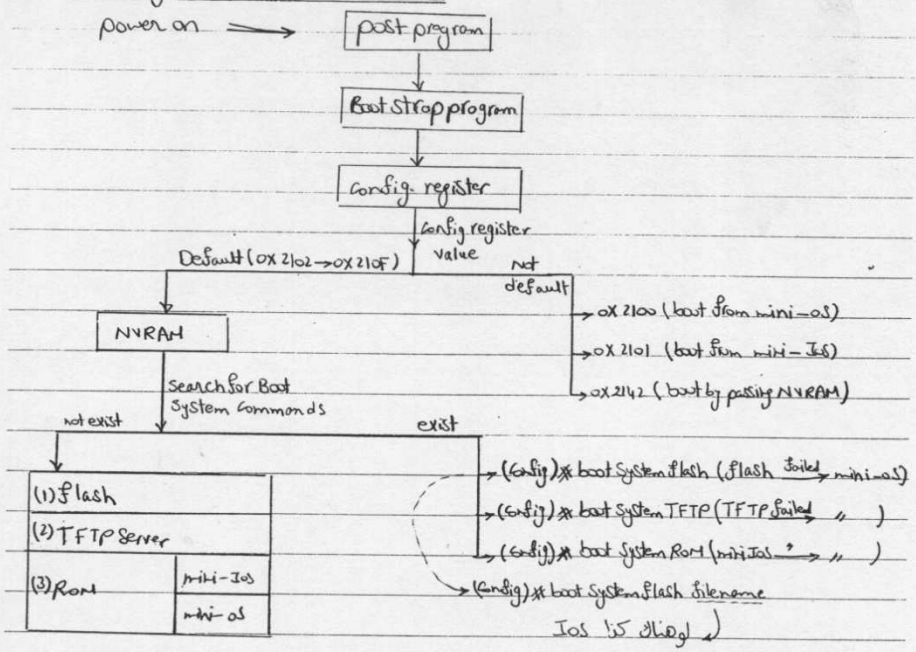
→ If we write these 3 commands ∴ they'll be excuted 1 by 1 & if they all failed
∴ Router will boot up from mini-OS (ROM MON)

(ii) Config register value is not default (≠ 0X2102 → 0X210F)

Config register value
- → 0X2100 ⇒ boot up from mini-OS (ROM MON)
  boot chact.
- → 0X2101 ⇒ boot up from mini-IOS (ROM boot)
- → 0X2142 ⇒ boot up by passing the NVRAM, starting at setup mode (useful in password recovery)

* to change the value of config register use
Router(config) # config-register 0X

* Summary on how we locate Ios



(3) Now Ios is loaded & it will take full control & will try searching for config. file

(1) NVRAM	Search for config. file
(2) TFTP Server	
(3) Setup mode (console)	

(1) NVRAM (Non-volatile RAM): It contains a back-up of the post configuration mode, this backup is taken & saved from the active config file in RAM to the NVRAM

At system up a copy is taken from NVRAM → RAM

(2) TFTP : The Router will search for config. file on other TFTP server

(3) Setup mode (console) : ... i.e config for 1st time

Some Shows

(1) To know the value of config register use

Router # Sh v version

(2) To know running config in RAM use

Router # Sh v run v config or Run # Sh v run

(3) To know the past config in NVRAM use

Router # Sh v start

(4) To know the inf. on flash use

Router # Sh v flash

default value for conf. register

no bootup commands

Question in exam : In the default router bootup sequence, what will be the default bootstrap access sequence for IOS

ROM	So!	NVRAM
TFTP		flash
NVRAM		TFTP
flash		ROM

Session (12)
16/5/06

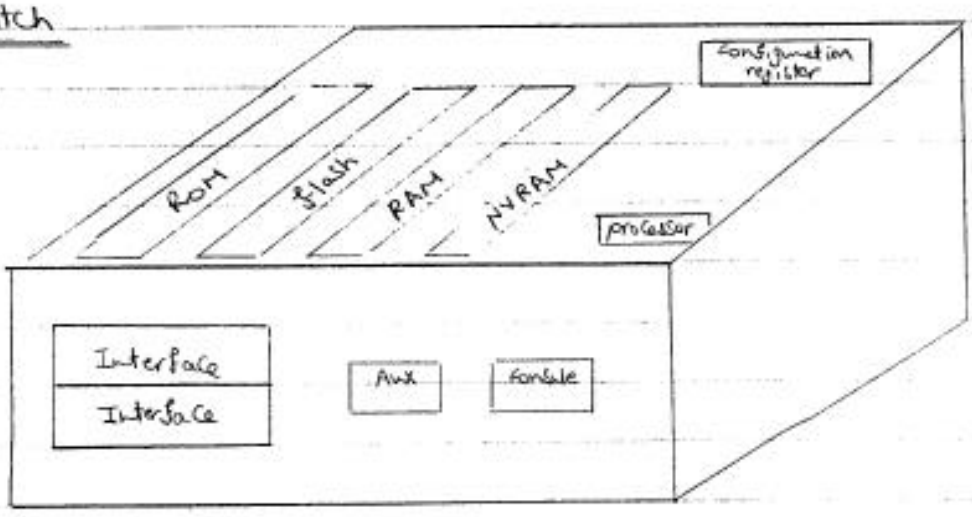
Topics :
* Review
* Routers & switches H/w Components
  - Routers boot up process
  - password recovery procedure
  - Saving IOS & Config files

* Review :

Internet layer
- logical addressing
- End-End delivery
- L3 devices (H/w & S/w) → today

L3 devices (S/w) "Simulation"
- Cisco IOS
- Configuration
  - Console line (Config. for the 1st time) ⇒ Setup mode
  - VTy line ⇒ Executive mode
  - Auxiliary line (in Routers only) ⇒ use RJ45 interface
    - Config. for 1st time (direct connection)
    - remote config. (by connecting it to a telephone line)

Router or Switch



ROM (Read only)	Flash (8M-16M)	RAM	NVRAM (Read-write) (32K)	config register	
POST program	IOS file	Active running config files	Startup config file	16 bit mem. according to its value the Router will bootup in different ways OX — hexa . to show the value use #sh ver	Interfaces
Bootstrap program	c2600-js-mz.121-bin ⇒ loaded from factory by default	IOS command executive (compiler) used to change comm. in to the lang. the Router understand	bootup System commands		
mini-IOS (RX-boot)		Routing, arp tables			
mini-OS (low level OS)		Buffer			

What we need? ⇒ we need to locate IOS & config file & load them

Bootup process (what happens at power on!)

(1) Router will access the ROM

ROM	POST
	Boot Strap

POST (power ON Self Test) : A program that tests all h/w (memories & interfaces) at power on ⇒ يعني لو في mem. بايظة كده كده الـ sys. مش حيقوم, بالتالي لازم اعمل check في الأول

Boot Strap program :- search for valid IOS to boot the system from
↳ ده البرنامج اللي بيقوم الـ system
like bios in PCs

(2) Boot Strap program will search for IOS following the next steps
Check the configuration register value (16-bit memory) to know how to boot up

(i) Config. register value is default
(0X 2102 → 0X210F)
(0X = hexa)

(ii) Config. register value is not default

(i) Configuration register value is default :-
bootstrap prog. will access NVRAM to check for boot system commands

(i.1) no boot system commands (config. for 1st time)

(i.2) There're boot system commands in the config. file
← ممكن نشوف هذا الجزء فقط من الـ config file عشان احنا لسه معملناش الـ IOS

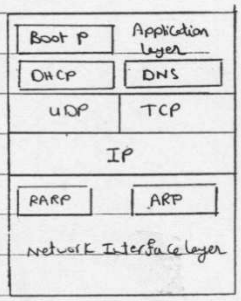
Session (12)
17/05/2006

Topics * obtaining inf. to get started for sending data
- obtaining src MAC
- " src IP
- " dst IP
- " dst MAC

* Transport layer
* Application layer

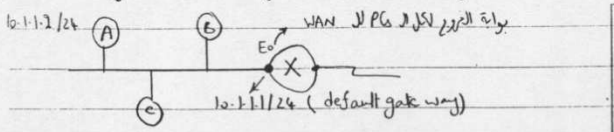
- When a PC is up & it needs to send data, it should know 4 information

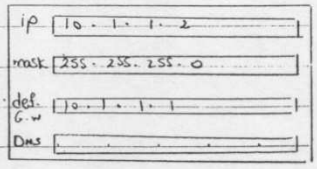
src MAC	src ip	dst ip	dst MAC
H/w add. burnt on ROM of NIC	(1) Manual (Static) (2) Automatic (2.1) RARP (static ip) (2.2) Boot P (2.3) DHCP	(1) Manual (Static) (2) DNS	using ARP protocol



src MAC : - It is a H/w physical add.
- burnt on the ROM of the NIC & the PC can read it at startup.

src ip :
(1) Manual (Static) method : you'll write the IP (usually the private ip), mask, default gate way & DNS IP
- on your PC → my network places "Right click" → choose properties



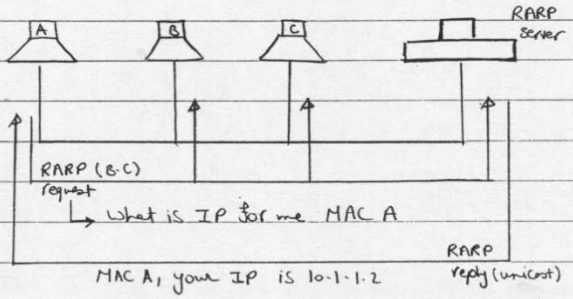


(2) Automatic

(2.1) RARP (Reverse Address Resolution protocol)

- Resolve an known ip to known MAC.
- It is a S/W, when it is setuped on a certain PC then this PC becomes a RARP server (gives IPs for PCs)
- RARP is a layer 2 protocol, i.e it hides in an Ethernet frame.
- The RARP server will form a table bet. different MACs of the PCs & certain allowed IPs but this table should be filled manually & i should know all the MACs
- It is still static ip, as i wrote it in the table

MAC	IP
A	10.1.1.2
B	10.1.1.3
C	10.1.1.4



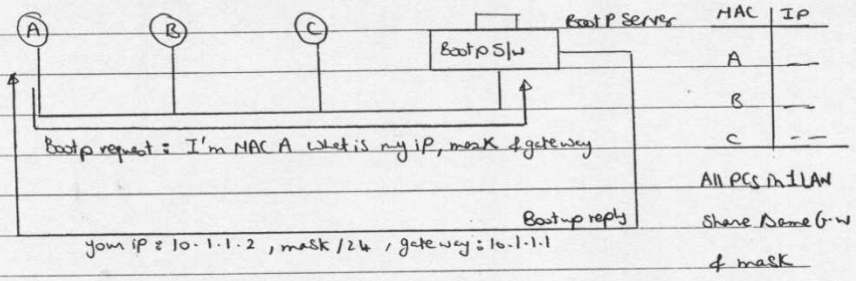
RARP request

dst MAC	src MAC	Type	data	
FFF---FF	A	RARP	RARP request	CRC

- It is sent B.C
- The reply is unicast, from the RARP server → the PC that sent the RARP request
- the RARP request is sent automatically at windows startup
- RARP is a layer 2 protocol, i.e the RARP request is not put in an IP pck but in Ethernet frame because RARP is used only in LANs
- RARP server can't be out of the LAN or in another LAN

(2.2) Boot P (Booting protocol) : may be used in WANS

- Still Static IP, as i fill the table manually.
- Boot p is a layer 7 protocol or S/w, when it is setupped on a certain PC it becomes a Boot P server.
- for a Boot P server we should fill a table between MACs vs IPs
- Boot p request is B.C & the Boot p reply is unicast containg (IP, mask & gateway)



- Boot p is L7 & so it hides in IP pkt & so the Boot p server may be in other LAN
- Boot p request is as follow :

Some Shows:

(1) To know the value of config register use
Router # Sh v version

(2) To know running config. in RAM use
Router # Sh v run v config or Run # Sh v run

(3) To know the past config in NVRAM use
Router # Sh v start

(4) To know the inf. on flash use
Router # Sh v flash

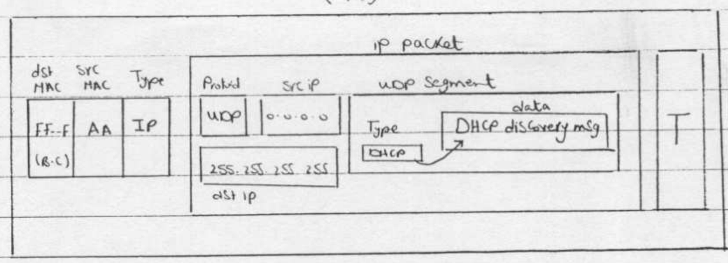
Question in exam: In the default router bootup sequence, what will be the default bootstrap access sequence for IOS

default value for conf. register

no bootup commands

ROM	Sol^n	NVRAM
TFTP		flash
NVRAM		TFTP
flash		ROM

DHCP discovery msg



Src ip : 0.0.0.0 ⇒ أى ip معرفوش يكون شكله بالطريقة دى

dst ip : 255.255.255.255 ⇒ بدوّر على أى حد يكون DHCP server

Src MAC : AA ⇒ The only inf. the PC knows

dst MAC : FF___FF ⇒ B.C

→ 255.255.~~255~~.255 → The Router will change it into a unicast ip in case the DHCP server is out of the LAN in order to search for DHCP server in WAN (N.B : In WANs ⇒ no B.C)

In exam: regarding the first msg sent from DHCP client.

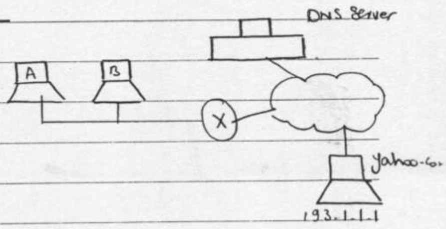
(a) use TCP ((b)) use UDP ((c)) use MAC FF___FF

(d) use unicast MAC (e) use unicast ip

- dst ip

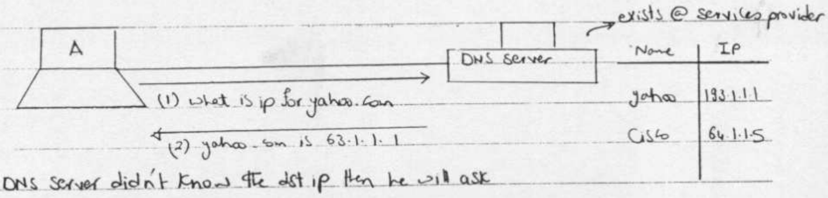
(1) Manually : open Internet explorer & type

193.1.1.1 → yahoo.com



(2) DNS (Domain Name Service) :

- When you type www.yahoo.com ≡ as if you make a DNS request to the DNS server to know the ip of yahoo (dst), where the DNS ip is known from the DHCP offer



Name	IP
yahoo	193.1.1.1
Cisco	64.1.1.5

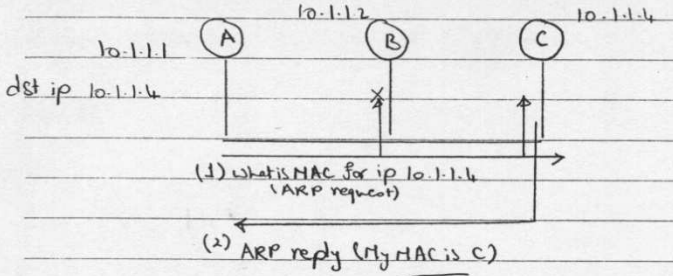
- if the DNS server didn't know the dst ip then he will ask a larger DNS server

dst MAC

ARP (Address Resolution protocol) Resolve unknown MAC to known IP

- It is layer 2 protocol i.e it hides in an Ethernet frame

Case 1 : If dst is in the same LAN (Segment)



الوحيد اللي حيرد هو اللي له ip 10.1.1.4

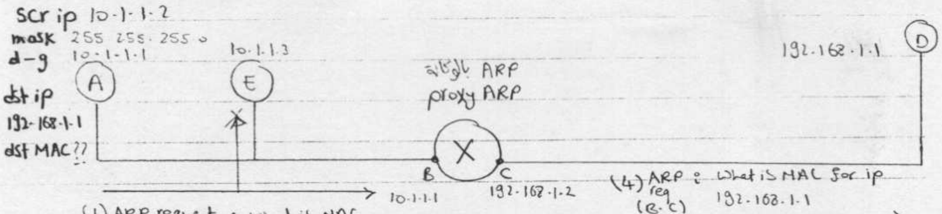
ARP request

dst MAC	Src MAC	Type	data	
FF---FF	A	ARP	ARP request	T

now ARP Table @ A will be as follow :

IP	MAC
10.1.1.4	C

Case (2) If the dst is in another LAN (segment) "Proxy ARP"



(1) ARP request : what is MAC (B.C) **MAC** for 10.1.1.1 "to reach 192.168.1.1"

(2) ARP reply (unicast) : The MAC add. for 10.1.1.1 is B

(4) ARP req (B.C) : what is MAC for ip 192.168.1.1

(5) My MAC is D

10.1.1.0	
192.168.1.0	

RTG Table

ال Router عرف أنه الوحيد اللى ممكن يوصل
A ← D ، عشان كده حط ال MAC بتاعه

(3) data →

dst MAC	src MAC	src ip	dst ip
B	A	10.1.1.2	192.168.1.1

B → Router'll accept it

dst ip → The Router will find that the final dst is not him so he'll check its RTG table & route the data to the proper dst.

(6) data →

dst MAC	src MAC	dst ip	src ip
D	C	192.168.1.1	10.1.1.2

⇒ N.B :- dst & scr ips are the same & don't change, but the nex hop MAC differs

- Each Router & PC make what is called ARP Table (ARP Cache) show IP vs MAC i.e each Router & PC learn each time to not send ARP requests every time

- to show it use

 \# Sh ip arp ↵

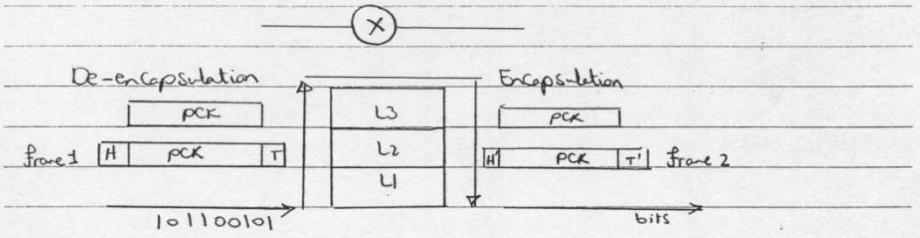
 OR

 \# Sh arp ↵

IP	MAC
192.168.1.1	B

ARP Table for A (ARP Cache)

Framing : The Router makes what is called framing i.e to put the frame into Another type of frame



Frame 1 & Frame 2 are not the same, because the headers are not the same, in WAN H' & T' May be for ATM or FR.

Session (13)
20/05/06

Topics :

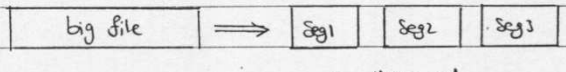
* Transport layer
* Application layer
* Routing introduction

Transport layer — PDU = segment

— host to host communication layer (L2 & L3 devices = SW)

It is responsible for

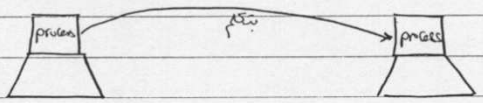
(1) Segmentation :



Small segments

(2) Error detection : using CRC

(3) Addressing through port no's (process address or session Address)



each prog. works on the PC will act as a SW port

port no's 0 ⟶ 65535

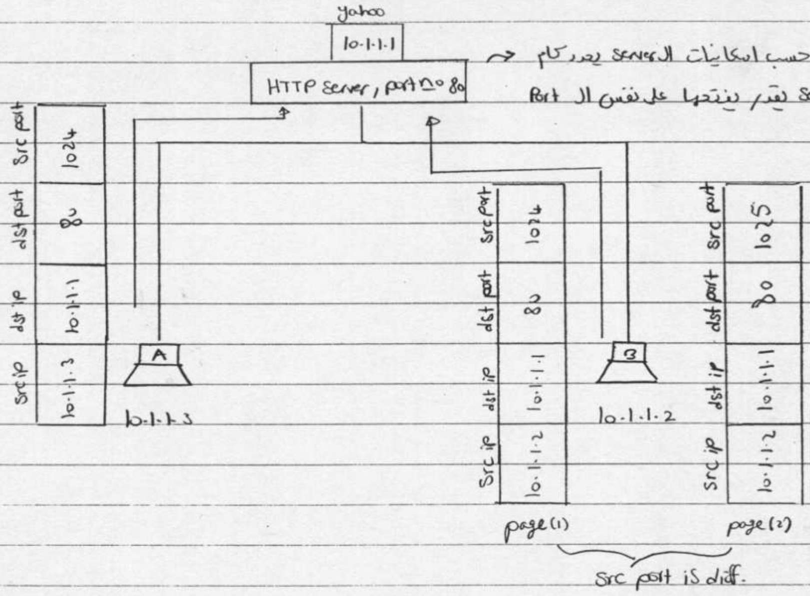
0 → 1023 (for servers)	1024 → 65535 (for client = host PC)
(well known ports)	(unregulated ports)
⇒ Application addresses for servers	⇒ they identify certain process on your PC
ex: 23 → Telnet	⇒ assigned randomly by the O.S for every session established
25 → SMTP	
80 → HTTP	⇒ every session has a unique port no., not repeated on the same PC until the session is terminated, but can be repeated on other PCs
443 → HTTP Secure	
20, 21 → FTP (1 control, 1 data)	

N.B : Socket no. = ip + port no.

(4) Multiplexing many sessions using port no (i.e socket no. = ip + port no)

i.e:
— ممكن كذا PC يتصفحوا نفس الصفحة على HTTP ser في نفس الوقت
— ممكن PC واحد يفتح صفحة على HTTP ser. مرتين وأي action يعمله على أي صفحة يكون الرد على نفس الصفحة.

— على حسب امكانيات الـ server يحدد كام ← session يقدر يفتحها على نفس الـ Port



⇒ عادي ممكن A,B يستخدموا نفس الـ port no ← 1024
عشان أنا بأفتح session عن طريق socket no.
↳ ip + port no ⇒ which is diff.

N.B :-
(1) Segmentation
(2) error detection
(3) Addressing through port no
(4) Muxing many sessions

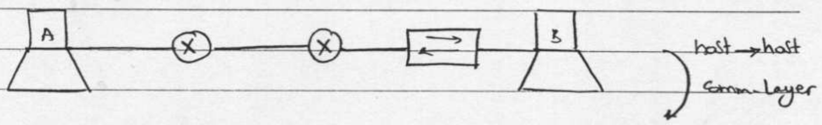
} made by both UDP & TCP

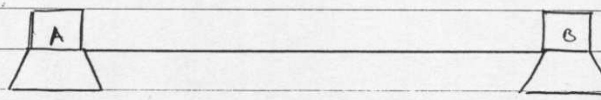
(5) Transport layer supports both

→ connection less (UDP)
  ↳ no establishing / termination / managing of sessions
→ connection oriented (TCP)
  ↳ no transmission before opening a session & make check to know wheathere the data received correct or not.

(6) TCP only make these f^ns "connection oriented"

(6.1) Establish connection/session "3 way handshake" ⟹ نتأكد إن هناك حركة إلى الـ dst





أول واحد هيبعت على الـ Seg. هوه الـ dst.
(حركة ← Router & SW)

(1) SYN (initial seq. no., initial window size) →
A بيقول لـ B عايز أفتح معاك conn.
وأول رسالة صحيحة رقمها مثلاً = t0

(2) ACK / SYN (initial seq. no., intial window size) ←
ACK ↳ وصلتني رسالتك
SYN ↳ عايز أفتح معاك connec.

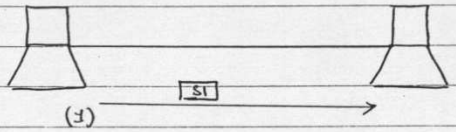
(3) ACK (لازم A يرد عشان B ميفضلش يبعت علطول) →

(6.2) managing | maintenance of connection

(6.2.1) Sequencing : gives seq. no. for each segment so the dst can collect back the whole data.

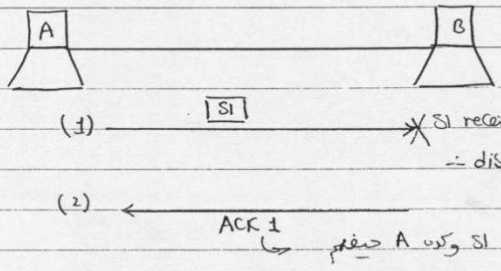
← في الـ UDP بقسم الـ data segments و ابعتهم من غير ما أديهم أرقام

(6.2.2) reliability : ازاي اتأكد ان كل حاجة وصلت صح



ACK 2 ← معناها S1 وصلت وعايز S2

(6.2.3) error correction : by discarding the errored segment & asking the src for retransmission

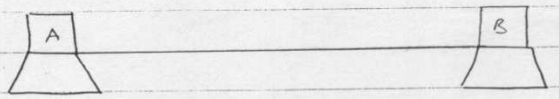


ACK 1 ← معناها A وصلت S1 وعايز S1 تاني

(6.2.4) flow control : (windowing ≡ positive ACK with retransmission (PAR)) ← exam

seq. لازم retransmit لو ACK جالي بعد وقت معين

- window size : no. of segments that can be sent before waiting ACK.
  & this information is sent in SYN msg at 3 way handshake.



(1) SYN (window size = 2)

(2) ACK / SYN (window size = 3)

(3) ACK

S1

S2

B will wait until ACK is received or a certain time expired & in this case he will retransmit S1 & S2

ACK 3 / SYN (window size = 3)

S3

S4

expired

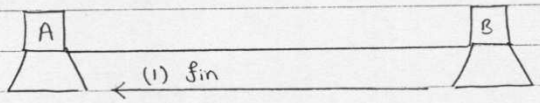
S5

ACK 5 / SYN (window size = 2)

S5

S6

(6-3) Termination of connection "4 way handshake"



(1) fin

(2) ACK

PCA will wait a certain time to know if anything is needed

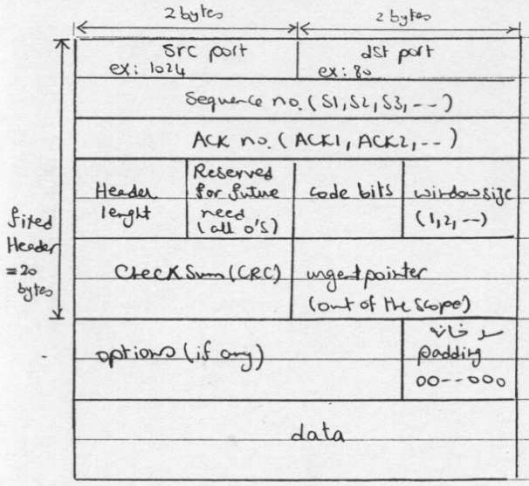
K

(3) fin

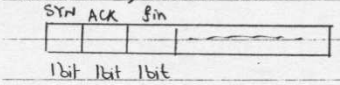
(4) ACK

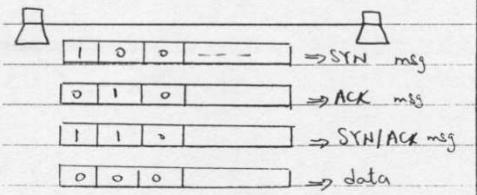
TCP vs UDP Segments

TCP Segment



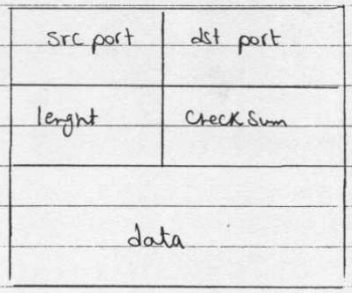
- Code bits ⇒ control bits





- N.B (1): for ACK msg there is no data only header.
- N.B (2): when i send data ∴ ACK no = 0's

UDP Segment



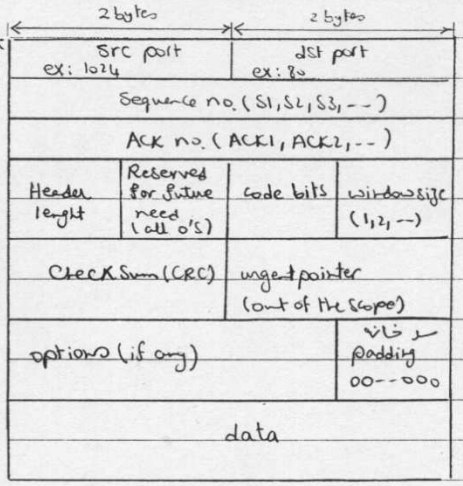
* no sequencing ⇒ no seq. no
  no reliability ⇒ no ACK no.
  no flow control ⇒ no window size
* addressing through port no. ⇒ src port, dst port

error detection ⇒ Check Sum

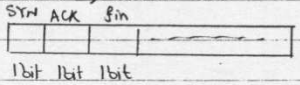
In exam: differences / similarities bet. TCP & UDP

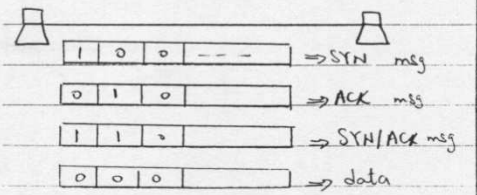
TCP vs UDP Segments

TCP Segment



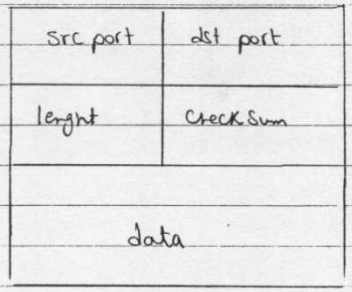
- Code bits ⇒ control bits





- N.B (1): for ACK msg there is no data only header.
- N.B (2): When i send data ∴ ACK no = 0's

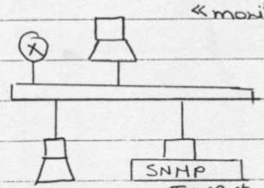
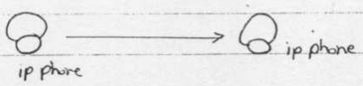
UDP Segment



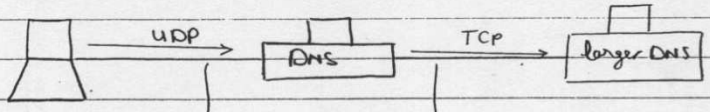
* no sequencing ⇒ no seq. no.
  no reliability ⇒ no ACK no.
  no flow control ⇒ no window size
* addressing through port no. → src port, dst port
  error detection → Check Sum

In exam: differences / similarities bet. TCP & UDP

Application layer: to work with TCP or UDP ⇒ this depends on the Application you use.

TCP	UDP
_ FTP	_ TFTP (Trivial file Transfere protocol)
_ HTTP (Browsing)	↳ for small files
_ SMTP (dst is far & we need ACK)	↳ Applic. layer will be responsible for sequencing, reliability, ... & no need for 3 way handshake/...
_ Telnet (need reliability	_ Bootp (to know src ip)
	↳ كلمو رد عطاها عنوان ال IP بتاعى و الا لأه
	_ DHCP (to know src ip)
	_ SNMP (Simple Network management protocol)
	↳ S/W setupped on some devices to become SNMP server & its responsibilit is
	(1) جهاز حصلته عيب وانا بالحق
	(2) أعمل spy من حاجة بتحصل على الشبكة «monitoring»
	
	_ RTP (Real Time Transport protocol)
	
	⇒ voice transmission is using UDP but @ first opening a session (signaling) ⇒ TCP

TCP	UDP
- DNS (protocol that gives me the dst ip)	- DNS (protocol that gives me the dst ip)



- لو الوقت أنا عارف الـ DNS ip فأنا أذهب لـ DNS Server بأقله عبر الـ ip بتاع الـ dst معين يكون ذلك عبر بروتوكول UDP
- لو الـ DNS Server اللي عارف الـ DNS Server يسأل الـ dst ip أكبر منه ويكون ذلك TCP (1) 3 way handshake (2)

⟹ Now we finished the Introduction & we'll go to the real course

Routing protocols

Static Routing

- Build the RTG Table manually with fixed entries

Network	Int
10.0.0.0	S_0
11.0.0.0	S_1

- used if only 1 Simple path to destination is available
- ex:
  - * Static route.
  - * default Static route.
  - * default Network

Dynamic Routing

- If multiple paths to dist are available

Category (1)

IGP
(Interior GW protocol)
"work within Autonomous System"

examples of IGP

- Distance vector
  - ex: RIP v1
  - IGRP
    - Cisco invented it
- Link State
  - ex: OSPF
  - IS-IS
    - CCNP

merge bet. 2 cats

Advanced Distance vector (Hybrid)

ex: RIP_{v2}

EIGRP (Enhanced IGRP)

Cat (2)

EGP
(Exterior GW protocol)
"work bet. Autonomous Systems"
- translate bet. IGPs or bet. routing protocols

ex: BGP
(Border GW protocol)
In CCNP

Autonomous System : – A group of devices that have single administration or have single routing policy

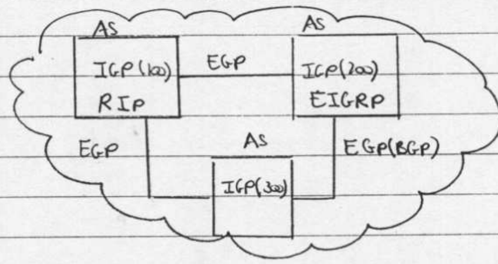
– i.e group of devices work with certain criteria & have compatability with each other

– AS ≡ 1 Routing policy (protocol ⇒ CCNA في ال)

– ex: link → AS

Egynet → AS

Internet → group of ASs



N.B

→ The Routing protocols's target is to form the RTG Table.

→ The RTG Table contains the best protocol & the best path.

(Q1) How to choose the best protocol ?

Ans : The protocol that have the least Administrative distance is the best.

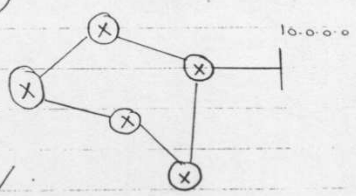
Administrative distance : A no. bet. 0 → 255 given to every protocol indicating the trustfullness of this protocol.

← رقم يعبر عن مدى مصداقية ال protocol

i.e (Best protocol ≡ least admin distance)

example :

protocol		Admin
RipV1	10.0.0.0	120
EIGRP	10.0.0.0	90 ✓



Protocol	Admin dist.
C	0
S(Static)	0 or 1
D(Dynamic RTG protocol)	20 → 170

directly connected ← C

(Q2) How to get the best path?

i.e If one protocol gives u 2 paths to dst, which path would you choose?

The Best path ≡ least metric → معيار

Metric (, معيار) may be :

- → hop : less hops to dst is better.
- → BW : شارع عريض وشارع آخر ضيق
- → delay : path gives less delay is better
- → load : we may have large BW but used by all people (utilization)
- → cost : المشقة ⇒ عن طريق الـ B.W أو الـ delay
- → reliability : أد إيه الشبكة بتقوم , تقع
- → MTU (Maximum Transmission Unit) : As MTU is large, then we don't have to divide the data & that is better.

⇒ Any protocol use only 1 metric (Rip, ...)

⇒ Cisco Routers use all of these metrics using a certain equation.
↳ (IGRP, EIGRP)

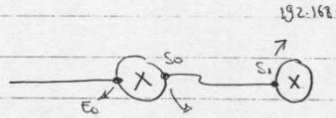
Session(14)
22/05/06

Topics :
- Static Routing
  - (1) direct connected
  - (2) Static Route
  - (3) default Static Rout
  - (4) default network
- Dynamic Routing
  - (1) IGP
    - Distancevector operation

Routing protocols(methods)

(1) Static Routing : used if there is a single path bet. scr & dst

(1.1) Direct connected



- no need to define a routing protocol as you're directly connected
- mask is very important information & should be known.
- The Router can form the Routing Table of the directly connected Networks to him through the ip & mask i give for its ports.

protocol	IP/mask	Int.
C	10.1.1.0/24	E0
C	192.168.1.0/24	S0

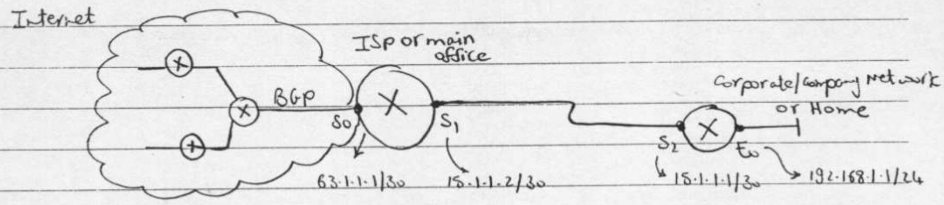
automatically generated → RTG Table

(1.2) Static Route : Build your Routing Table manually

↳ this is used with the Internet Service provider's Routers (ISP)

* Use the following config. command

(Config)# ip route dst Net add dst Netmask { name of o/p interface or ip of next hop }



C	63.1.1.0/30	S0
C	15.1.1.0/30	S1
B	———	S0
B	———	S0

RTG Table of ISP

يعني الـ ISP Rout. شايف كل شبكات العالم ع الـ Int. عن طريق S0 وإتعلم هذا الكلام عن طريق الـ protocol الي اسمه BGP ← "B"

- only ISP Routers can work with BGP protocol (الـ Routers الكبيرة)

C	15.1.1.0/30	S2
C	192.168.1.0/24	E0

RTG Table of Corporate Router

وعشان هذا الـ Router يقدر يوصل للـ Internet نستخدم (1.3) default Static Route as this Router can't learn to work with BGP

⇒ عشان الـ ISP Router يتعلم الشبكة الي عندها 192.168.1.0/24 لازم نعمل config.

(i) (config)# ip route 192.168.1.0 255.255.255.0 S1 ⇒ مباشرة

OR

(ii) (config)# ip route 192.168.1.0 255.255.255.0 15.1.1.1

} ISP or Main office

What is the difference bet. (i) & (ii)

(i) using S1

- RTG Table

C	63.1.1.0/30	S0
C	15.1.1.0/30	S1
S	192.168.1.0/24	S1

(S → Static)

- administrative distance = 0

- used if the Router connection is point - to - point

(ii) using ip of next hop 15.1.1.1

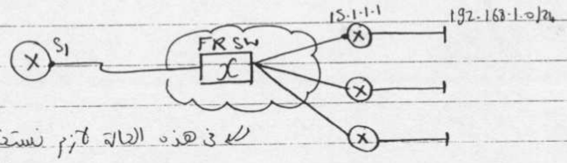
- RTG Table

			next hop
C	63.1.1.0/30	S0	
C	15.1.1.0/30	S1	
S	192.168.1.0/24	S1	15.1.1.1

- administrative distance = 1

عشان لسه حنرجع لل Router
عشان إحنا بنقول له ان طريق ال packets
لل net. اللي تحتها 192.168.1.0 هوه نفس
الطريق لل net. اللي تحتها 15.1.1.0

- used if the Router connection is point - to - multipoint.



في هذه الحالة لازم نستخدم (ii) أي مع طريقة
ال nexthop وإلا قال ال FR SW يعمل لها
discard

→ to change the admin distance use the following config command

ISP(config)# ip route ▾ dst net add. ▾ dst net mask ▾ { name of o/p int. or ip of next hop } ▾ [distance]

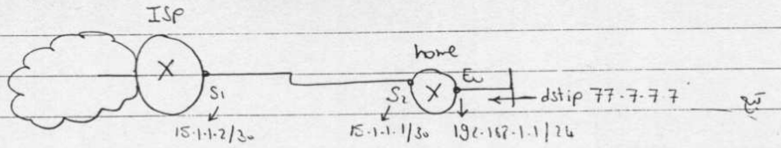
[distance]: 0 → 255 — optional may be not written, by default (0 or 1)

(1.3) Default Static Route : Gateway of last resort ⇒ سكة اللي ملوش سكة

use the following config. command

(config) ※ ip ▿ route ▿ all networks ▿ all masks ▿ { name of o/p interface / ip of next hop }

(config) ※ ip ▿ classless → to activate the default Route, but it is enabled by default (care in exam)



home (config) ※ ip ▿ route ▿ 0.0.0.0 ▿ 0.0.0.0 ▿ S_2

home (config) ※ ip ▿ classless

OR

home (config) ※ ip ▿ route ▿ 0.0.0.0 ▿ 0.0.0.0 ▿ 15.1.1.2

home (config) ※ ip ▿ classless

	C	15.1.1.0/30	S_2
	C	192.168.1.0/24	E_0
default route ←	S*	0.0.0.0/0	S_2

to deactivate the command use (config) ※ no ▿ ip ▿ classless

يعني ال entry مكتوب بس مش activated

(1.4) Default Network

طريقه إلى كل الشبكات الغير معروفه هوه نفس طريق شبكة أخرى معروفه مسبقاً في ال RTG Table

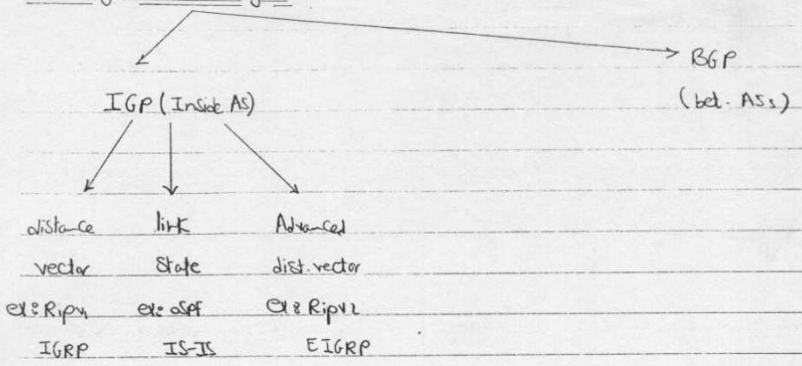
use the following config command

(config) ※ ip ▿ default-network ▿ network

ex : (config) ※ ip ▿ default-network ▿ 15.1.1.0

C	15.1.1.0/30	S_2
S*	0.0.0.0	S_2

(2) Dynamic Routing : used if there are multiple paths bet. Src & dst

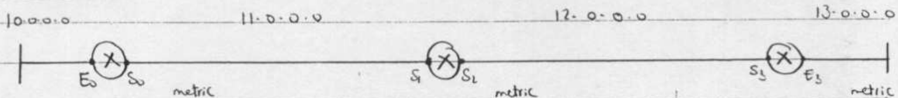


Distance vector

we'll see the operation of the Routers that work with distance vector

at → Startup
→ convergence (Steady State)
→ change (one net. fails, one net. up & so on)

At startup



			metric
C	10	E_0	0
C	11	S_0	0

			metric
C	11	S_1	0
C	12	S_2	0

			metric
C	12	S_3	0
C	13	E_3	0

each Router will Fwd its routing Table on all its interfaces after incrementing the metric by 1 every certain periodic time (Rip = 30sec, IGRP = 90sec) & updates his RTG Table

1st periodic update (After 30sec)

1 = metric بتاعة 10 الشبكة أقدر أوصل لـ
↳ hop (Rip)

↔ 10,1 / 11,1 — ↔ 11,1 / 12,1 — ↔ 12,1 / 13,1

C	10	E_0	0
C	11	S_0	0
~~R~~	~~11~~	~~S_0~~	~~1~~ ✗
R	12	S_0	1

R admin dis. = 120
C admin dis. = 0 → أحسن
R ≡ Rip

C	11	S_1	0
C	12	S_2	0
~~R~~	~~12~~	~~S_2~~	~~1~~ →✗
R	13	S_2	1
R	10	S_1	1
~~R~~	~~11~~	~~S_1~~	~~1~~ →✗

الـ Rip كله كداب
→ وصل خلاص للـ convergence

C	12	S_3	0
C	13	E_3	0
R	11	S_3	1
~~R~~	~~12~~	~~S_3~~	~~1~~ →✗

2nd periodic update (After 30sec)

↔ 10,1 / 11,1 / 12,2 — ↔ 11,1 / 12,1 / 13,2 / 10,2 — ↔ 12,1 / 13,1 / 11,2

				Timer
C	10	E_0	0	
C	11	S_0	0	
R	12	S_0	1	[00:00]
R	13	S_0	2	
~~R~~	~~11~~	~~S_0~~	~~1~~ →✗	
R	12	S_0	1 →✗	
~~R~~	~~10~~	~~S_0~~	~~2~~ →✗	

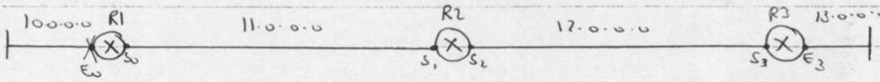
→ يلغي الجديد ويصفر الـ Timer بتاع القديم
أي أن هذه المعلومة وصل لها تحديث

C	11	S_1	0
C	12	S_2	0
R	13	S_2	1
R	10	S_1	1

وصل الـ conv. من المرحلة السابقة وكل update حيستقبله حيلاقي أن اللي عنده في الـ RTG Table أفضل

C	12	S_3	0
C	13	E_3	0
R	11	S_3	1
R	10	S_3	2
~~R~~	~~11~~	~~S_3~~	~~1~~ →✗
~~R~~	~~12~~	~~S_3~~	~~1~~ →✗
~~R~~	~~13~~	~~S_3~~	~~2~~ →✗

At Change One Network is down or a new Network appears



(1) E_0 is down

(2)

~~C~~	~~10~~	~~E_0~~	~~0~~ ✗
C	11	S_0	0
R	12	S_0	1
R	13	S_0	2

(4)

C	11	S_1	0
C	12	S_2	0
~~R~~	~~10~~	~~S_1~~	~~1~~ ✗
R	13	S_2	1

(6)

C	12	S_3	0
C	13	E_3	0
R	11	S_3	1
~~R~~	~~10~~	~~S_3~~	~~0~~ ✗

(3) R1 wait for periodic update & then send its full RTG Table as follow

⟵•⟶

10, 16 ↳ un valid Metric ≡ host unreachable
11, 1
12, 2
13, 3

In Rip : Max. no. of hops = 15 i.e max no. of series routers = 16
وعندما أقول ان metric = 16
هذا يعني أن هذه الشبكة
وتعتبر لا يمكن الوصول لها

(4) R2 will update its Routing Table by omitting the entry of Net. 10 & it will wait another 30 sec to FWD its full RTG Table

(5) After 30 sec. R2 make FWD to its full RTG Table

⟵•⟶

11,1 / 10,16
12,1 / 13,2

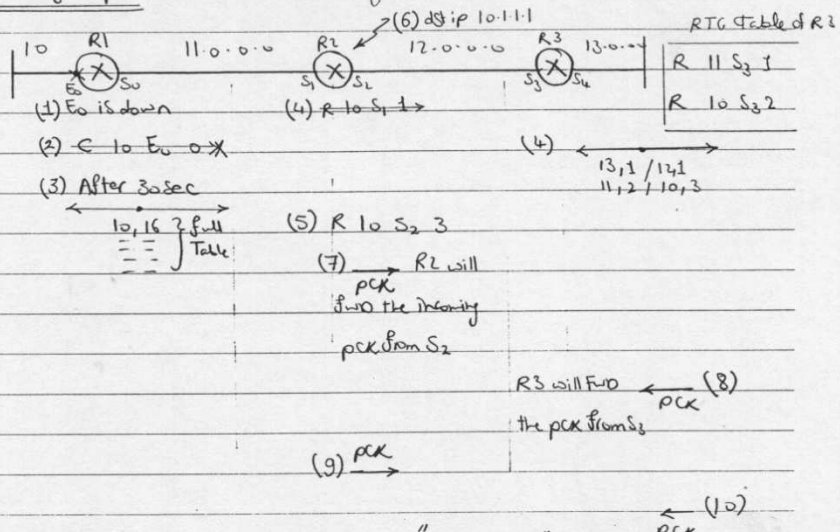
(6) R3 will accept this update & updates its RTG Table

Rip ⟹ very poor Routing protocol, only three Routers & R3 sensed the Network failure after 1 min

Problems :

(1) Slow convergence : R_3 sensed E_0 failure after 60 seconds

(2) Routing loop : Consider the following case



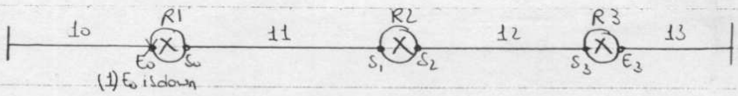
& the pck will loop between R1 & R2 ⇒ "Routing loop"

Solutions

(1) TTL expire : TTL of the pck starts with 255 & when it reaches zero ⇒ the pck will be discarded ⇒ يتم حذفها ولا يتم ارسالها

(2) triggers update + poisoned route + poison reverse

- we don't wait until 30 sec (Rip) but whenever the update occures the Router will fwd its full RTG table
- Any Router receives this update will FWD it & it will reply with An ACK (poison reverse).



(1) E_0 is down

(2) ⟵•⟶

triggered update

10, 16 → poisoned route

11, 0

12, 1

13, 2

⟵

(3) poisoned Reverse (ACK)

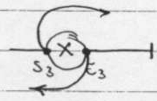
عشان R1 ميفتكرش يبعتها

وبعد كده R1 يبعت ال RTG table

من غير 10 اللي وقعت

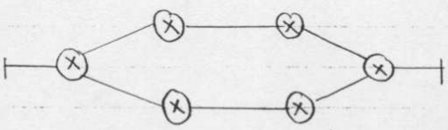
<u>(3) Split Horizon</u> : " Route learned from interface can never be sent back on the same interface"

Concerning R3 ⟹ الحاجة اللي اتعلمتها من interface مبيبعتهاش على نفس ال interface تاني



C	13	E_3	0	→ أذيع عنها من S_3 فقط
C	12	S_3	0	} أذيع عنهم من E_3 فقط
R	11	S_3	1	
R	10	S_3	2	

but split horizon doesn't solve this connection ?!



(4) hold down Timer (Rip = 180 sec , IGRP = 280 sec)

"The Router that learns about a failed route will never try to learn about it unless" : يعني R2 لو عرفت ان E0 وقعت متتعلمش أي حاجه عن E0 إلا إذا

(a) the Router (R2 in our example) is learned from the same source (R1) with the same metric ⇒ يعني E0 قامت تاني

(b) the Router (R2) is learned from another source with better metric
حصل تغيير جذري في الشبكة وبقى هناك سكة ↵
أفضل لـ Net.10 عن طريق سكة غير E0

(C) Hold down time is expired ⇒ خلاص دلوقتي تقدر تعرفه

Session (15)
24/05/06

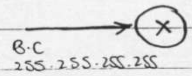
Topics * Routing protocols
- Distance vector
  - . Ripv1 c/c's
  - . IGRP c/c's
  - . D.V Configuration

Ripv1 (Routing Information protocol)

⇒ It is a L7 protocol, i.e the PCs will accept Routing updates every 30 sec but they won't understand these updates ⇒ يعني ال PCs حتشتري وتأز نزحها
والمشكلة إن Ripv1 ← L7

(1) Distance vector Routing protocol

(2) Send periodic updates containing full Routing Table every 30 sec out of all its interfaces on address 255.255.255.255



- the Router will accept the B.C msg & of course it will not pass it as a B.C msg, but it will take an action, like updating his routing Table when he understands that this is a Rip msg.

- Ripv1 deals with UDP (fast & not compact) & most protocols deal with UDP send B.C

(3) At Change (Net. is up or Net. is down) the Router send triggered update containing full Table & the changed entry (ex: 10, 16 → metric)

(4) Symbol in RTG Table is "R"

(5) Admin distance = 120

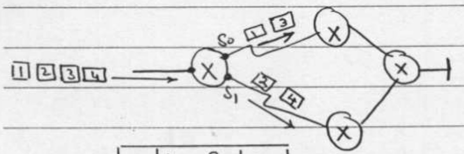
(6) Metric is hop count (max = 15 hop)

⇒ we can put as max. a 16 Router in series

(7) classfull : doesn't send the mask in updates

⇒ The Router that receives the update will estimate the mask

(8) Support equal load-Sharing (Balancing) : 4 paths by default & 6 paths max.



R	10	S0	2
R	10	S1	2

↓ metric

} the two paths are equivalent in everything & i pay for each path a large sum of money so to make use of both of them we send ½ of the data on each path .

← من غير أي config لو عندك لغاية 4path ال Router حيوزع عليهم ال data

ومن طريق ال config ممكن لو عندك 6path زي بعض تخلي ال Router يستخدمهم كلهم .

(9) use BellmanFord Algorithm to calculate RTG Table

← يعني التطبيق اللي بيحصل في ال RTG Table وشوية بعض ال paths لأن هناك

paths أفضل يكون عن طريق هذا ال Algorithm

(10) support solutions :

- triggered update + poisoned route + poison reverse (ACK)
- split Horizon
- Hold down timer = 180 sec.

IGRP (Interior Gate Way protocol)

(1) Distance vector (D.V) Routing protocol (Cisco proprietary)
Cisco router) فقط

(2) like RipV1, but periodic updates every 90 sec.

(3) like RipV1

(4) Symbol in RTG Table "I"

(5) Admin distance = 100
⇒ IGRP is more trustfullness than RipV1

(6) Metric is composite one ($= \frac{K_1}{BW} + K_2 * load + K_3 * delay + K_4 / reliability + K_5 / MTU$)

by default ⇒ $K_1 = K_3 = 1$ ⇒ the most import. factors are BW & delay
& $K_2 = K_4 = K_5 = 0$

composite means a combination of : B.W, load, delay, reliability, MTU)

N.B : the small metric is better & so as :

B.W ↑ ∴ metric ↓ (from eq^n) ⇒ better

load ↓ or delay ↓ ∴ metric ↓ ⇒ better

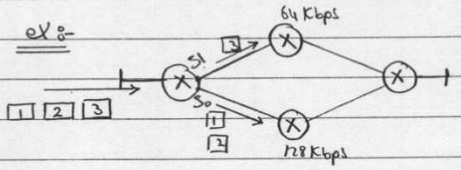
reliability ↑ or MTU ↑ ∴ metric ↓ ⇒ better

According to this composite metric we can use as max 100 routers in series (default) & by config. we can use as max 255 routers in series (according to TTL = 255)

(7) IGRP is a classfull protocol

(8) Support equal & non-equal load sharing
(4 paths default & 6 paths max. ⇒ by config.)

ex :-



*N.B : by default all pcks will go out through S0 as it is the best path, but by config. we can make non-equal load sharing

(9) Use Bellman Ford Algorithm to calculate the RTG Table ⇒ like RipV1

(10) Support Solutions : . triggered update + poisoned route + poison reverse
. split horizon
. Hold down timer = 280 sec
(cz the periodic update is every 90 sec)

Configuration

Config of RipV1

(Config)# Router Rip

(Config-Router)# Network IP of direct connected networks

← يا Router أنا عايز أحكي لل Rip وأقوله على ال Interfaces اللي حتشتغل Rip

N.B: updates ≡ RTG information
data ≡ user information

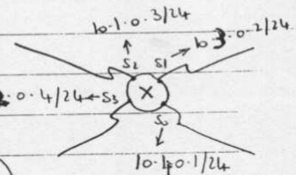
***
This command will:

(1) Activate interface to T^x updates
(2) Activate interface to R^x updates
(3) Routes learned from that interface can be advertised to other routers.

ex:

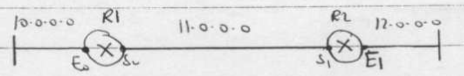
(Config)# Router Rip

(Config-Router)# Network 10.0.0.0



All interfaces that're connected to subnetworks of the main Net. 10.0.0.0 will be activated by Rip

ex :



C	10/—	E0
C	11/—	S0

C	11/—	S1
C	12/—	E1

} with no config.

عشان R2 يعرف الشبكة دي لازم ← (1) E0 تبقى available انه حر يبيع منها

(2) S0 تبقى = عشان تبيع منه E0 لـ S1

(config) # Router ▿ Rip
(config-router) # Network ▿ 10.0.0.0
(config-router) # Network ▿ 11.0.0.0
} R1

(config) # Router ▿ Rip
(config-router) # Network ▿ 11.0.0.0
(config-router) # Network ▿ 12.0.0.0
} R2

⇒ to make a certain interface passive use the following

(config) # Router ▿ Rip
(config-Router) # passive-interface ▿ name of interface

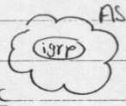
passive interface : (1) doesn't T^x updates
(2) R^x updates
(3) Routes learned from that interface can be advertised to other routers

To make E0 passive use : عشان E0 متبعتلش تبقى updates لل PCs ← حرام

(config) # Router ▿ Rip
(config-Router) # Network ▿ 10.0.0.0
(config-Router) # passive-interface ▿ E0
} R1

Configuration of IGRP

(config) # Router ▽ igrp ▽ AS # → no. of AS

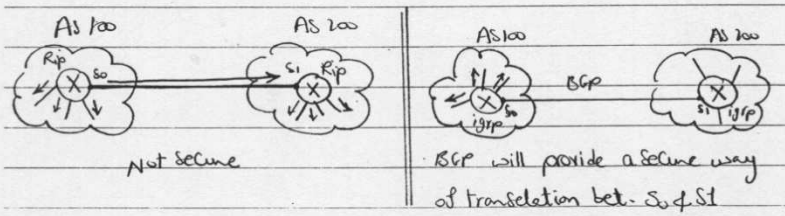


(config-router) # Network ▽ ip of direct connected Network

⇒ passive interface use :

(config-router) # passive-interface ▽ interface name

⇒ In IGRP we use the Autonomous System (AS) no. in order to make the updates only shared within the AS



Trouble Shooting :

Sh ▽ ip ▽ route
Sh ▽ ip ▽ protocols
} L3 trouble Shooting

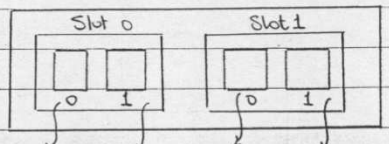
debug ▽ ip ▽ rip (monitoring) ⇒ for rip

debug ▽ ip ▽ igrp ▽ transactions ⇒ for igrp

Session (16)
27/5/06

Simulation (lab 2)

- Slots & interfaces for routers



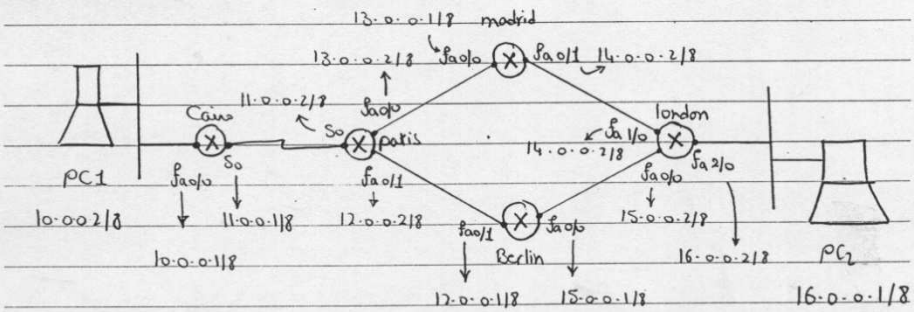
fa 0/0 — fast ethernet interface 0 on Slot 0

fa 0/1 — slot interface

fa 1/0

fa 1/1 — interface 1 on Slot 1

Our example :



- To give the PC an ip / G.w & mask use

C:> winipcfg ↵

ip : 10.0.0.2	← this window will open & you'll fill it
mask : 255.0.0.0	
G.w : 10.0.0.1	

to check the ip use

C:> ipconfig ↵

Trouble Shooting :

L1 & L2 : use # Sh ▽ ip ▽ interface ▽ brief

or

Sh ▽ interface ▽ So ⇒ Cairo

	L1 Status	L2 protocol
appears if the interface is Shutted down	← admin down	down
if there is physical failure	← down	down
	up	down ← Encapsulation mismatch (ex: FR with Ethernet) / missing Clk
	up	up

N.B : Between Cairo & paris we've serial connection & so we should Adjust the clking between them .

- first to know who is DTE & who is DCE use :

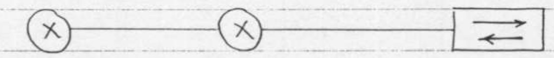
Cairo # Sh ▽ Controller ▽ So ↵

- Assume Cairo is DCE ∴ to adjust the Clk on So of Cairo use :

Cairo (config-if) # clock ▽ rate ▽ 2000000 ↵

Trouble Shooting on L2 using a Cisco protocol

CDP (Cisco Discovery Protocol) : Cisco proprietary & enabled by default



Every 60 sec each device send a CDP msg

It contains : (1) Device ID (Host name)
(2) Capability (Router, Switch, --)
(3) platform (Model)
(4) Local & remote interfaces (my interfaces & next hop interfaces)
(5) IP Address
(6) IOS version

use : # Sh ▿ cdp ▿ neighbors ⇒ to see from pt(1) → pt(4)

hold time ⇒ لو مستقبلتش من جاري لمدة معينة حاعتبره وقع

capability ⇒ R ≡ Router , TS ≡ Transparent Switch

port ID ⇒ ال Interface بتاعة جاري اللي واصل بيها عليّ

to show all points from pt(1) → pt(6) use :
Sh ▿ cdp ▿ neighbors ▿ detail

To Show IOS version use : # Sh ▿ flash or # Sh ▿ version

To Show Config. register use : # Sh ▿ version
0 X 2102 → default
or 0 X 2142 ⇒ passing NVRAM & enters the setup mode

L3 Trouble Shooting

- Cairo # Sh ip route ↵
  - we get only the direct connected Network As we up's now we don't define any protocol.

C 10.0.0.0/8	fa0/0
C 11.0.0.0/8	S0

  - let's configure the rip protocol
    - Cairo (config) # Router ip
    - Cairo (config-router) # Network 10.0.0.0
    - Cairo (config-router) # Network 11.0.0.0

- Cairo # Sh ip route ↵
  - C 10.0.0.0/8 [0/0]
  - C 11.0.0.0/8 [0/0]
  - R

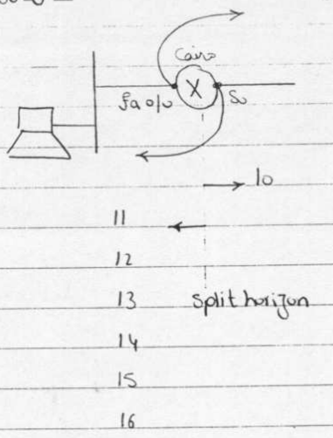
R 16.0.0.0/8 [120/3] via 11.0.0.2, — , — , — , S0

- R ← Rip
- 16.0.0.0 ← ip of Network
- /8 ← estimated mask
- [120/3] ← admin dist. / no. of hops
- via 11.0.0.2 ← through
- next hop
- S0 ← Cairo serial

In static configure may use only 1 them

- # Sh ip protocols ⇒ gives
  - (1) Active protocols
  - (2) Timer about protocols ⇒ if next due = 10sec ∴ the last update was sent from 20 sec
  - (3) Hold time = 180 sec
  - (4) Active interfaces ⇒ Send 1 ≡ Send version 1 updates
  - (5) Routing for Networks → Networks I!
  - (6) Routing information source → updates
  - (7) Admin distance

Debugging : Cairo # debug ip rip ⇒ debug from Router



– يعني مش يذيع من Net 10 بس لأن
ال Router عرف عنها من fa 0/0
وأيضاً fa0/0 يذيع من كل الشبكات اللي
اتعلمها من S0 زي 11, 12, 13, 14, 15, 16

Debug from PC use : # debug ip rip
terminal monitor

to terminate the debugging use : # no debug all
or
no debug ip rip

Static Routing (ISP)

Cairo (config) # ip route 16.0.0.0 255.0.0.0 11.0.0.2
if we see the RTG Table in past R 16/8 [120/3]
now S 16/8 [1/0]
(Admin, metric)

⇒ Gateway of last resort in not set

Default route (config) # ip route 0.0.0.0 0.0.0.0 { S0 / 11.0.0.2 }
⇒ Gateway of last resort is set

N.B: with the default route we may use

Cairo(config)# ip route 0.0.0.0 0.0.0.0 11.0.0.2 ← (11.0.0.2 ← ip of next hop)

Cairo(config)# ip classless ←

↳ to activate the up command but it is enabled by default.

or we may use Default Network

Cairo(config)# ip default-network 11.0.0.0 ←

11 ← الطريق الى كل الشبكات في هذه الشبكة

ARP Table : It is a relation between ip & MAC

↳ ARP protocol used to obtain unKnown dst MAC

ARPA = Ethernet (Mac)

IP	MAC (Hw Address)

DNS (Domain Name Service) Server

- When the Router is configured as a DNS Server then it will supply other devices with dst. ips.
- when you write www.yahoo.com :- the DNS Server will understand it & send to you the ip of yahoo to use it.
- to configure a Router as a DNS server we may use

Cairo(config)# ip host paris 11.0.0.2

Cairo(config)# ip host london 16.0.0.2

⇒ to show hosts use

Cairo # show hosts

⇒ If we type Cairo # Ping London ⇒ Success

Cairo # ping paris ⇒ un recognized name

Telnet on london

Cairo # Telnet london ↵

⇒ Telnet is not available ??!

عشان لازم london نعمل activate لل vTy lines ⟵

london(config) # line VTy 0 4 ↵

london(config-line) # password CiSCo

london(config-line) # login

now on Cairo

Cairo # Telnet london

password: CiSCo

london # ⇝ دلوقتي إحنا على london وممكن نعمل أي config. عليه

⇒ to terminate Session use

london # exit

⇒ to Suspend Session use

london # < Cltr + Shift + 6 >

then ← شيل إيدك واضغط على

< X >

⇒ to Show Sessions use ⇒ Cairo # Sh session

29/05/06
Session (17)

Advanced D.V

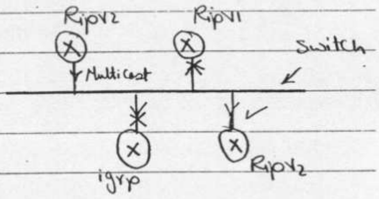
Rip v2

It is a layer 7 protocol

(1) It is advanced protocol

(2) It sends updates on multicast address 224.0.0.9

⇒ Rip v2 sends only multicast msg & those who're learned this multicast address will accept the msg

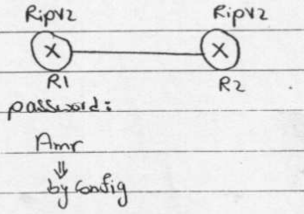


⇐ يعني من الأول أي حد يلاقي ان dst add. مش بتاعه ميستقبلش الرسالة ك مش زي ال Ripv1 اللي كان بيبعت B.C وبالتالي كل Router أو PC يستقبلها وبعد كده يفكها يلاقي انها مش بتاعته.

(3) It supports authentication using password

⇒ It is used for security, before sending updates R₂ should enter a password.

⇒ for wrong password ∴ R1 will discard the request & shut down the interface.



(4) classless : It sends mask with updates

⇒ classless ≠ classfull (to save B.W the Transmitting Router doesn't send the mask & the Receiving Router will have to estimate the mask & the estimation may be wrong)

(5) Send periodic updates every 30 sec out of all its interfaces.

6 _ Symbol in RTG Table "R"

⇒ how to know wheather our Router works RipV1 or RipV2 & both have symbol "R"

Sh ip protocols

	on Cairo	send	Rec
f ⇒	S0	1	1/2
f ⇒	S0	2	1/2

(f ⇒ S0 1 1/2): 1 → this interface sends updates of RipV1

(f ⇒ S0 2 1/2) → this interface sends RipV2 updates & can receive RipV1 or RipV2 " .

7 _ use triggered update, split horizon & Holddown timer

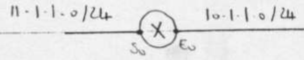
8 _ Support equal load sharing (4 default & 6 max)

9 _ Admin distance = 120

10 _ metric = hop count (max = 15)

Configuration
(Config) # router rip
(Config-router) # version 2
(Config-router) # Network direct connected Networks

ex :



C	10.1.1.0/24	E0
C	11.1.1.0/24	S0

(Config-router) # network 10.0.0.0
↳ يعنى شغّل كل ال ints اللى على السبكات اللى subnets من الشبكة 10.0.0.0

OR

(Config-router) # network 10.1.1.0

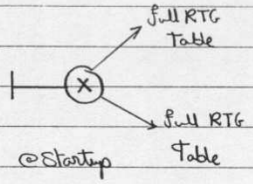
here we T^x the mask → 10.1.1.0/24, metric = 1 ; 11.1.1.0/24, metric = 1

EIGRP (Enhanced IGRP) ⇒ It is the best protocol → Routing ال فيه أحسن

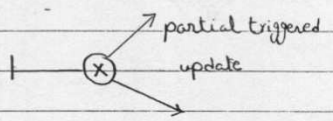
-1- Advanced D.V Cisco proprietary.

-2- Sends full RTG Table at startup to its neighbors.

-3- At Change only partial triggered updates are transmitted.



@Startup



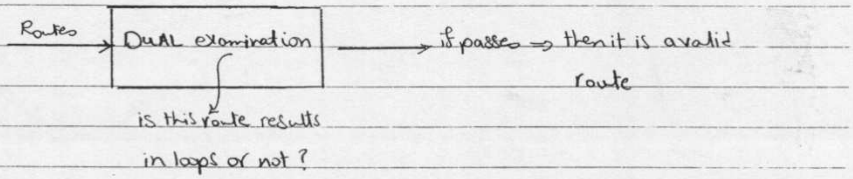
@Change

← يعني الحاجة اللي تغيرت (شبكة وبعت تحديث)

-4- no periodic updates (no B.w waste) ∴ AS no updates (overhead) are T^d

-5- no Routing loops → use DUAL

⇒ DUAL (Diffusion update Algorithm) : this Algorithm put some conditions for the selected route & never results in loops

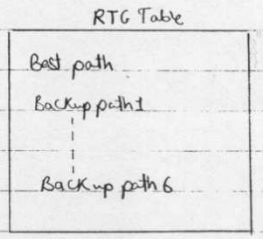


-6- Fast convergence → use DUAL

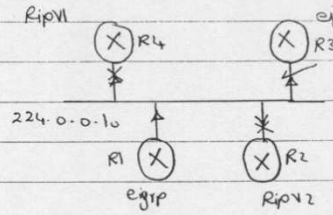
(Backup path for every best path)

⇒ we save the Best path & up to 6 Backup paths so if 1 path is down we use the following one.

→ All the backup paths don't result in loops (i.e they should also pass the DUAL exam) but they're of higher metric (As metric ↓ it is better)



-7- Send updates on multicast address 224.0.0.10



. only R3 will accept that msg

← switch & receive these updates

(8) classless : sends the mask with the updates

(9) Symbol in RTG Table is "D" ⇒ refered to DUAL

⇒ N.B : Most of the letters in EIGRP where reserved & so we can't use them (EGP, IGRP, Ripv1/RipV2)

(10) Admin distance = 90 (the best)

(11) Metric of EIGRP = 256 * metric of IGRP (24 bits)

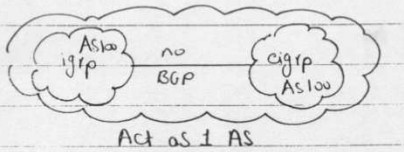
↳ $(K_1/B.w + K_3 * delay)$ by default

(32 bit)

↙ metric of EIGRP is presented in 32 bits

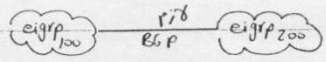
(12) Compatible with igrp (same AS)

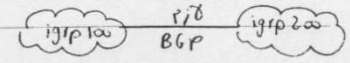
⇒ In the same AS (same AS no.) : igrp & eigrp act as 1 AS & no need for BGP bet. them

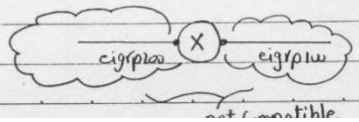


Act as 1 AS

N.B :







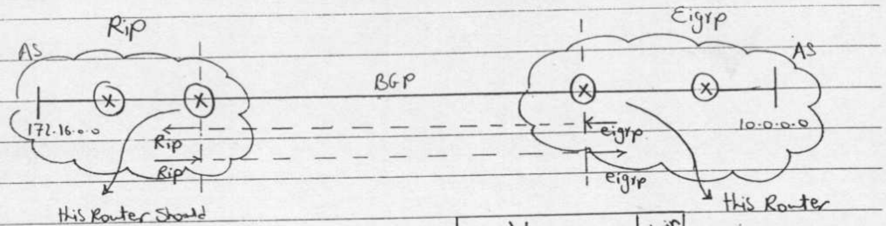
not compatible

(13) Maximum hop count = 224 hop

⇒ i.e we may use 225 Routers in Series

(14) Differentiate bet. internal & external routes

↳ (DEX, Admin dist = 170)



R	172.16.0.0
R	10.0.0.0

protocol	Network	admin
D	10.0.0.0	90
DEx	172.16.0.0	170

. ال Rip معرفش يفرق بين مين جوه ذ ال AS ومين من بره

. الرسالة كان أصلها BGP
يعني مش معايا ذ نفس ال AS
يعني eigrp(D) external ولها
admin = 170

(15) Support equal & non-equal load Sharing

⇓

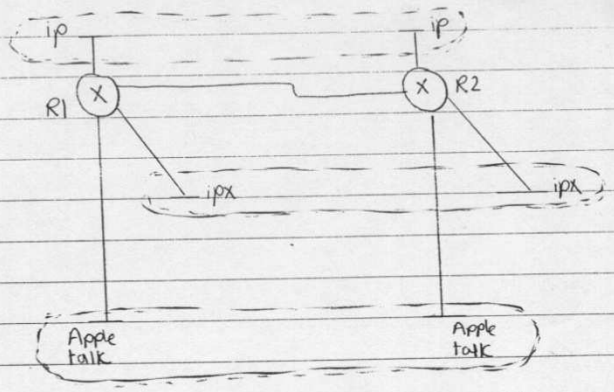
(non-equal load balancing)

(16)* Support Routing for multiple Network layered routed protocols (IP, IPX, Apple Talk)

. IP pck, IPX pck & Apple talk pck are different & so IP, IPX & Apple talk can't understand each others

Consider the following case : we're 3 departments

IP IPX Apple talk



→ for R1 & R2 to support 3 Routed protocols they need to define :

ip Rip	IPX Rip	Appletalk Rip
RTG protocol	RTG protocol	RTG protocol

→ OR Simple to define Eigrp RTG protocol which can support multiple layer Routed protocol & do :

- the 2 ip routed protocols on R1 & R2 can talk to each other
- " " ipx " " " " " " " " " " " "
- " " Appletalk " " " " " " " " " " " "

Configuration : (config) # router eigrp AS #
(config-router) # Network direct connected Networks

→ to eliminate certain protocol use

(config) # no router rip

(config) # no router igrp AS #

(config) # no router eigrp AS #

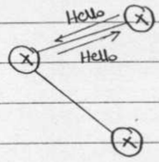
Eigrp Terminology

(1) Neighbor Table : "List of all neighbors"

. جدول الجيران : يتم تسجيل فيه الجيران اللي تم التعرف عليهم ← only in eigrp
عن طريق Hello msg وذلك قبل إرسال ال updates

. ماهو الجار؟ ← (1) direct connected to me + (2) understand eigrp
له Router لازم فرق ومتكلم eigrp مثلي

Sh ▿ ip ▿ eigrp ▿ neighbors
↓
may be ipx or Apple talk



(2) Routing Table : "List of best routes to dst"

Sh ▿ ip ▿ route ▿ [eigrp]
→ optional

(3) Topology Table : "List of All Routers to All destinations"
(your neighbor's RTG Tables)

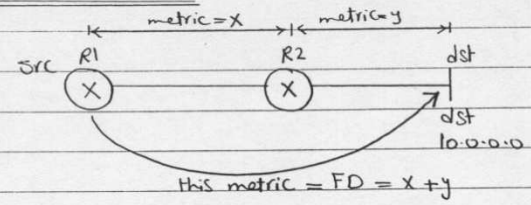
≪ جدول مكتوب فيه إزاى كل Router فى ال AS يقدر يوصل لكل الشبكات فى ال AS
≪ عن طريق هذا الجدول عكيه نستنتج ال RTG Table
≪ هذا الجدول مكتوب فيه ال RTG Table + backup paths

Sh ▿ ip ▿ eigrp ▿ topology

(4) Successor (S) : "Best path" ⇒ مصطلح فى ال Topology Table

(5) Feasible Successor (FS) "Backup path"
↳ Topology Table الـ is كلمة

(6) Feasible Distance (FD) "Metric bet. src router & dst router"

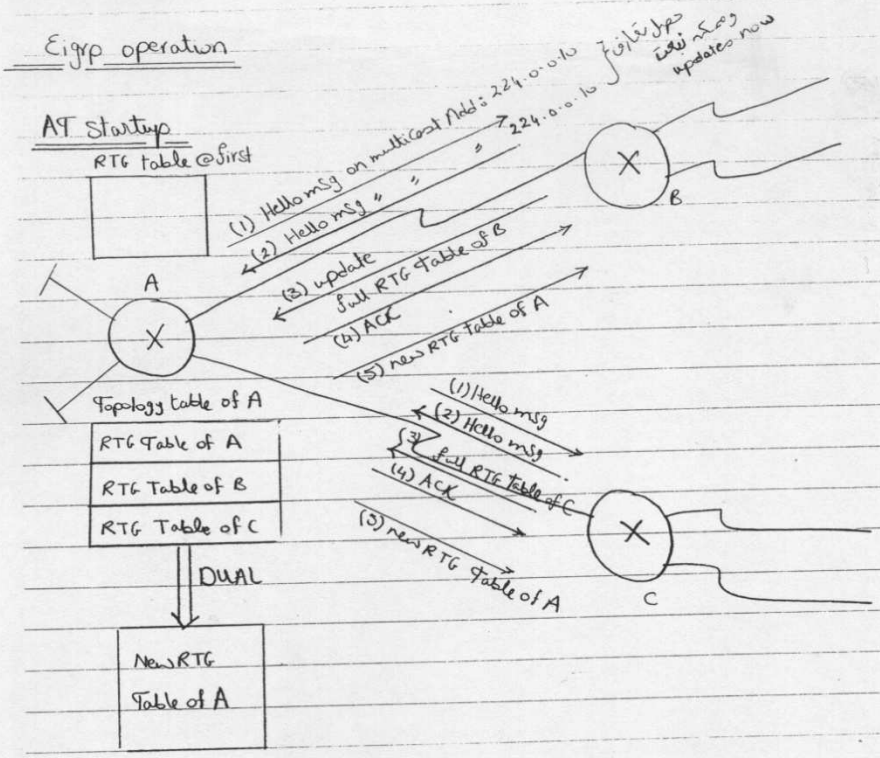


(7) Advertised Distance (AD) "Metric bet. my neighbor & dst"
⇐ يعني جارك يبيع لك الـ metric اللي بينه وبين الـ dst وتجمع أنت عنده العلوية مع الـ metric اللي أنت واصل بيها على جارك فتحصل على FD
AD = y metric is f^{n} (delay, B.w, ---)

N.B : RTG Table Shows Successor by certain AD
↓
best path

Topology Table Shows Successor by certain AD &
Shows the feasible Successor by certain AD

Eigrp operation



Notes :-

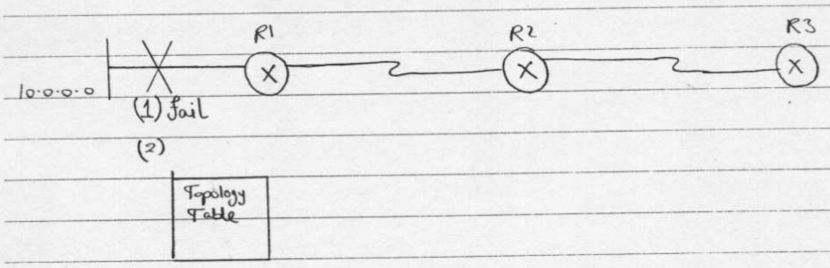
- Cisco invented certain protocol like TCP to deal with the hello msg.
- if B & C reply with a hello msg on amulticast add. 224.0.0.10 then they both operate with eigrp
- A Should Send An ACK to make B & C know that thier full RTG Table was sent successfully
- What we draw above occur with B & C also & at the end of this operation B & C will form a topology table like A & each of them will form its new RTG table & now All hosts connected to A, B & C can communicate with each other.

At Convergence : Since each Router doesn't send his full RTG Table except @ startup & we've no periodic updates, then we reach stability condition (convergence)

- But during convergence periodic Hellos 're sent as keepalives
  - fast link (>1.5Mbps) → Hello 5 Sec, dead 15Sec
  - slow link (<1.5Mbps) → Hello 60Sec, dead interval 180Sec

At Change

- If there is no FS (مفيش Backup route في متخزنه)



R1 didn't find FS in Topology Table

(3) query msg on 224.0.0.10 (plst)

I've no route for 10.0.0.0 do anyone have another path ?

R1 will enter active state

active ≡ trying to search for Network

← ACK

(4) R2 will check his Topology Table & if he didn't find FS he will send a query msg to the following Router

→ query msg

← ACK

(5) ← reply

ok there is route / No there is no route

→ ACK

(6) ← reply

ok or No

→ ACK

R1 will enter passive state

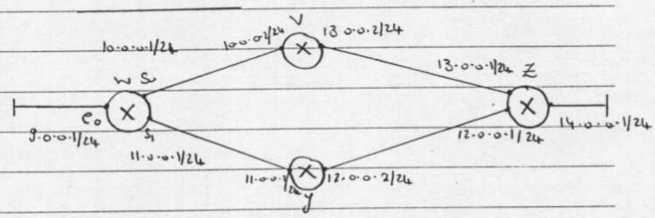
- **If there is FS** : the FS in the topology table is changed to S & is transformed to RTG table

DUAL (Diffusion update Algorithm) :- ال updates بيعملها diffusion ف الشبكة من ال Router للي وراه بحثاً عن FS عند اى Router

Session (18)
31/05/06

Topics * Routing protocols
- link State Routing
  - @ Startup
  - @ Convergence
  - @ Change
- OSPF C/C'S
- OSPF Configuration

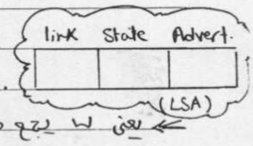
link State Routing



AT Startup

(1) Each Router will try to discover the link state neighbor (i.e direct connected + operate with link state protocols)
↳ using a hello msg

(2) Each Router will form a packet describing itself called LSA (Link State Advertisment) & sends it to all its neighbors.



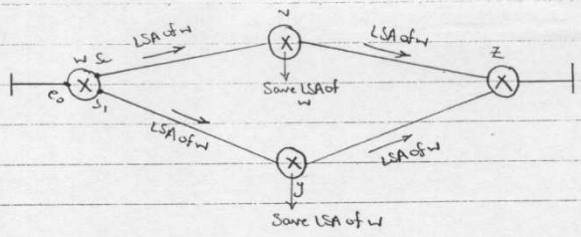
⇐ يعنى W يجمع معلومات عن نفسه (عنده interfaces كذا وعليها كذا ووصل على networks كذا ولها mask كذا) ويبعتها لجيرانه V & y ونفس الكلام بيعمله كل router

LSA for W

link	State		Advertisment
9.0.0.1/24	up	metric 10	Router ID
10.0.0.1/24	up	metric 10	W
11.0.0.1/24	up	metric 10	

Advertisment → مين الذى أعلم عن هذا الكلام أو ال LSA دى بتاعت مين.

↳ will be stored in memory



(3) Each neighbor that receives a LSA will take a copy of it in its LSDB (Link State Data Base) & then sends it as it is to all its other neighbors, so LSA of each Router will be flooded in the AS.

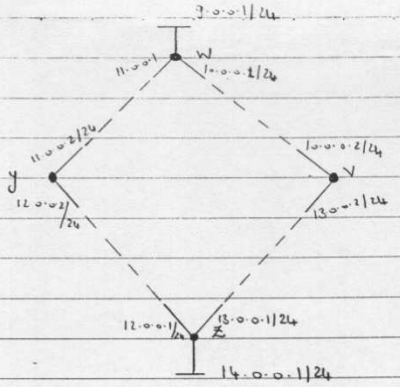
LSDB of W

W	9.0.0.1/24	C_0	metric 1	up
	10.0.0.1/24	S_0	metric 1	up
	11.0.0.1/24	S_1	metric 1	up
V	10.0.0.2/24		metric 1	up
	13.0.0.2/24		metric 1	up
J	11.0.0.2/24		metric 1	up
	12.0.0.2/24		metric 1	up
Z	12.0.0.1/24		metric 1	up
	13.0.0.1/24		metric 1	up
	14.0.0.1/24		metric 1	up

N.B:
- 1- V, y & Z will receive 2 copies from LSA of W 1 copy from each interface
- 2- When LSA of W returns back to Router W he will discard it
- 3- Also V, y & Z will form a LSDB like W

(4) Each Router will then draw a tree from its LSDB called LSDB Tree

← شجرة تحتوي على كل الناس اللي عرفتهم بكل الطرق الممكنة

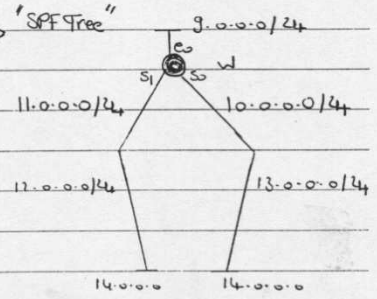


LSDB Tree of W
الشجرة من وجهة نظر "W"

* link state is very smart & it succeeded to draw the whole Network

(5) Each device will apply Dijkstra Algorithm (SPF Algorithm) on the LSDB tree to get "SPF Tree"
SPF ≡ Shortest path first

"LSDB Tree" → Dijkstra Algorithm "SPF Algorithm" → "SPF Tree"



بالنسبة لـ W احسب طريق كل شبكة من وجهة نظره مع اقل تأخير (delay)

(6) The SPF Tree will be then translated to a RTG Table

RTG Table

g.0.0.0	e0
10.0.0.0	S0
11.0.0.0	S1
12.0.0.0	S1
13.0.0.0	S0
14.0.0.0	S0
14.0.0.0	S1

} Load Sharing bec. both paths are identical in metric (ex: delay)

At Convergence : Each Router will only send periodic LSA every 30 min (↑↑) to make LSDB refreshment

→ **N.B :-** ال Rip ميستنش وبيبعت علطول updates كل 30 sec

At Change

- Router that feels change will send triggered partial update Assume Net. on e_0 is down ∴ "w" will send the following

link	State	Advertisment
9.0.0.1	down	w

→ LSA

- each neighbor will take a copy of this LSA & updates its LSDB & redraw the LSDB tree & then redraw the SPF tree & reform his RTG Table & in the same time FWD the LSA of w as it is to the following neighbors.

Linkstate disadvantages

(1) Very complex implementation
(2) Network instability will affect the entire AS.
(3) High CPU usage "Dijkstra is a very CPU intensive Algorithm"
(4) High memory utility.

Advantages
(1) No Routing loops
(2) No BW waste
(3) reliable
(4) Classless
(5) use multicast

link state protocols

OSPF (open Shortest Path First)

(1) open standard link state Routing protocol
"open" ← Router ... ليس حكراً على شركة معينة

(2) sends triggered update called LSA @ startup
& @ change on multicast address 224.0.0.5 & 224.0.0.6
to its neighbors
↓
each has diff. use

(3) Symbol in RTG Table "O"

(4) Admin distance = 110 (R = 120, O = 110, I = 100)
⇒ on non-Cisco Routers we can only use Rip or OSPF (OSPF is better)
⇒ on Cisco Routers we may use Rip, OSPF, igrp or eigrp (eigrp is the best)

(5) metric = cost (أولوية) = $\frac{10^8}{BW_i}$ if B.w is 100 Mbps ∴ cost = 1

- BW_i is the Bw of the interface = by default 1.54 Mbps
  = T1 Speed (for serial interfaces)
- e_0 → 10 Mbps, f_a → 100 Mbps
  S_0 → 1.54 Mbps, to change B.w of int use
  (config) # int S_0
  (config-if) # Bandwidth ? in Kbps

- no. of hops is unlimited

Clk rate <u>VS</u> B.W;

Service ↙   ↳ only needed to calculate the Metric (in our course)

القيمة تبع ال data

(config-if) # clock rate 64000

(6) use Dijkstra algorithm to calculate the RTG Table

"LSDB Tree" ⟹ [Dijkstra Algorithm] ⟹ "SPF Tree" → RTG Table

(7) classless & reliable

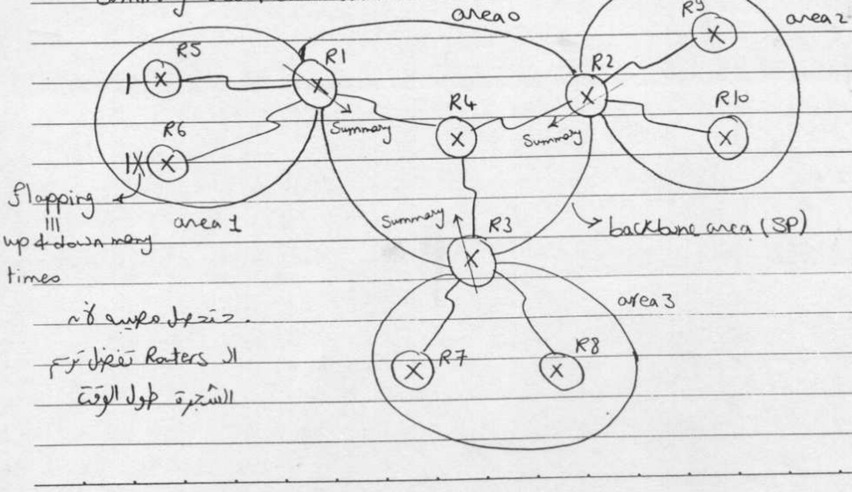
classless : transmitt the mask

reliable : transmitt ACK

(8) Sends periodic update every 30min (LSDB refreshment)

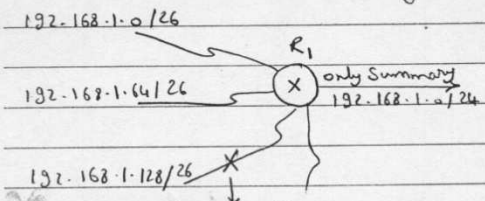
(9) Supports hierarchial design

⇒ Each Router can know full details about its area & know only summary about other areas.



ال Routers تفضل ترسم
الشجرة طول الوقت

- area 0 ⇒ backbone area (0 → 4 billions ≈ 2^{32})
  ↳ areas ال كل لازم تتصل area 0
  i.e: All areas should be connected to area 0.
⇒ All areas are divided by configuration.
- All these areas lie in 1 AS.
- R1, R2, R3 & R4 lie in the core Network / backbone area.
- R1, R2, R3 will send only Summary about there areas ??



- if this link flapped
  ∴ the Summary won't flapped & no other routers won't update there LSDB
- only if the 4 links flapped ∴ the Summary will flapp

← دلوقتي لو الشبكة الي وراها على R5 وقعت ال Summary من R1 متش حتتغير ؟ طب دلوقتي لو R8 عايز يبعت حاجة للشبكة الي وقعت هل R8 حيفضل يبعت لشبكة واقعة وبيملأ ال B.W على الفاضي ؟؟
← لأ طبعاً لأنه في اثناء ال 3 way handshake بين R8 و R1 حيبعت ل R8 انه الشبكة وقعت ل "host unreachable msg"

Hierarchical design

(1) More very complex design ⇒ disadvantage
(2) Network instability will affect only the area & not the entire network
(3) less CPU usage
(4) less memory utility

} Adv.

* In our course (CCNA) we only deal with 1 area (area 0) & no multiple areas.

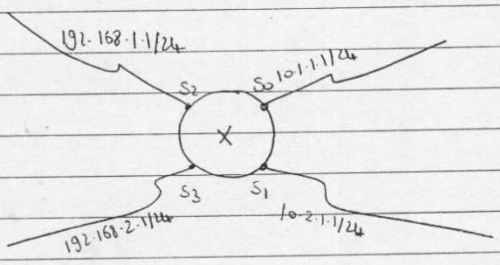
OSPF Configuration

(config)# router ▽ OSPF ▽ Process ID (1 → 65535) → can never be zero (Exam)

(config-router)# Network ▽ direct connected Net. ▽ wild card mask ▽ area ▽ area ID

wild card mask ← only in OSPF

area ID → 0 → 4 millions



wild card Mask (WCM): 32 bit mask (inverted subnet mask)

(000 ... 111) 0 ≡ exact

1 ≡ don't mask

ex: Activate S_0 only

(config)# router ▽ OSPF ▽ 1

(config-router)# Network ▽ 10.1.1.0 ▽ 0.0.0.255 ▽ area 0

شوف كل ال int. اللي تبدأ 10.1.1.x

ex: Activate S_0 & S1

(config)# router ▽ OSPF ▽ 1

(config-router)# Network ▽ 10.x.x.x ▽ 0.255.255.255 ▽ area 0

N.B.e In Rip we activate All interfaces connected to Subnetworks belong to Net. 10 (classA)

to activate all interfaces use :

(config) # router ↓ ospf ↓ 1

(config-router) # Network ↓ 10.1.1.1 ↓ 255.255.255.255 ↓ area 0

Net. add. يعني مش حيعرف على أي حاجة من الـ

OR

(config-router) # Network ↓ x.x.x.x ↓ 255.255.255.255 ↓ area 0

N.B.e- In Exam the best W.C.M ≡ inverted Subnet mask

to activate So we may use

(1) 10.1.x.x ↓ 0.0.255.255
(2) 10.1.1.1 ↓ 0.0.0.0
(3) 10.1.1.x ↓ 0.0.0.255

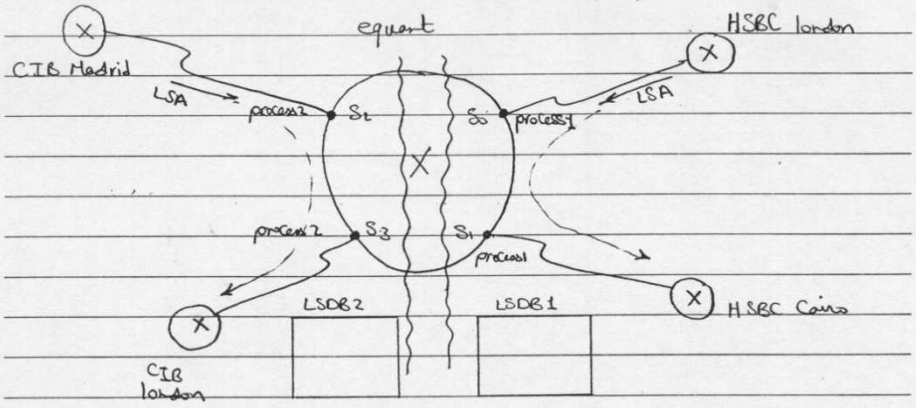
All these 're of the same meaning & will activate So but the third one is the best

↳ this is the best bec. W.C.M ≡ inverted Subnet mask

process ID ⇒ As if we divide our router into no. of Routers

(1) No. that identify a unique LSDB on the local Router

(2) locally significant (affect the local router only & not advertised to other routers)



- Is equant is going to assign a diff. router for each bank ?

⇒ ofcourse no, but equant will divide its Router between the 2 banks such that each one will have a different process ID & will have a different LSDB.

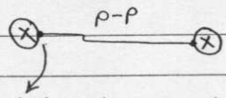
⇒ LSAs will be sent to those who share the same process

ميبعتش بنك يعرف المعلومات بتاعت البنك التاني

* Topics
- OSPF Network types
- OSPF operation for : BMA & NBMA
  Pt - to - Pt
- VLSM
- Classless vs Classfull

- OSPF Network types :

(1) Point - to - point :



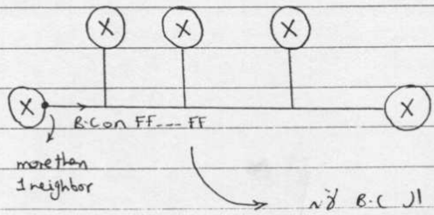
only 1 neighbor on the segment → As the previous session discussion

(2) BMA (Broadcast Multiple Access)

- Broadcast ≡ Routers lie in the same local area & Affected by thier broadcasts (Ethernet OR Token Ring)

⇐ ممكن يكون ال Service provider بتاعي عنده موجود ال Routers جنب بعض ومربوطة Ethernet
تـ ـاعه لـ Support ـ سرعة عالية = 10 Mbps ⇐ Ethernet

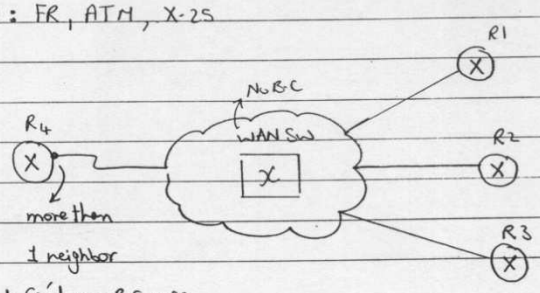
- Multiple Access ≡ more than 1 neighbor on 1 interface



- هنا ال Routers حتستقبل ال B.C لأن
إحنا شغالين Ethernet لأننا داخل LAN

(3) NBMA (Non Broadcast with Multiple Access)

ex : FR, ATM, X.25



- The WAN Switch(ex: FR Switch) discards any B.C msg , So if R_4 needs to send a B.C to R_1, R_2 & R_3 then he will use "Simulate B.C"
- Simulate B.C ≡ replicate unicast msg

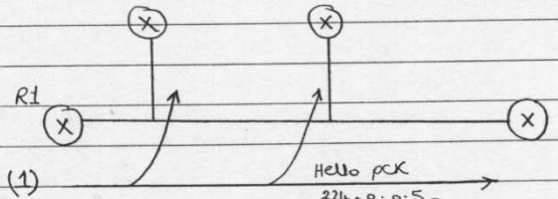
R1 بتاع unicast add. بال R1 لـ B.C msg يعني R4 بيعت الـ
R2 بتاع unicast add. بال R2 لـ وبيعتلها تاني
R3 = = = بال R3 لـ تالت = = و

OSPF operation for BMA & NBMA Network Typologies

(1) Neighbor discovery "Hello protocol"

→ Hello msg is keep alive msg sent periodically every 10 seconds to refresh with neighbors

→ Dead interval (Hold down time) ≡ Time After which i consider my neighbor dead (40 sec)



(2) Hello pck 224.0.0.5 → each Router will reply with a Hello msg if the neighbor ship is accepted

← only if neighborship is accepted

Neighborship is accepted if 4 conditions are verified

(1) The Router lie in the same area
(2) The Router has the same Hello interval
(3) The Router has the same dead interval
(4) The Router has the same OSPF **password**
password defined by configuration on all OSPF Routers & should be the same

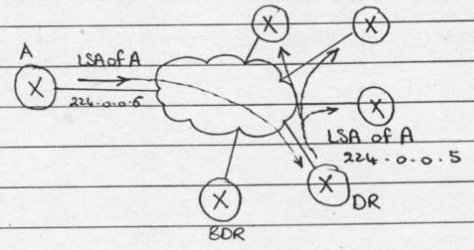
Hello msg
Area ID
Hello interval
Dead interval
OSPF password
Who is DR
Who is BDR

N.B : for eigrp
- → high speed > T1 (1.54Mbps) : Hello every 5sec & dead every 15sec
- → low speed < T1 (1.54Mbps) : Hello every 60sec & dead every 180 sec

---

(2)' Election for designated Router (DR) & Backup designated Router (BDR)

← يتم انتخاب رئيس ونائب رئيس وأى LSA يتم ارسالها للرئيس على multicast add. 224.0.0.6 وعلى الرئيس مسئولية توزيعها على بقية ال Routers (DRothers) على multicast add. 224.0.0.5



← ال Router اللى حيسمع حاجة من الرئيس ميبعتهاش لحد تانى لأنه أكيد أن رئيس بعتها للناس كلها

How to Elect a DR

*لازم نمشى بنفس الترتيب من فوق لتحت

- → (1) first Router to boot up : the Router that boots before others by 40 Seconds

  then

- → (2) Router having higest priority per interface
  by default the priority = 1 & we can change it by config from (0 → 255)
  *If Priority = 0 ∴ the Router can't be DR or BDR

  then

- → (3) Router having highest RID (Router ID) . . .

Router ID

if the loop back doesn't exist
- "Higest ip add. configured on loopback interface"
- "Highest ip configured as active interface"

RID = highest loop back & if it doesn't exist then, RID = highest active physical interface

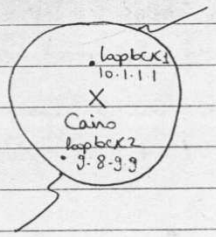
loopback interface :
- virtual S/w interface
- always up, need no "no shutdown"
- used in DNS Table, because if we use a physical interface it may be down any time
- we may use 0 → 4 milliars loopback interfaces
- configuration :

(config) # int ↓ loopback ↓ no (0 → 4 milliars)

(config-if) # ip ↓ address ↓ ip ↓ mask

⇒ we use mask /32 ≡ 255.255.255.255

a bit for host ⇒ 2^0 = 1 host as we've only 1 Router



RID = 10.1.1.1

we've no active interfaces to compare with

Cairo	10.1.1.1

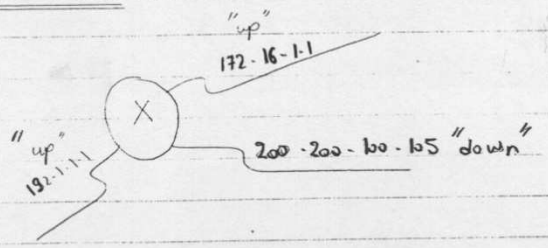
DNS Table

⇒ instead of using # Telnet ↓ ip we use ⇒ # telnet ↓ Cairo

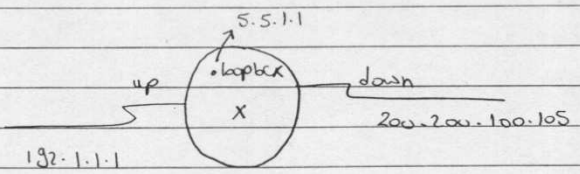
Higest IP configured as active interface

RID = 192.1.1.1

(highest physical active interface)

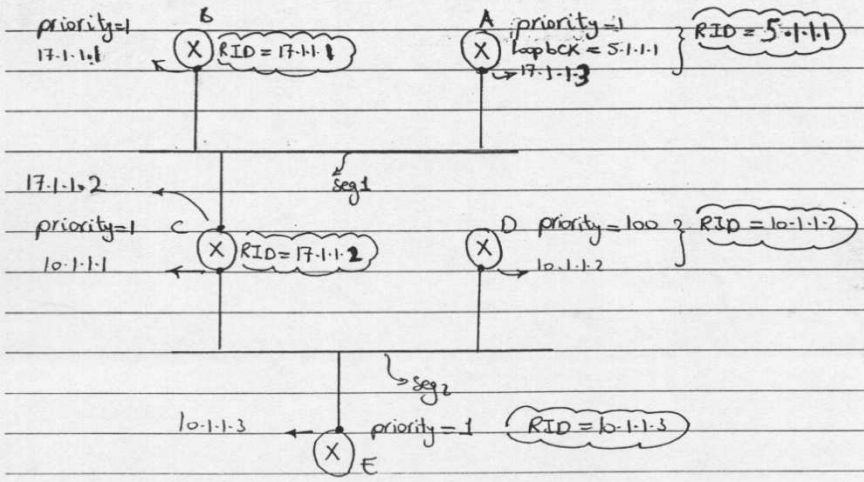


Consider this case



⇒ RID = 192.1.1.1 if no loopback, exist
but due to there is a loopback ⇒ RID = 5.5.1.1

ex: for each segment show who is DR & who is BDR

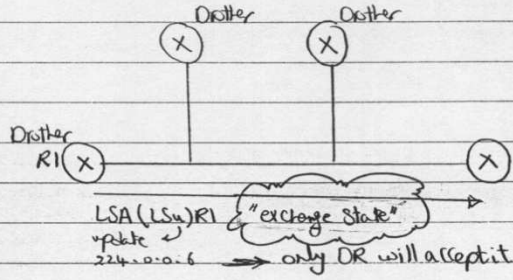


Seg1 : A, B & C are of the same priority
C has highest RID ⇒ "C is DR"
"B is BDR"

Seg2 : D has highest priority ⇒ "D is DR"
bet. C & E C has higher RID ⇒ "C is BDR"

(2) Route discovery " exchange protocol "

If a Router is not a DR or BDR ∴ It is called "Drother"



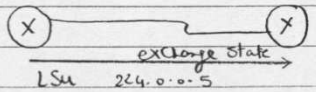
LSACK
↳ DR will reply with ACK

LSA (LSu) R1 to Drothers
224.0.0.5

LSACK
↳ each Drother will reply with ACK

& we reach Full State (Full adjacency) : All Routers have Data Base of each others ⇒ Full Convergence

In Case of point-to-point topology → No DR & No BDR



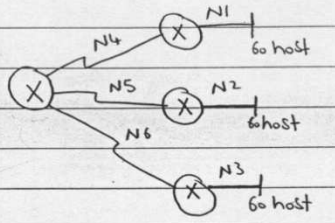
LSACK

LSu 224.0.0.5

LSACK

VLSM (variable lenght subnet mask)

Consider this case : we've major network 192.168.1.0/24 & we want to make Subnetting to cover this Networks



we've 6 networks, 3 of them each've 60 host, at least needs 6 bits & so we've only 2 bits for Networks (4 Networks only) ? so what shall we do

first we'll use mask /26 $\Rightarrow 2^2 = 4$ Networks

(1) new mask 255.255.255.192

(2) interesting octet = 192

(3) hop = 256 − 192 = 64

(4) 1Subnet 192.168.1.0/26 ⟨ .0 , .63 ⟩ } hosts ⇒ N1

2nd Subnet 192.168.1.64/26 ⟨ .64 , .127 ⟩ } hosts ⇒ N2

3rd Subnet 192.168.1.128/26 ⟨ .128 , .191 ⟩ } hosts ⇒ N3

4th Subnet 192.168.1.192/26 will be subnetted another time & ∵ N4, N5, N6 are pt-to-pt we'll use mask /30 ($2^4 = 16$ Net.)

(1) new mask 255.255.255.252

(2) interesting octet = 252

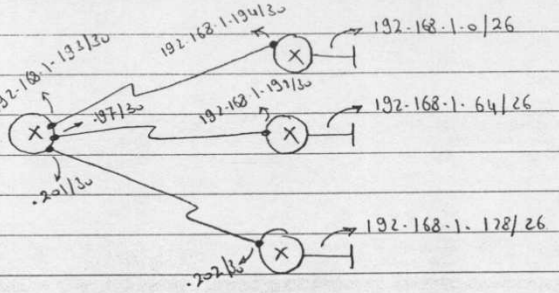
(3) hop = 256 − 252 = 4

1st Subnet = 192.168.1.192/30 ⟨ .192 , .195 ⟩ } hosts ⇒ N4

2nd Subnet = 192.168.1.196/30 ⟨ .196 , .199 ⟩ } hosts ⇒ N5

3rd " = 192.168.1.200/30 ⟨ .200 , .203 ⟩ } hosts ⇒ N6

& our final distribution will be as follows



⇒ When we've 2 bits for Network ∴ we may've 4 Networks, but is the 1st & 4th Networks are valid or not

To make the 1st & 4th Network valid use:

(config) * ip * Subnet-zero ⇒ enabled by default (Exam)

if we write (config) * no * ip * Subnet-zero

⇒ 1st & 4th Networks are invalid

& if you write 192.168.1.1/26 a msg will appear "Bad mask" (Exam)

(Exam) Which protocols can support VLSM ?

only classless protocols ⇒ that send the mask

ex: Ripv2, Eigrp, OSPF, IS-IS, BGP

(Exam) Which protocols can't support VLSM?

classfull protocols ⇒ that don't send the mask

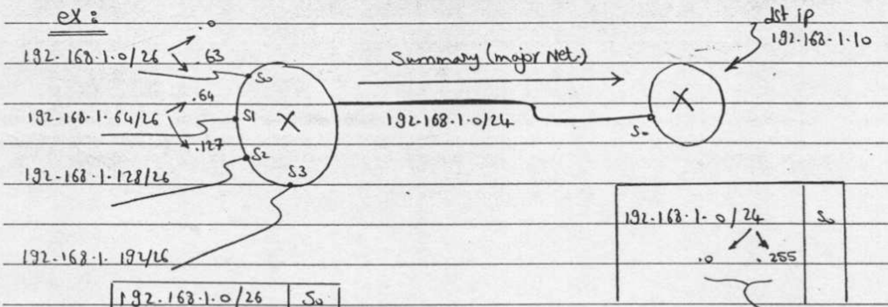
ex: Ripv1, igrp

Route Summarization (Rout aggregation) → تجميع

vs CIDR (Classless Interdomain Routing) "Super Netting"

Route aggregation It is the grouping of many subnets & advertising them as a single major network

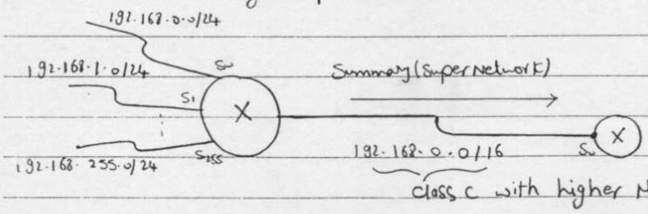
ex:



192.168.1.0/26	S0
192.168.1.64/26	S1
192.168.1.128/26	S2
192.168.1.192/26	S3

هيودي أضيق ال mask فى ال RT table
عشان ال router يعرف ال range of valid hosts

CIDR : It is the grouping of many major Networks & advertise them as a single super network



class C with higher Mask

* on Internet Routers know only Super Networks

C/C's of VLANs

(1) Each VLAN is a B.C domain (exam).

⇒ If a Switch has 4 VLANs ∴ this Sw has 4 B.C domains

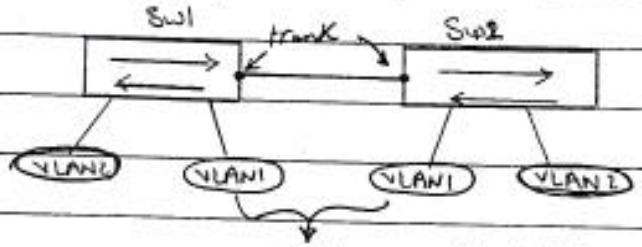
(2) VLANs Can enhance Network security

(3) Each department can be set in a VLAN (exam).

⇒ Sales → VLAN1 , Engineers → VLAN2

Secretaries → VLAN3

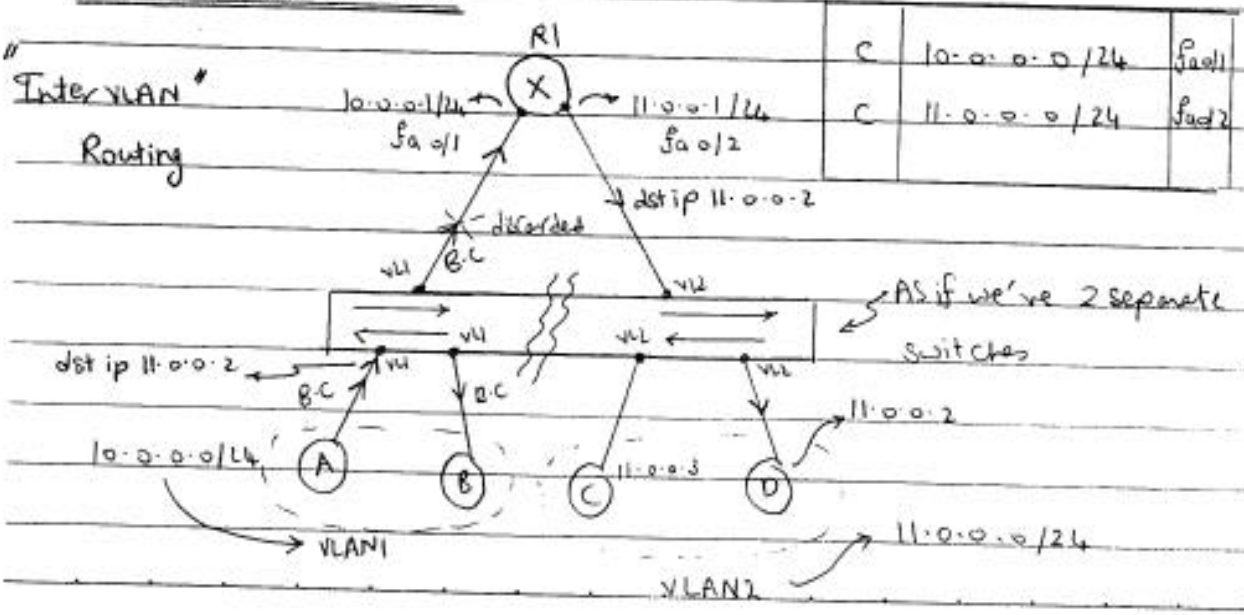
(4) VLAN Can Span multiple Switches



All the ports that belong to VLAN1 Share the same B.C domain.

To make a PC in a certain VLAN talk to another PC in another VLAN then we'll use a Router

"Inter VLAN Routing"



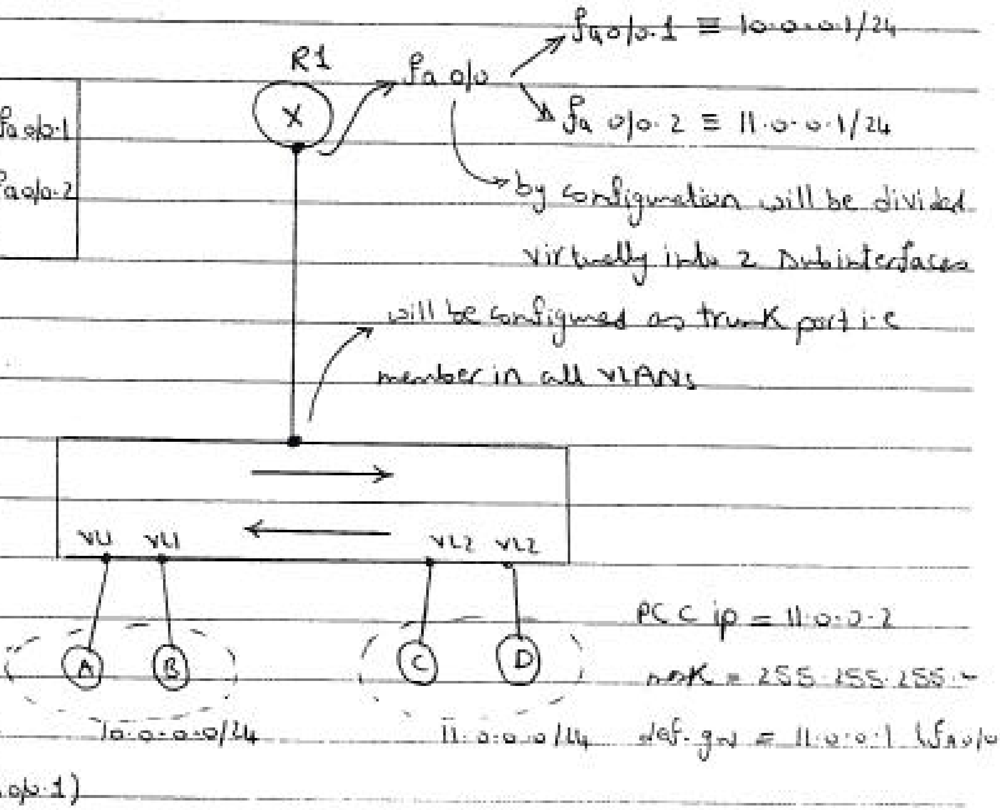
C	10.0.0.0/24	fa0/1
C	11.0.0.0/24	fa0/2

- Inter VLAN Routing: عشان A يعرف يكلم D لازم نستخدم Router

- لازم كل VLAN تكون في Subnet مختلفة وتكون واصلة على port من ال Router يكون منتمي لنفس ال Subnet بتاعت ال VLAN
* كل port على ال Router يكون واصل على Net. مختلفة وبالتالي لازم له ip مختلف.

- As no of VLANs ↑ ∴ we need large no of ports on the Router which is not desirable so we will use the concept of "Subinterfaces" as follow

C	10.0.0.1/24	fa0/0.1
C	11.0.0.1/24	fa0/0.2

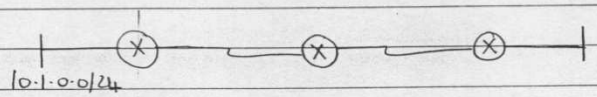


PC A ip = 10.0.0.2
mask = 255.255.255.0
def g.w = 10.0.0.1 (fa0/0.1)

PC C ip = 11.0.0.2
mask = 255.255.255.0
def. g.w = 11.0.0.1 (fa0/0.2)

⇒ The physical interface can be divided into up to 4 millions subinterfaces (virtual interfaces) & R1 will think that each port is a physical interfaces.

Eigrp & Rip v2 : Classless → Send the mask
Auto Summary → make auto Summary



10.1.0.0/24

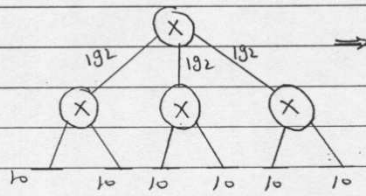
update
with mask
but still
auto Summary
10.0.0.0/8

to disable it we

(config) # router v eigrp v 200
(config-router) # no v auto-Summary

or (Config) # router rip
(Config-router) # version 2
(Config-router) # no auto-Summa

(Exam) we work with eigrp

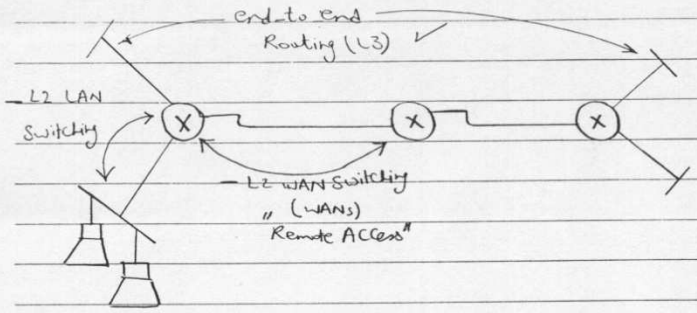


⇒ discontigeous
here we've to disable
the auto Summary

* on OSPF ⇒ summarization is manual

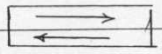
Session(20)
05/06/06

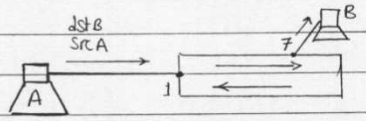
Switching



- Security
- NAT (Network Address Translation)

L2 LAN Switching :

Transparent Switch : L2 Switch 



MAC Table

MAC	port
A	1
B	7

Function of Transparent Switch

(1) learning : using Src MAC

(2) Forwarding :

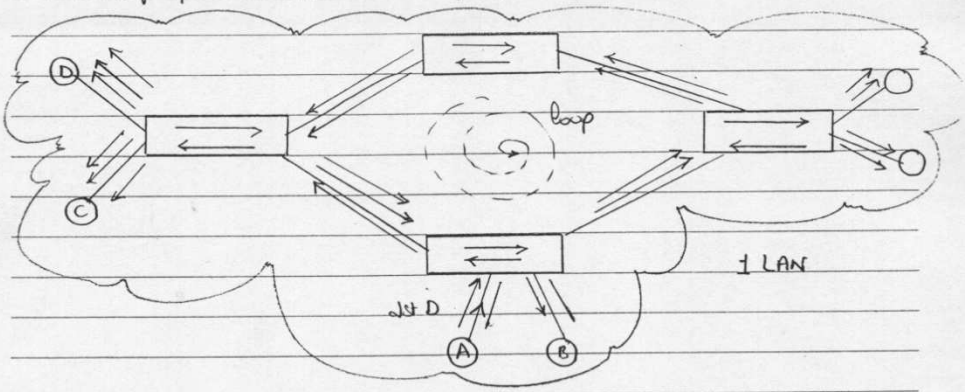
forwarding by flooding → unknown unicast dst
→ B.C
→ Multicast

(self Study)

RTG Table

(3) Remove L2 loop's

- using STP (Spanning Tree protocol) which will make virtual blocking for a certain port.
- STP work by default
- L2 loop's problem arises from multiple (redundant links)



→ this loop occur when only A decided to send to D, but imagin that at first all PCs will send a B.C msg, then a B.C Storm will occur so the only solution is to use STP.

STP operation "IEEE 802.1d"
↳ ie: Cisco متش تابع

At Start up

(1) Each Switch will form BPDU (Bridged protocol Data Unit = Bridged frame) describing itself & send it out of all its interfaces every 2 seconds

port ID	Accumelated path cost	Switch ID
port 1, 2, ..	المسافة التراكمية	مبدئ الى أدناه

(2) Root bridge (Switch) Election: All Switches (Bridges) will try to elect a root Switch (Bridge) which has the least Switch ID.

الأقل هو الأحسن

default = 32768	priority (2 bytes) 0 → 65535	System MAC Address (6 bytes)	= "Switch ID"

MAC adr. for the internal processor of the Switch & it doesn't repeated

الأقل هو الأحسن

⇐ الأول نشوف الـ priority ونختار الأقل ولو زي بعض نختار اللي الـ System MAC أقل

* ⇒ After we elect the Root Switch (Bridge) then, the root only will send BPDUs.

(3) Elect Root port (RP) : It is the best port on every non-root switch (bridge) that can reach the root switch (bridge) based on :

(1) least accumulated path cost (Bw)

(2) port connected to least neighbor ID

Bw	cost
10M	100
100M	19
1G	4
10G	2

(4) Elect Designate port (DP) :

- Best port on each segment that can reach the root switch, based on :
  (1) least accumulated path cost (Bw)
  (2) port connected on least switch ID

N.B - All ports of the root switch (bridge) are considered DPs

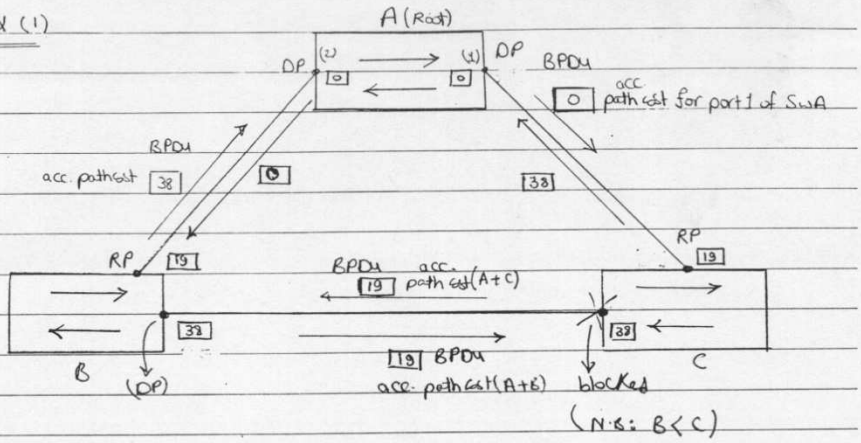
(5) Blocked port (BP) : port that is neither DP or RP

best port on the segment

best port on the switch

if we've 2 ports : the port connected on least switch ID is better & we'll block the other port.

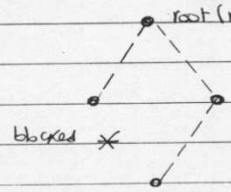
ex (1)



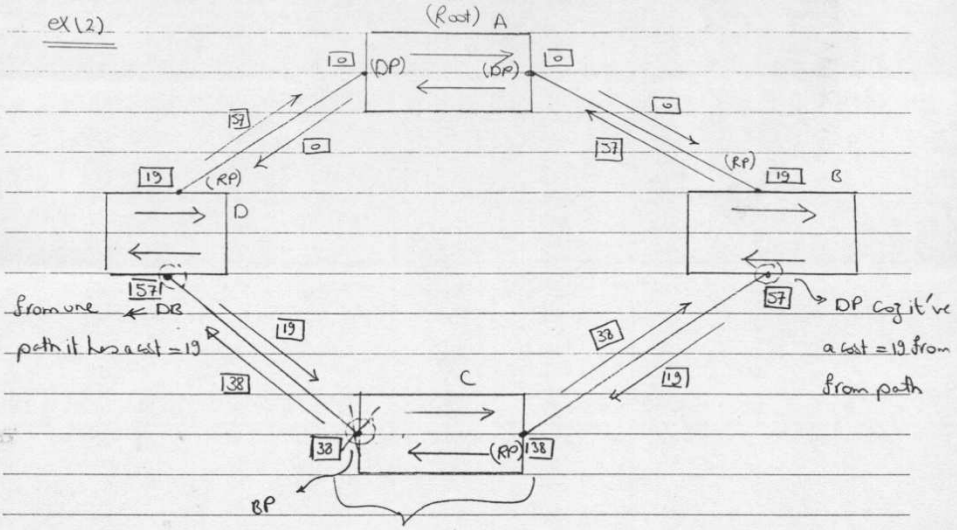
assume :- SwA, B, C All operate with Fast ethernet 100 Mbps
i.e cost = 19

STA (Spanning Tree Algorithm)

يتم انتخاب root switch (reference) وكل سك يحاول الوصول الـ root بسكة واحدة فقط وهذا معناه انه كل واحد يعمل الـ سك الثاني بسكة واحدة فقط ولكنه لا يركل الـ سك تتفعه على الـ blocked link



ex(2)

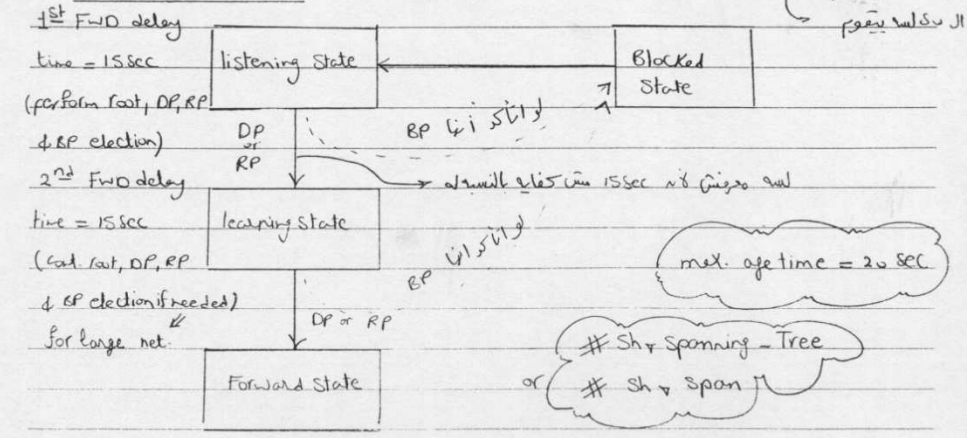


2 ports of same acc. cost but one connected to SwB & the other connected to SwD & ∵ B<D

∴ the one connected to SwB is chosen as (RP)

STP port states (@ Startup)

POST & IOS & config. file loading



. max. age time : It is the time the port stays in blocked state before it

(1) <u>Disabled</u> : No Cable is connected or port is Shut down

(2) <u>Blocked State</u> : the port won't T^x data frames & will drop received data frames
but listen to received BPDUs

← عشان لو أي port تانية بقت Blocked هذه ال port تعرف
وترجع تشتغل تاني

(3) <u>listening State</u> : the port won't T^x data frames & will drop received data frames
but process BPDUs for Root, RP, DP election

(4) <u>learning State</u> : the port won't T^x data frames & will drop received data
frames but after learning from them to build the MAC Table
& still process BPDUs to double Check Root, RP, DP

← ال data اللي جاية يتعلم منها ويرميها

(5) <u>Forwarding</u> : The port will start forwarding the data frames &
still processing BPDUs (R^x & FWD BPDUs)

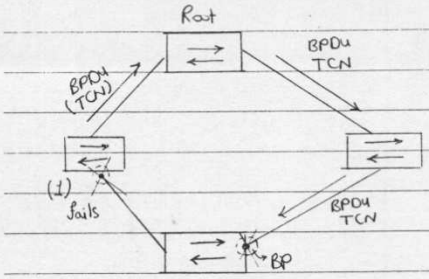
By default all ports of the switch are "no shutdown"
≡ plug & play

<u>At Convergence</u> : Any port will be either

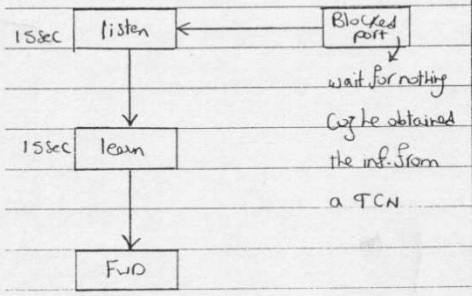
- Blocked state
- DP or RP

At Change :

(1) Normal Change
(If cable is down)

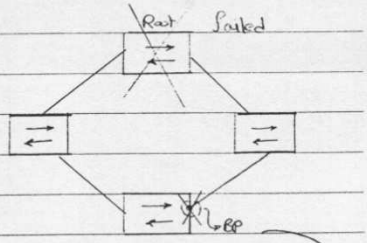


_TCN ≡ Topology Change Notification
It is a BPDU sent from the Sw that sensed the change to the root, So the BP goes to the listen state then learn state then activated

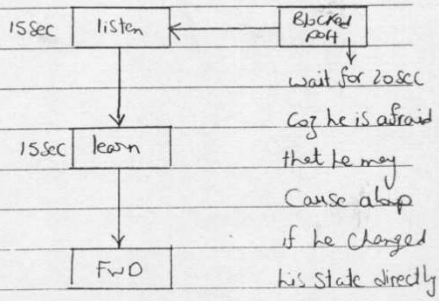


⇒ Convergence occurs after 30 sec

(2) Fatal Change
(If the Root failed)



الفروم الـ Root بيبعت كل BPDU
2osec بيستنى Blocked port خلال 2 sec
مقبل ولو الـ 2osec فاتت to BPDUs
من غير ما يصح حاجة من الـ
Root يعتبر وقع ويبدأ الـ Blocked port
يشتغل



⇒ Convergence occurs after 50 seconds

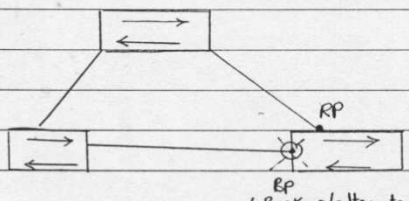
⇒ STP is not used now Coz its convergence time is high ~ 50 sec, Instead RSTP is used.

Rapid STP (RSTP) IEEE 802.1w

It introduced the following

(1) disabled, blocked & listen state is grouped in only 1 state called "Discard State"

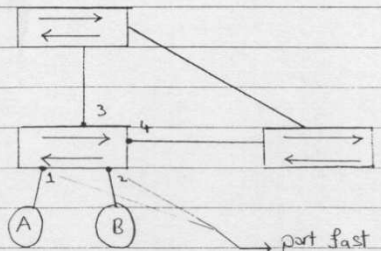
(2) Introduced Backup (or alternate) port for every RP & DP for the same switch



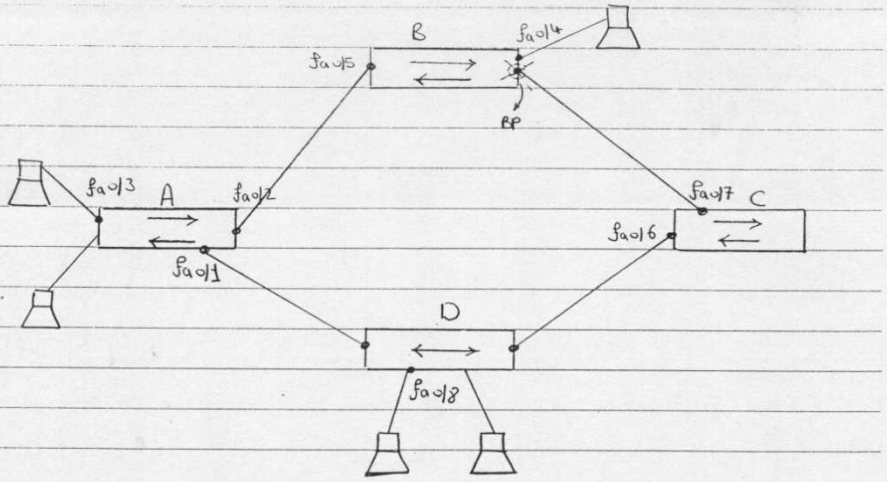
→ If the RP is down then the RP will change its state immediately to be RP & it doesn't wait for 30 sec. as before (rapid change)

(3) Introduced the concept of port fast (port that can enter the fwd state immediately, in case it is connected to a PC or server)

• When the Network is up, ports 1 & 2 go immediately to the Fwd state while ports 3 & 4 are still in the blocked state & so PC A can T^x & R^x data to PC B & ∵ PC A & B lie on the same switch then they won't cause loops



Example : "come In all exams"



- Which ports can be port fast

(a) Fa 0/1 (b) Fa 0/2 (c) Fa 0/3 (d) Fa 0/4 (e) Fa 0/5
(f) Fa 0/6 (g) Fa 0/7 (h) Fa 0/8

ans: (c) Fa 0/3 & (d) Fa 0/4

- Which of the following devices can be the root

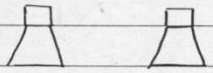
(a) A (b) B (c) C (d) D

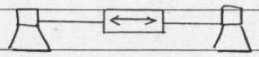
ans : (a) A

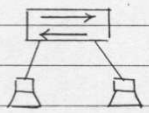
Session (21)
07/06/06

Topics :
* VLANs over view
* VLAN membership
* Switch port types (Access ports, Trunk ports)
* Trunking Types
* Configuration VLANs
* VTP
* VTP Configuration

VLANs (virtual LANs)

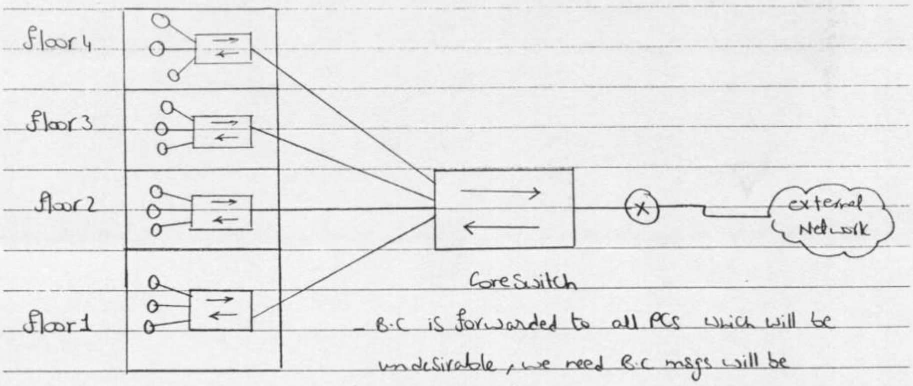
(1)  2 Separate devices (No Sharing)

(2) Hub 
- Single collision domain
- Single B.C domain

(3) Switch 
- multiple collision domains
- Single B.C domain
  becomes a problem for large LANs

main B.C msgs
- frequent ARP Requests (to know dst MAC)
- Multicasting applications

B.C Storms may occur



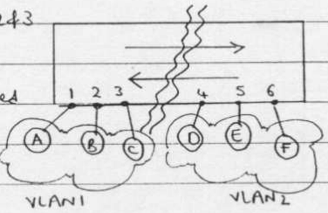
- B.C is forwarded to all PCs which will be undesirable, we need B.C msgs will be within the floor switch but Any PC can talk using a unicast add. to Any other PC in any floor.

__To Solve this we'll use VLANs__

. VLAN is a S/W defined on the switch

. When no. of ports belong to a certain VLAN then as if we divide our switch to no. of groups each group belong to a certain VLAN.

. by config. when ports 1, 2 & 3 are defined in VLAN1 & ports 4, 5 & 6 are defined in VLAN2 ∴ PCs connected to each port will belong to a certain VLAN according to the port, the PC is connected to.



PCs A, B & C ⇒ VLAN1 & PCs D, E & F ⇒ VLAN 2

. B.C msg from A goes to → B & C only

unicast msg from A to D → will be discarded !! ⇒ unicast msg ال احنا عايزين .

Routing توصل ← لازم نستخدم

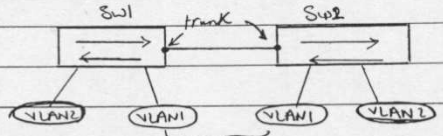
C/C's of VLANs

(1) Each VLAN is a B.C domain.
⇒ If a Switch has 4 VLANs ∴ this Sw has 4 B.C domains

(2) VLANs can enhance Network security

(3) Each department can be set in a VLAN
⇒ Sales → VLAN1 , Engineers → VLAN2
Secretaries → VLAN3

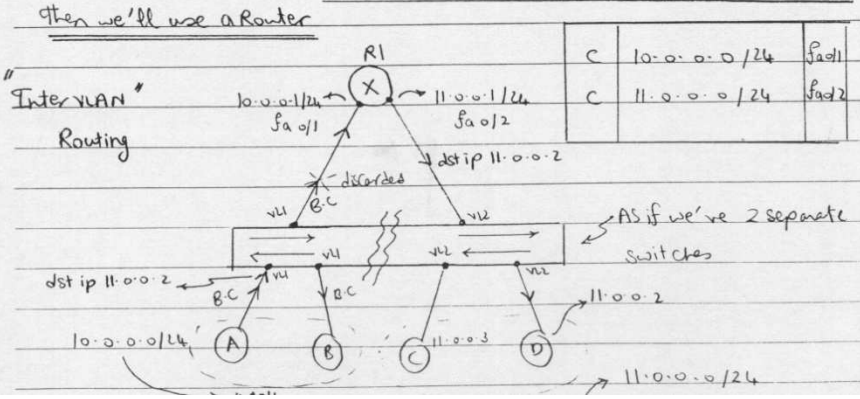
(4) VLAN can span multiple Switches



All the ports that belong to VLAN1 share the same B.C domain.

To make a PC in a certain VLAN talk to another PC in another VLAN then we'll use a Router

"Inter VLAN" Routing

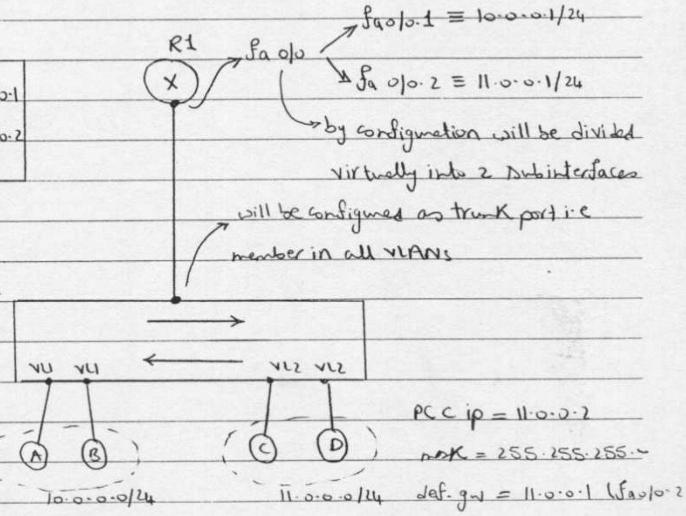


— InterVLAN Routing: عشان A يعرف يكلم D لازم نستخدم Router

— لازم كل VLAN تكون ذ Subnet مختلفة، وتكون واصلة على port
من ال Router يكون منتمي لنفس ال Subnet بتاعت ال VLAN
* كل port على ال Router يكون واصل على Net مختلفة وبالتالي لازم
له ip مختلف.

— As no. of VLANs ↑ ∴ we need large no. of ports on the Router which is not desirable so we will use the concept of "Subinterfaces" as follow

C	10.0.0.1/24	fa0/0.1
C	11.0.0.1/24	fa0/0.2

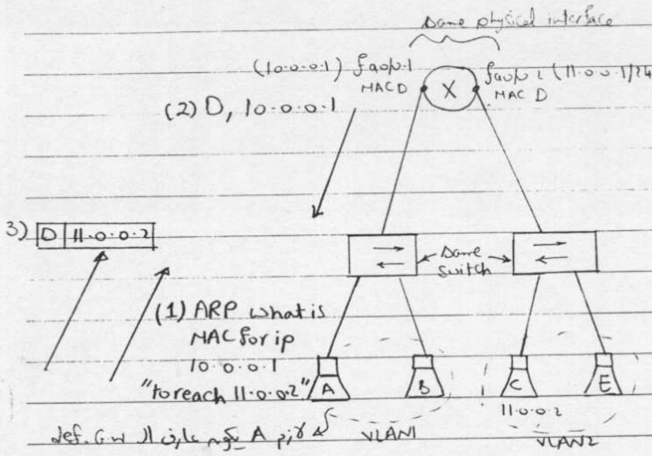


PC A ip = 10.0.0.2
mask = 255.255.255.0
def. g.w = 10.0.0.1 (fa0/0.1)

PC C ip = 11.0.0.2
mask = 255.255.255.0
def. g.w = 11.0.0.1 (fa0/0.2)

⇒ The physical interface can be divided into up to 4 millions subinterfaces (virtual interfaces) & R1 will think that each port is a physical interfaces.

ARP & proxy ARP



لازم A يكون عارف ال def. GW
عشان تقدر تعمل ال unicast لـ dst
موجود في VLAN تانية

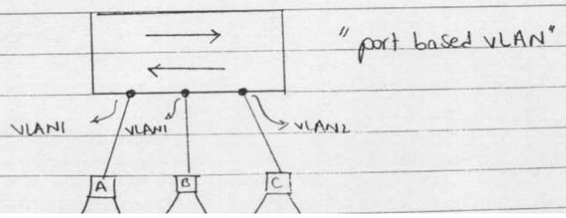
ARP Cache of PCA

ip	MAC
10.0.0.1	D

VLAN membership

(1) Static membership : Static VLAN assignment

→ VLAN assignment for the port & not for the PC
→ The PC will belong to the VLAN that the port belongs to
→ By default all ports belong to VLAN1



(2) Dynamic membership: "MAC based VLAN"

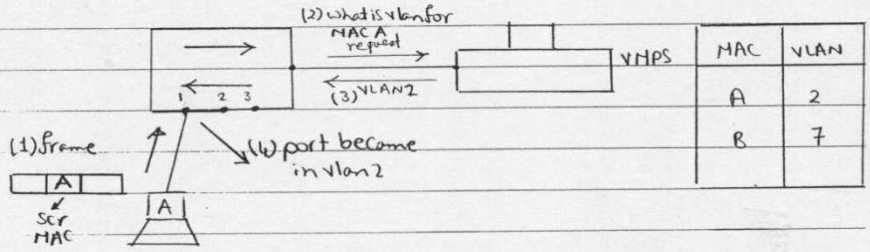
⇒ assign certain MAC to certain VLAN

⇒ ex:-

MAC	VLAN
A	2
B	7

- If PC A will belong to VLAN 2 either it is connected to port 1 or port 2 or ---
- but how the PC knows the VLAN he belongs to ??

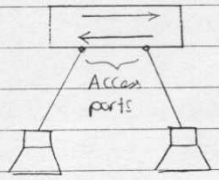
⇒ the PC will send a request to a VMPS (VLAN Membership Policy Server) to know the VLAN he belongs to



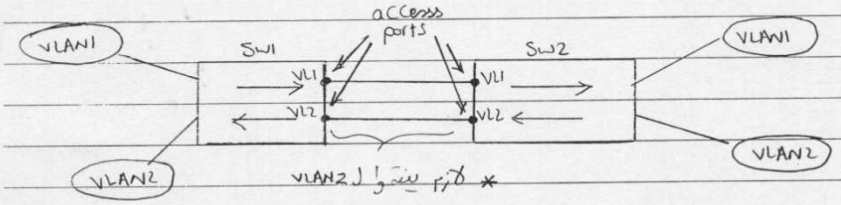
MAC	VLAN
A	2
B	7

Switch port types

(1) Access port : port that is member in only 1 VLAN
i.e port connected to a PC



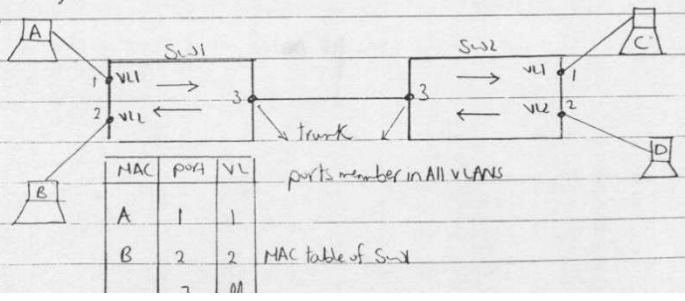
consider the case we've 2 switches as follow



* لازم ينتموا لـ VLAN2
عشان يقدروا يوصلوا كل الـ PCs
اللي بتنتمي لـ VLAN2

⇐ معنى كده لو عندنا 100 VLAN لازم يبقى عندنا 100 port يوصلوا بين Sw1 & Sw2
وهذا الكلام مش logic !!!

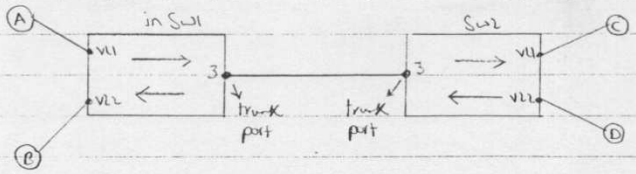
(2) Trunk port : port that is membered by default in all VLANs
(port connected to Switch or Router)
help to make lan spans multiple SWs → يساعد



MAC	port	VL
A	1	1
B	2	2
	3	All

ports member in All VLANs

MAC table of Sw1



⇒ A can't talk to D coz there is no Router to permit intersting between different VLANS

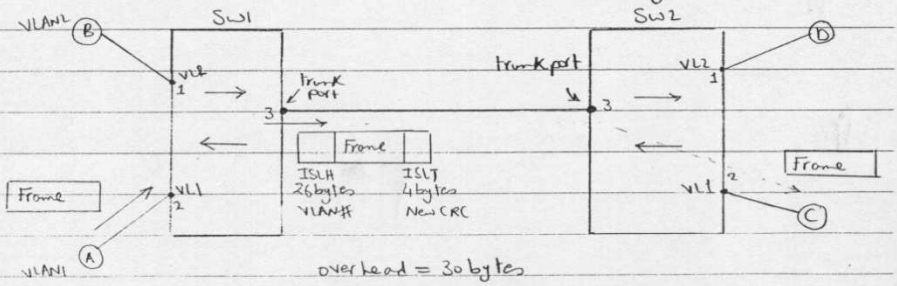
⇒ there is a big problem ?!!

If A send a B.C msg, this B.C msg should go to C only who lies in VLAN1 but ∵ port 3 in Sw2 is trunk & member in all VLANS then he will forward it to all VLANs he is connected to i.e PC C & D ?!

⇒ to solve this, port 3 on Sw1 should add a tag to the original coming frame to make the other trunk port know which port he will fwd the msg to.

Tagging types : Help in inter-Switch communication

(I) ISL (Inter Switch Comm. link) ⇒ Cisco proprietary i.e works on Cisco Switches only
↓
between

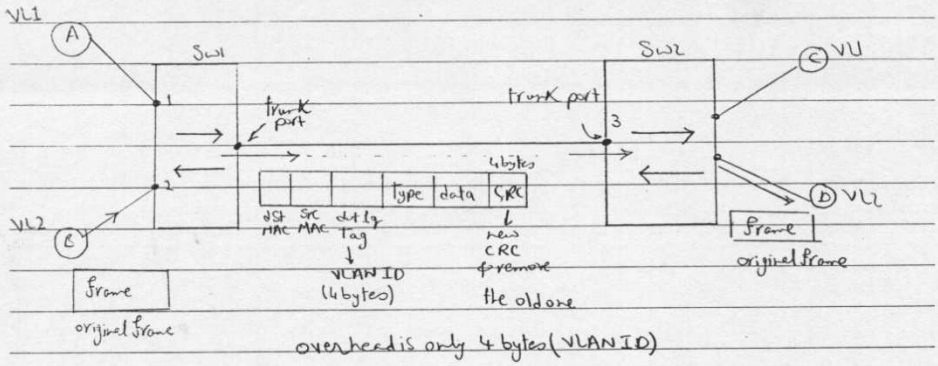


overhead = 30 bytes

⇒ the trunk port (port 3) on Sw1 will add an ISL header (26 bytes) contains the VLAN ID & an ISL trailer (4 bytes) to make port (3) on Sw2 know to where the msg will go, port 3 on Sw2 will remove ISLH & ISLT & Forward

N.B: If Sw2 doesn't know C, then Sw2 will flood the frame through all ports that belong to VLAN1 only

(II) IEEE 802.1q (dot1q)



overhead is only 4 bytes (VLAN ID)

Dot1q Supports both Tagged & un Tagged frame ??

⇒ by default all ports belong to VLAN1 "native VLAN", so if we don't add a tag ∴ the trunk port will direct the frame automatically to all devices that belong to VLAN1

⇒ when A wants to talk to C then port 3 on Sw2 will direct the frame automatically to those who're members in VLAN1

Tagging types "cont'd"

(III) 802.10 for → FDDI

(II) LANE for → ATM
(LAN Emulator)

Configuration of VLANs

(1) Create VLANs (2) name VLANs (optional) ex: sales, engineers

(3) assign VLAN to switch ports → obligatory

To create & give a name to a VLAN we've 2 methods

	OR	
⇒ This configuration is saved in config. file in NVRAM		⇒ This config. is saved in a file called VLAN.dat on the flash memory of the switches
# conf t		# VLAN database
(config)# VLAN _____ #		(VLAN)# VLAN _____ # [name _____]
(config-VLAN)# name _____		(VLAN)# {apply / exit} → to save file on flash memory
# copy run start (important)		

To remove a VLAN we

(config)# no VLAN _____ #

⇒ VLAN1 is created by default but we can give it a name but we can't remove it.

To assign VLAN to switch ports

(I) Access ports (config)# interface _____ Fa 0/2

(config-if)# switchport mode access

(config-if)# switchport access VLAN _____ VLAN #

* N.B: access port can't be member in all VLANs, we've no

(config-if)# switchport access VLAN all

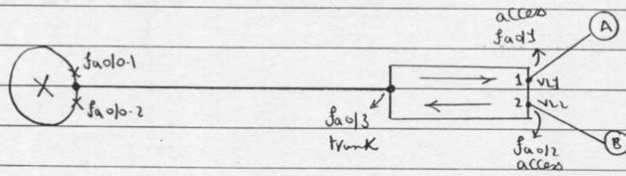
II Trunk port

(config)# interface fa0/3
(config-if)# switchport mode trunk
(config-if)# switchport trunk encapsulation {isl / dot1q}

⇒ Cisco switches 're called catalyst 2950 ⇒ supports only dot1q format
→ this command doesn't exist on cisco switches 2950 or 2960

Inter VLAN Routing : "Router_on_Stick"

configuration of the subinterfaces on the Router



Router(config)# interface fa0/0
Router(config-if)# no ip address → مينفعش احط ip لل port بل subint
Router(config-if)# no shutdown

Router(config)# interface fa0/0.1 → .1, .2, ... upto 4 millions
Router(config-subif)# ip address ip mask
Router(config-subif)# encapsulation {dot1q/isl} VLAN #
علشان ال Router يعرف الحاجة اللي جاية من ال Switch شغالة بأي format
isl / dot1q

DTP (Dynamic Trunk protocol) : Auto negotiate wheather port is access or trunk
↳ Cisco proprietary

⇒ on Cisco Switches you don't have to configure the switch ports access or trunk, but there is a slw (protocol) used by switch ports to know wheather it is access or trunk according to the device that the port is connected to

⇒ The switch port will send a DTP msg
(1) If no reply, then this port is connected to PC as PCs can't understand DTP msg. & this port will be access

(2) If there is a reply, then this port is connected to either a Cisco Switch or [illegible]

modes :

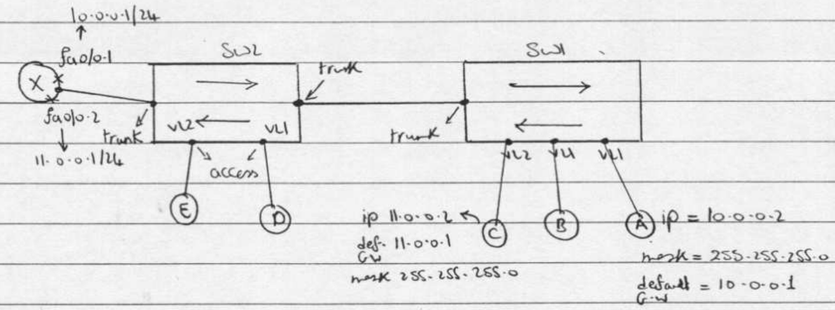
- no negotiate ≡ on (between Switches Mode)
↳ the port won't send DTP msgs & still trunk always

- Trunk ≡ off (" " ")
↳ the port will send DTP msgs & negotiate to remain trunk

- Dynamic desirable ≡ Desirable (" " ")
↳ the port well negotiate & it may be trunk or access
- Dynamic auto ≡ auto (" " ")

A VLAN can span multiple switches "توضيح"

⇐ يمكن أن يتم توصيل بعض ال ports على Sw معين ببعض ports
آخرين على Sw تاني بعيد بجعلهم ف VLAN واحده



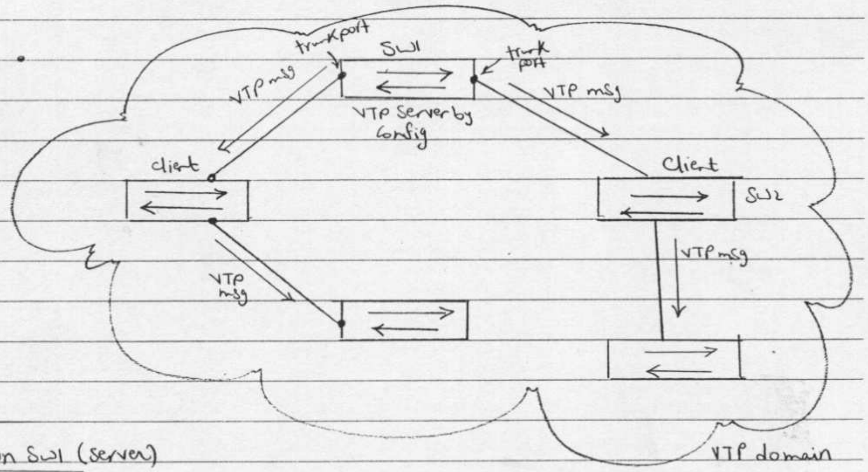
– now A, B & D ⇒ share the same B.C domain (VLAN1)
C & E ⇒ 〃 〃 〃 〃 〃 (VLAN2)

– A can send a unicast msg to C or E coz we've a Router, a msg from A to C will go first to the Router & then Back to C to Sw1

VTP (VLAN Trunking protocol) "Cisco proprietary"

- It is an easy administration method for configuring VLANs.
- It allows configuration of VLANs (create, delete, modify & naming) to be made on only 1 switch & to be propagated to all other switches through VTP msgs, but with only 1 condition:

  All switches must be in 1 VTP domain.



On SW1 (server)

(config) # VLAN 7
(config-VLAN) # name Sales
copy run start

} we create VLAN #7 & give it a name = Sales

→ then SW1 will send a VTP msg to the clients & each client that receives the VTP msg will save it & FWD it to other clients.

→ When SW2 save the VTP msg coming from SW1, this is as SW2 create a VLAN #7 that has a name sales

← يعني Sw2 مش محتاج يـ create VLAN7 ويعملها pt لأن ال server عملها creation خلاص

← أي port على Sw2 يعملها assigning إنها في VLAN7 حتاخد بنفس ال config.

N.B :-

(1) VTP msgs are sent on trunk ports only

(2) VTP msgs are flooded inside a single VTP domain

Switch VTP modes

(1) VTP Server

⇒ by default any switch is a VTP server

(2) VTP Client

⇒ we can't write config. on it manually, but only configured by VTP msgs

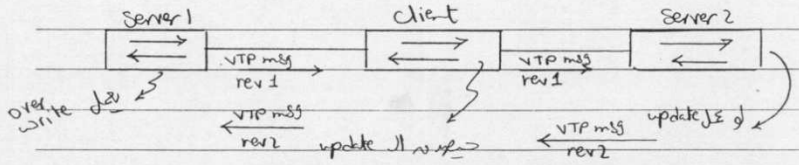
(3) VTP Transparent

⇒ Fwd the VTP msgs & doesn't affected by it

⇒ we can write on it manual configuration & he will not fwd this configuration.

Exam :- If we've no. of VTP Servers ⇒ !!! [illegible]

this is using "configuration Revision no." ~> incremented by 1



Server 2

N.B :- VTP version 1 & VTP version 2 are incompatible

Configuration of VTP

(config) # VTP domain domain name
(config) # VTP mode {client/server/transparent}
(config) # VTP password password

لازم ال switches يكون ليها نفس ال password عشان
ترضى تستقبل ال VTP msgs ، وممكن منستخدمش password أصلاً"

OR

On VLAN mode → (VLAN.mod)
(VLAN) # VTP domain domain name
(VLAN) # VTP {client/server/transparent}
(VLAN) # VTP password password

Showing use: # Sh VTP status ↵

VTP domain :
VTP mode :
VTP rev. no. :
VTP password :
VTP version :

note : VTP version 1 is incompatible with VTP version 2

Another Shows

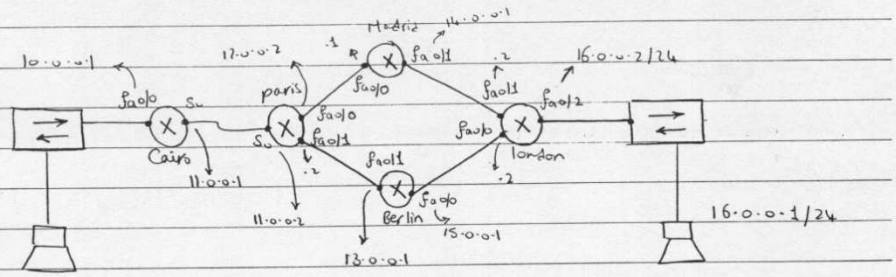
Sh Mac-address_Table (port vs MAC vs VLAN #)
→ or # Sh mac
Sh VLAN (port vs VLAN)

Sh interface trunk (show which interfaces are trunk)

Session (22)
10/06/2015

Simulation (lab3)

open Simulator lab 2 → lab 2 new topology



⇒ By default for any router at starting of config. we'd make the following

Router > en
conf t
(config)# hostname ——
(config)# int ——
(config-if)# ip address ——
(config-if)# no shut down

- if you've a serial interface you should know weather it is DCE/DTE

sh controller S0

If this is a DCE interface use the following command to set CLK rate

(config-if)# clock rate ——

⇒ Then you should make L1 & L2 check using

sh ip int brief

OR

sh cdp neighbors ⇒

→ Then you should make L3 Check using

* Sh ip route

OR

* Sh ip protocols

↳ if you types this command you'll find nothing cz we define no RTG protcol

---

Let's define a RTG Protocol

Eigrp : "classless"

on each Router we should activate all interfaces to work with eigrp as follow :-

on Cairo (config) * router eigrp 100 → AS *

(config-router) * network 10.0.0.0 } will activate all interfaces that lie in Subnets taken from the major networks 10.0.0.0 & 11.0.0.0

(config-router) * network 11.0.0.0 ↗

- eigrp is classless i.e send mask in updates but this is not an update it is just the network no.

→ After we activate all interfaces on all Routers to work with eigrp we'll make some shows

* Sh ip route

D 16.0.0.0 [90/2455040] via 11.0.0.2, 00:14:38, Serial0

D : eigrp
[90/2455040] : 90 Admin dist, 2455040 composite metric
via 11.0.0.2 : ip of next hop
Serial0 : through my interface S0

* Sh ip protocol

K's (Eigrp metric weight) $K_1 = K_3 = 1$ & $K_2 = K_4 = K_5 = 0$

distance : internal = 90 external = 170

Eigrp make some tables

(1) RTG Table → # Sh ip route [eigrp]

(2) Neighbor Table → # Sh ip eigrp neighbors
↳ direct connected + working eigrp

(3) Topology tables → Sh ip eigrp topology
↳ RTG Table of your neighbors

on pairs

P 12.0.0.0/24 , 1 successor , FD is 28160 via --- (28160/0)

P → passive (convergence state)

1 → best path only

FD → feasible distance (src → dst metric)

via → if not direct connected

(28160/0) → FD → Advertise distance

if a Network is down it will convert into active state (A)

active state = sending a query msg to ask if any other router knows a better path to the failed Network

224.0.0.10 →

If reply comes (ok/not) ← the Router will return back to the passive state

let's define another RTG protocol → "OSPF"

Now OSPF will work in parallel with eigrp but in the RTG Table we'll see only eigrp ("D") ∵ it has lower admin distance = 90

N.B: In RTG Table we show the best protocol & the best path

On Cairo

(config)# router OSPF 1 (1 → 65535) → process ID (local significant)

(config-router)# network 10.0.0.0 0.0.0.255 area 0

(config-router)# network 11.0.0.0 {0.0.0.255 / 0.255.255.255 / 0.0.0.0} area 0

wild mask = inverted subnet mask

process ID & AS# take no.s from 1 → 65535 & can't be zero "exam"

N.B: The perfect ans. in exam is to use the wild mask as the inverted subnet mask

we may activate all the interfaces on the router to work with OSPF as follow

(config-router)# network X.X.X.X 255.255.255.255 area 0

↳ متبقيش مطابقة لل net-ID

* but don't use it in exam or you won't get the full mark

→ then activate all other interfaces on paris, london, Madrid & Berlin to work with OSPF

→ to deactivate the eigrp use:

(config)# no router eigrp 100

→ now we can see OSPF in the RTG Table

→ لو عايز ترجع لل eigrp لازم نكتب كل حاجة تاني
يعني لازم نعرف ال Networks تاني

Shows on layer (3)

on pairs

Sh ▾ ip ▾ route

O — [110/64]
↓ OSPF — Admin distance — metric = $\frac{10^8}{B.W}$

Sh ▾ ip ▾ OSPF ▾ neighbor ( ) → no "S"

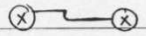
neighbor ID	Pri	State	Address	Int
13.0.0.2	0	Full / ( )	11.0.0.2	S0 (my interface)

"Router ID"
- loopback
- IP of highest physical int

Full/( ) →
- DR
- BDR
- Drother
- —

Full/( ) → Full state = Full adjacency

in case of pt-pt connection we only've 1 path & no there is no elections



** # Sh ▾ ip ▾ OSPF ▾ interface (All details (v Imp))

(1) Fa 0/0 } list of active interfaces
Fa 1/0 }

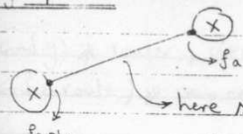
(2) Area 0 (3) process ID 1 (4) Router ID 15.0.0.1

(5) DR/BDR/Drother (6) cost 1 = $\frac{10^8}{B.W}$

(7) DR ID is 15.0.0.2 BDR ID is 15.0.0.1

(8) Hello every 10 sec & dead interval 40 sec

very very imp. rule



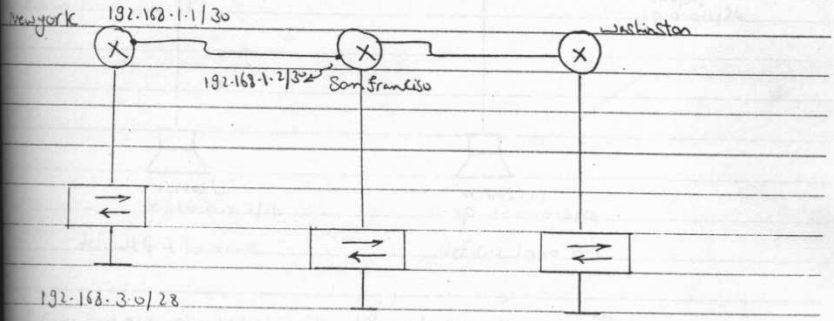
→ here some switches exist that appear ESL on L3

⇒ This is not a pt-pt connection so we may connect a router. any time we need on the intermediate switches

In Exam : where is the fault?

load Netmap → new exam simulator OSPF

load multidevices config → new exam Sim OSPF



mask/28 ≡ 255.255.255.240

the wild mask = 0.0.0.15

mask/30 ≡ 255.255.255.252

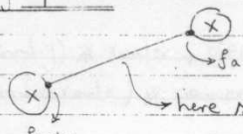
the wild mask = 0.0.0.3

The faults : (1) Network Mask is wrong

(2) area # is wrong

(3) 1 Network is missing

* Very very imp. note



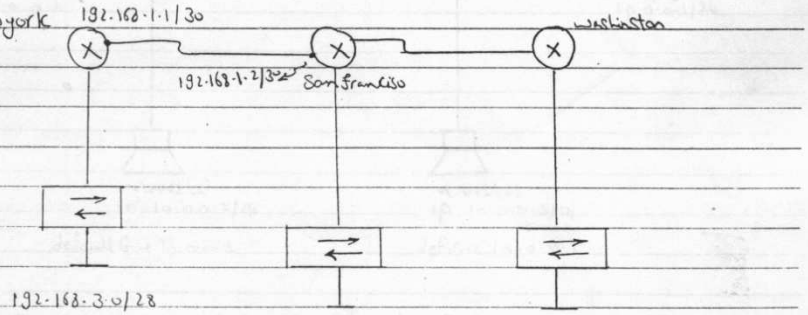
here some switches exist that appear as L2 on L3

⇒ This is not a pt-pt connection so we may connect a router any time we need on the intermediate switches

In Exam : where is the fault?

load Netmap → new exam simulator OSPF

load multidevices config → new exam Sim OSPF



⇒ mask/28 ≡ 255.255.255.240

∴ the wild mask = 0.0.0.15

⇒ mask/30 ≡ 255.255.255.252

∴ the wild mask = 0.0.0.3

The faults : (1) Network Mask is wrong

(2) area # is wrong

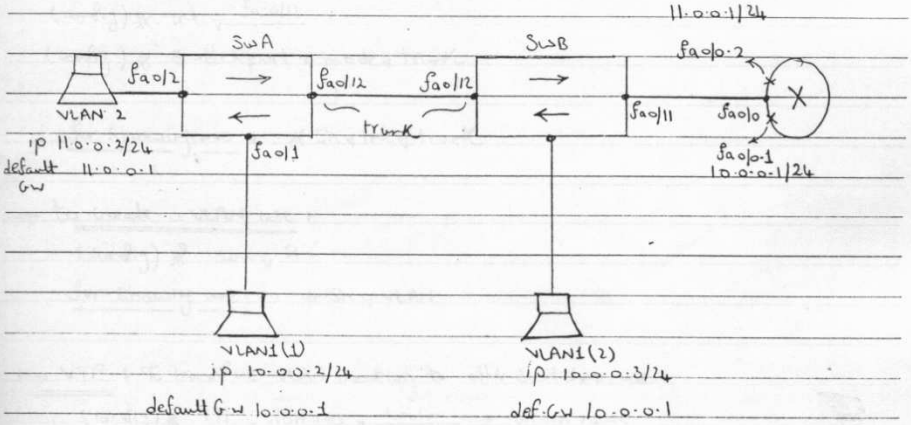
(3) 1 Network is missing

NB: To enable Centum ID configuration use the following

(config) # router ▽ OSPF ▽ 1 ↵
(config-router) # no ▽ network ▽ ip ▽ wildmask ▽ area ▽ 0 ↵

Switching:

load Netmap → interVLAN Routing



N.B:- Each VLAN should belong to different Subnet.
. the default G.W of VLAN1 should belong to the same Subnet of VLAN1
= = = = VLAN2 = = = = = = VLAN2

Configuration will be made on any switch @ startup'

on SwA

(config)# hostname SwA → give the switch a certain name

⇒ Then you've to designate wheather your port is trunk or access, we've no DTP on the simulator so there is no automatic negotiation & we will assign ports to VLANs manually as follow:

(config)# int fa 0/12
(config)# switchport mode trunk

for showing use: # Sh int trunk

⇒ to create a VLAN use:
(config)# vlan 2
for showing use: # Sh VLAN

⇒ VTP: To transfere VLAN creation to other switches use
(config)# VTP domain Cisco → domain name
(config)# VTP mode Server → by default all switches are servers
(config)# password amr
→ لازم يتم كتابتهم على كل ال Switches مش على واحد فقط

Showing: # Sh VTP Status
VTP domain:
VTP mode:
VTP rev. no.:
VTP password:
VTP version:

on SwA

→ To create port access

(config)# int fa0/1

(config-if)# switchport mode access

(config-if)# switchport access VLAN 1 ⇒ Any port is by default in VLAN1, so we may not write this command

(config-if)# int fa 0/2

(config-if)# switchport mode access

(config-if)# switchport access VLAN 2

→ on the Router : to make VLAN1 talk to VLAN2 we'd use RTG

(config)# int fa 0/0.

(config-if)# no ip address

(config-if)# no shutdown

(config)# int fa 0/0.1

(config-subif)# ip address 10.0.0.1 255.255.255.0

(config-subif)# encapsulation dot1q 1 → VLAN1

(config-subif)# int fa 0/0.2

(config-subif)# ip address 11.0.0.1 255.255.255.0

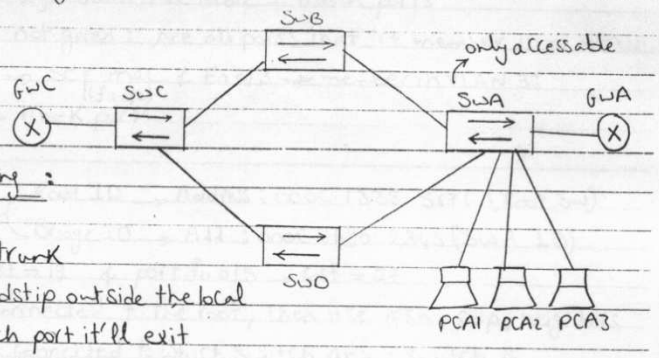
(config-subif)# encapsulation dot1q 2 → VLAN2

The as previous. but with different method of illustration.

example :-

load netmap → new exam simulator Switching 2

load multidevice configuration → command 1



⇒ you only have the rights to access SwA

⇒ Answer the following :

(1) which ports're trunk

(2) If a pck with dstip outside the local LAN from which port it'll exit

(3) If a frame with dst MAC _____ & Scr MAC _____ from which port it'll exit

(4) which switch is the root bridge of VLAN

(5) If a new switch enters the Network with the following

SwX # Sh vTP v Status

VTP domain : big domain , VTP mode : Server , Config revision = 1

how it will affect the Network

(6) which switch is the VTP server

on SwA _____

(1) # Sh int trunk ⇒ get the trunk ports & thier modes (ON/off)

or # Sh run ⇒ get all interfaces access & trunk

or # Sh cdp neighbors ⇒ ports that are connected to Router (R) or Switch (T S) will be trunk

ans : fa 0/4 , fa 0/5, fa 0/6

(2) # Sh cdp neighbors ⇒ to know ports that are connected to a Router

ans : fa 0/6

(3) assume scr MAC = 000C.5e16.2460

(i) If dst MAC is given use: # Sh ▾ mac ↵ (Port vs MAC)

ans: access port u get from mac table + trunk ports

(ii) If dst MAC is not given: see all ports that're member in u VLAN

Sh ▾ mac ↵ ⇒ scr mac (fa0/2) & Fa0/3 ⇒ member in VLAN 33

ans: fa 0/3 + trunk ports

(4) # Sh ▾ Span ↵ — Root ID → Address: 000C.1335.5676 (Root Sw)

Similar, A is not root ↵ — Bridge ID → Add.: 000C.1696.2345 (Sw A ID)

port fa 0/4 → cost = 19 & port fa 0/5 → cost = 57

→ fa 0/4 is directly connected to the root, then use # Sh ▾ cdp ▾ neighbors to know fa 0/4 is connected to which switch ans: switch B

(N.B: for fast Ethernet, the path cost = 19)

(5) on Sw A: # Sh ▾ VTP ▾ Status ↵

VTP domain = big domain ⇒ in the same domain of Sw X

revision no. = 2 > 1 (Sw X) ⇒ Sw A will affect the config. of Sw X

Sw X is server ⇒ may send updates

(6) on Sw A: # Sh ▾ VTP ▾ Status ↵

configuration last modified by 0.0.0.0 at 3-1-93 04:55:57

you're the VTP server ↵

⇒ our switch may have a management ip for telnetting ex: 192.168.1.1

to see it use: # Sh ▾ ip ▾ interface ▾ brief

& to see ips of u neighbors i.e Sw B & Sw D use

Sh ▾ cdp ▾ neighbors ▾ detail

Session (22)
12/06/06

Switching "cont'd"

⇒ In order to manage our switch, we should give it an ip, mask & default gateway.

⇒ we will imagine that we've a virtual interface, which we'll give it an ip & mask & assign it to certain VLAN.

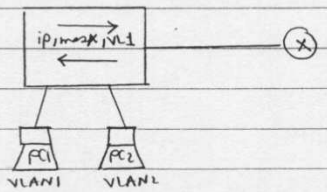
on the Switch

(config)# ip default-gateway ip of router interface
(config)# int VLAN 1
(config-if)# ip address ip mask
(config-if)# no shutdown

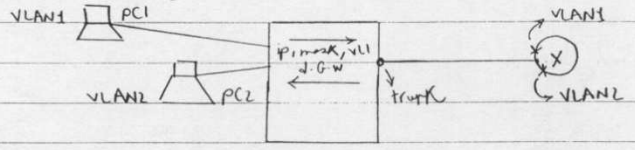
ip → from range of subnet of VLAN1

Consider this case

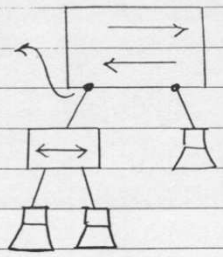
(i) If we assign our switch an ip, mask only ⇒ pc1 only can manage the switch



(ii) If we assign our switch an ip, mask & default gateway
⇒ PC1 & PC2 & any other PC can manage the Switch



Securing the switch access :



- The switch port by default is : no shutdown & no security
- The MAC Table (Ports vs MACs) is aged (يتم) every 5 min
- The port of the switch can accept up to 1024 MAC (using Hubs)

(1) Switch port security

(config) # int ▼ _____

(config-if) # Switchport ▼ port-security

↳ only 1 MAC can access the port but we didn't define it — there is aging

"OR"

(config) # int ▼ _____

(config-if) # Switchport ▼ port-security ▼ max ▼ {0-1024}

↳ now the interface of the switch can accept upto 1024 MAC, but uptill now we still didn't define these MACs

"OR"

(config) # int ▼ _____

(config-if) # Switchport ▼ port-security ▼ max ▼ {0-1024}

(config-if) # Switchport ▼ port-security ▼ mac ▼ mac add. 1

(config-if) # Switchport ▼ port-security ▼ mac ▼ mac add. 2

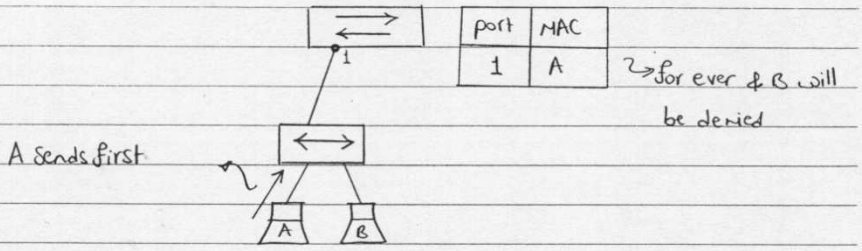
(config-if) # Switchport ▼ port-security ▼ mac ▼ mac add. 1024

} defining the MACs

(config) # int ▽ _____

(config-if) # switchport ▽ port-security ▽ mac ▽ sticky

↳ here the first device that will access the port, will be the only one that is permitted to access the port forever & no aging will occur for the MAC Table



↳ for ever & B will be denied

← لو حَبّة الـ port بتاعت الـ sw حتتعرف إزاى لو واحد بعت مه الغير مرغوب فيهم

⇒ by default the switch port will be shutdown

⇒ but we may change this feautre by configuration as follow

(config) # int ▽ _____

(config-if) # switchport ▽ port-security ▽ violation ▽ { shutdown (default) / restrict / protect }

- restric & protect will give the same action :

⇒ drop the violating user data only

---

(2) Form MAC Table manually

(config) # mac-address-Table ▽ static ▽

interface ▽ _____ ▽ mac ▽ _____ ▽ [vlan ▽ ___]

Router security

Access Control lists (ACL) قائمة الدخول

⇒ It is used to provide security so as not to let anyone see & ping a certain router "used in firewalls"

IP ACL : Is a group of statements that can permit or deny specific users from accessing the network

- The Access list will be assigned
  - number ✱
  - name (alphabetic)
  - alphanumeric (but 1st char must be a no.)
- Every interface on the Router will be assigned an ACL

ex:

ACL ✱7 or ACL "Ahmad"

Statements	
	permit 10.1.1.1
	deny 11.1.1.1
	permit 13.1.1.1

(V. Imp) : ACL deals with routed protocols i.e permits & denies data packets & not the updates.

(V. Imp) : If you want to permit/deny some one from accessing certain host that is connected to certain Router called R1, then the ACL should be created on R1 & can't be created on any other Router.

Configuration

(1) Create ACL : we've two types

Standard ACL — Extended ACL

⇒ we'll see the configuration of each type in details later

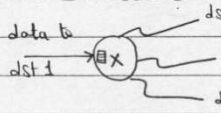
(2) Activate ACL on certain Interface

⇒ assume that we already created an ACL & we're going to assign the ACL to certain interface

(config)* int ▼ S0

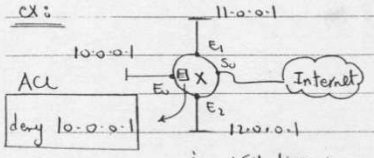
(config-if)* ip ▼ access-group ▼ ACL# or name ▼ {in / out}

in = in bound



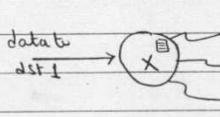
. in bound ACL is processed before RTG i.e the data must be checked when it comes to the interface & before it is routed.

ex :



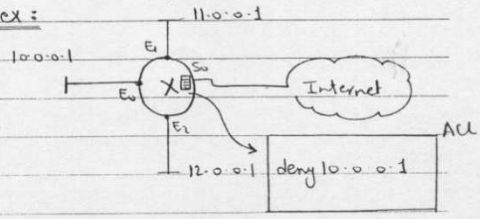
. معنى هذا الكلام أنه 10.0.0.1 مش حيقدر يـ access E0 ومش حيقدر يبعت لحد

out = out bound



. out bound ACL is processed after routing

ex :



. معنى هذا الكلام أنه 10.0.0.1 يقدر يبعت لـ 11.0.0.1 و 12.0.0.1 ومش مسموح له يكلم حد على S0

ACL processing

(1) ACL statements 're processed from up to down & Statements are placed in the ACL according to the order i wrote them in configuration

(2) Once a match is found, the router excutes the order (permit / deny) & exists the ACL & No further statements 're processed.

(3) If no match is found, the data will be denied coz at the end of the ACL there is an imaginary statement at the bottom of the ACL called "deny any". ← إللي متعرفش عنه حاجة ومش موجود في ال ACL وقعه

ex: If you've 10 PCs, 9 PCs are permitted & 1 PC is denied then you've 2 options to write the ACL

Option 1:

```
permit PC1
  :
permit PC9
deny any
```

→ PC10 will be denied automatically

Option 2:

```
deny PC10
permit any
```

→ (permit any) Cancell the order of "deny any" & so all PCs except PC10 will be permitted

(4) you can't insert a statement bet. statems, only @ the end

(5) for numbered ACL: deleting a certain statement will delete the full list

for named ACL: deleting a certain statement will not delete the full list

Types of IP ACL

(1) Standard IP ACL
- numbered ACL: 1 → 99 or 1300 → 1999
- named ACL: "any name"

(2) Extended IP ACL
- numbered ACL: 100 → 199 or 2000 → 2699
- named ACL: "any name"

max. no of Active ACL: no of interfaces * 2 (in, out) * no of routed protocols (ip, ipx, Appletalk)

(1) Standard ACL : It filters traffic based on source ip address in an incoming packet.

Configuration → to create the ACL

(i) numbered Standard ACL :

(config) # access-list [no. (1→99) unique to ip Standard ACL] { permit or deny } scr ip [scr w.c.m] (optional → default w.c.m if i don't put it is 0.0.0.0 i.e this scr ip specifically)

(ii) named Standard ACL :

(config) # ip access-list { standard / extended } ACL name

(config-std-nacl) # { permit / deny } scr ip [scr w.c.m]

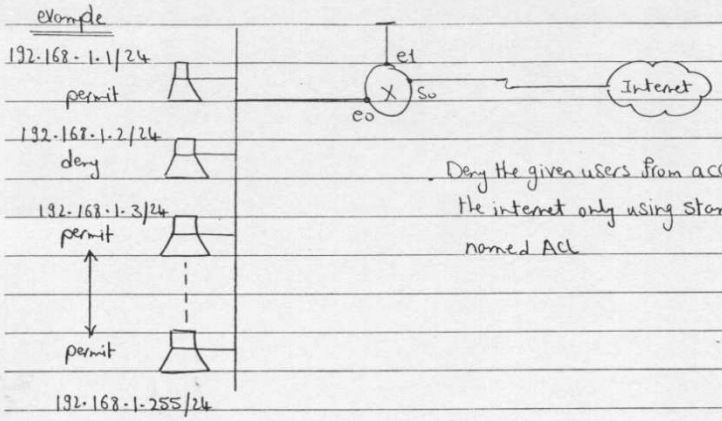
(config-std-nacl: Standard — named ACL)

(2) Activate ACL : assign certain ACL to certain port

(config) # int so

(config-if) # ip access-group no. or name { in / out }

example



Deny the given users from access to the internet only using standard named ACL

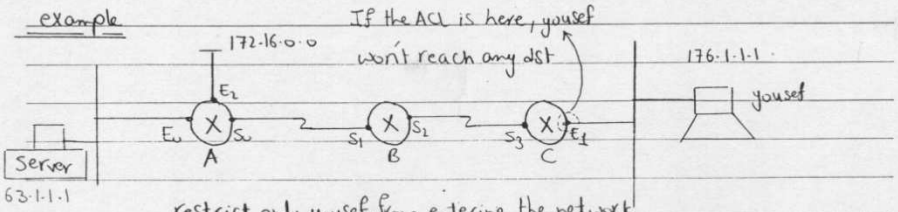
✗ (config)# access-list 1 permit 192.168.1.0 0.0.0.255
(config)# access-list 1 deny 192.168.1.2
→ This ans. is wrong cuz the router will never deny 192.168.1.2 after permitting the whole network in the 1st statement.

Sol^n:

(config)# access-list 1 deny 192.168.1.2
(config)# access-list 1 permit 192.168.1.0 0.0.0.255
(config)# int s0
(config-if)# ip access-group 1 out

} It is wrong to activate the ACL on e1 & e0 cuz these 2 interfaces won't be able to talk to each other

example



restrict only yousef from entering the network that contains the server 63.1.1.1 using standard named ACL

Soln : on Router A

A(config) # ip access-list standard yousef

A(config-std-nacl) # deny 176.1.1.1

A(config-std-nacl) # permit any ⇒ to remove the deny any command

= ip 0.0.0.0 0.0.0.0 255.255.255.255

A(config-std-nacl) # exit

A(config) # int e0

A(config-if) # ip access-group yousef out

N.B: (1) The Standard ACL should be placed as close as possible to the dst

*(2) If you write A(config-std-nacl) # no deny 176.1.1.1 in order to remove the statement from the ACL, then the entire ACL will not be deleted.

---

(2) Extended ACL

It filters traffic based on :

1- Scr ip address & dst ip address

2- TCP/IP protocol (filter based on IP, UDP, TCP, ICMP, ...)

3- protocol information(deny certain applications & permit others i.e deny HTTP& permit Telnetting)

Configuration

(1) Numbered Extended ACL :

(config) # access-list 100 → 199 { permit or deny } protocol (TCP, UDP, IP) scr ip scr w.c.m (ex: 10.1.1.1 0.0.0.0 or host 10.1.1.1)

[operator scr port protocol] dst ip dst w.c.m [operator dst port protoc (80 or HTTP or WWW)]

equal ≡ eq

less than ≡ Lt

greater than ≡ gt

range

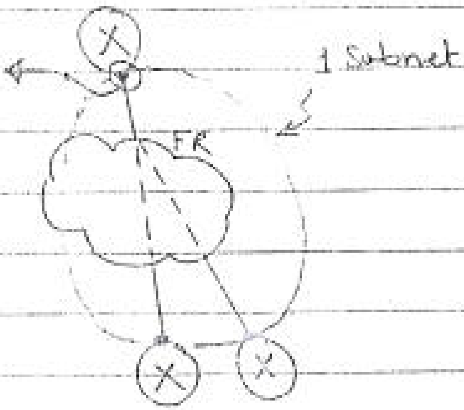
ex : eq 80, eq HTTP, range 80-90

Case in Class: To reserve ip's but it doesn't solve the split horizon problem use:

(1) point-to-point subinterface

(2) point-to-multipoint subinterface (✓)

- Configure this interface as pt → multipoint only to reserve ips



FR congestion management

Cisco LAPF & itef LAPF Frame is as follow

← Control →

Flag	DLCI	DE	FECN	BECN	Type	Data	CRC	Flag

DE: قابلية ال رمى ل ⇐ Discard Elligibility
frame ال discard
as DE↑ ∴ discard elligibility ↑

BECN → Backword Explicit Congestion notification

FECN → Forword Explicit congestion notification

we've 2 definitions

CIR (Committed Information Rate): ال rate اللي ال SP ملتزم بيه
↳ guaranteed B.W ex: 512 Kbps

EIR (Excessive Inf. Rate): extra rate/B.W given in Case of non-congestion
ex: 128 Kbps.

Sol^n :

C(config)# access-list ▿ 100 ▿ deny ▿ TCP ▿ host ▿ 57.1.1.1 ▿ host ▿ 63.1.1.1 ▿ eq ▿ → Telnet port r

مش حنكتب scr port no لأنه بيكون random ومش معروف

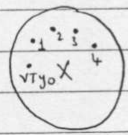
C(config)# access-list ▿ 100 ▿ permit ▿ any ▿ any

any → any scr (0.0.0.0 ip, 255.255.255.255 mask) ; any → any dst

C(config)# int ▿ E1

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

⇒ How to restric Telnetting using Standard ACL → by the means of VTy lines — do you remember them?



ex: deny 192.168.1.1 only from Telnet on R1 & permit 192.168.1.2

(config)# access-list ▿ 1 ▿ permit ▿ 192.168.1.2

(config)# access-list ▿ 1 ▿ deny ▿ 192.168.1.1

(config)# line ▿ vty ▿ 0 ▿ 4

(config-line)# access-class ▿ ACL no. (1) ▿ in

access-class → to activate ACL on lines → care in exam & not access-group

Trouble Shooting

\# Sh ▿ ip ▿ access-list → to Show ACLs of IP protocol

\# Sh ▿ ip ▿ access-list ▿ ACL # or name → to Show Certain ACL

} trouble-shoot ACL Creation

\# Sh ▿ access-list → to Show ACLs of all routed protocols (IP, IPX, ...)

{# Sh ▿ ip ▿ interface ⇒ displays which ACLs are activated on which interfaces & thier directions (in/out)

→ trouble shoot ACL activation

⇒ On the Router : to make VLAN1 talk to VLAN2 we'd use RTG

(config) # int fa 0/0

(config-if) # no ip address

(config-if) # no shutdown

(config) # int fa 0/0.1

(config-subif) # ip address 10.0.0.1 255.255.255.0

(config-subif) # encapsulation dot1q 1 → VLAN1

(config-subif) # int fa 0/0.2

(config-subif) # ip address 11.0.0.1 255.255.255.0

(config-subif) # encapsulation dot1q 2 → VLAN2

(ConFig) # VLan 2 name Anyname.

↳ do For One Switch Only. (Switch A) Only...

Then. #Sh VLAN

⟸ تجد أنه الـ updates تغيرت ;-) ...

3 Now we Need to assign Switch Port to VLan

Switch A

(ConFig) # int Fo1

(ConFig-if) # Switch Port mode access ← By default in Vlan 1 native.

(ConFig) # int Fo12

(ConFig-if) # SwitchPort mode access.

(ConFig-if) # SwitchPort access VLan 2. ⟸ هذا بسط معكم لأنها VLan2 غير VLan1 وليس

#Show VLan.

Switch B

(ConFig) # int Fo1

(ConFig-if) # Switch Port mode access ← By default in VLAN 1 (native).

#Sh. VLan

E-Station ⟹ Ping 10.0.0.3 ✓ ok. ← Because they have the Same VLan.

~~Vlan 1~~

All Switches are in the Same VTP domain.

Two Conditions For VTP

1) (ConFig)# VTP domain domain Name

* Repeat For the other Switches with the Same domain Name

To check

#Sh VTP Status

2) All Switches are Connected together Using Trunk Port "work with all VLans". (TrunKing).

Betn 2Switches Betn Switch & Router.

Switch A (has One Trunk Port)

(ConFig)# int f0/2

(ConFig-if) # SwitchPort mode TrunK

Switch B (has two TrunK Ports)

(ConFig)# int F0/2

(ConFig-if) #SwitchPort mode TrunK.

(ConFig) # int F0/1

(ConFig-if)# SwitchPort mode trunK.

one

FoR
Any Router do the Followings

1- (ConFig)# hostname anyname.

2- (ConFig)# int S0/e0 ---

(ConFig-if)# iP address iP Mask

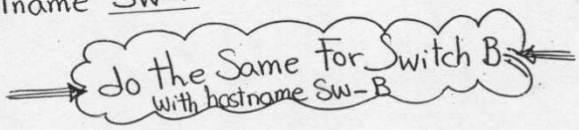
3- Routing Protocols ⇒ to add deFault gateway.
through Routing protocols.
dynamic, Static
Rip, OSPF, EIGRP, Static deFault.

Switch A

>enable

#ConFt

(ConFig)# hostname SW-A



#Sh VLan

1 We have to Create VLAN
2 Name VLAN (Optional)
3 assign Switch Port to VLAN.

Steps.
very long
we May use VTP

Eng. Ahmed Nabil

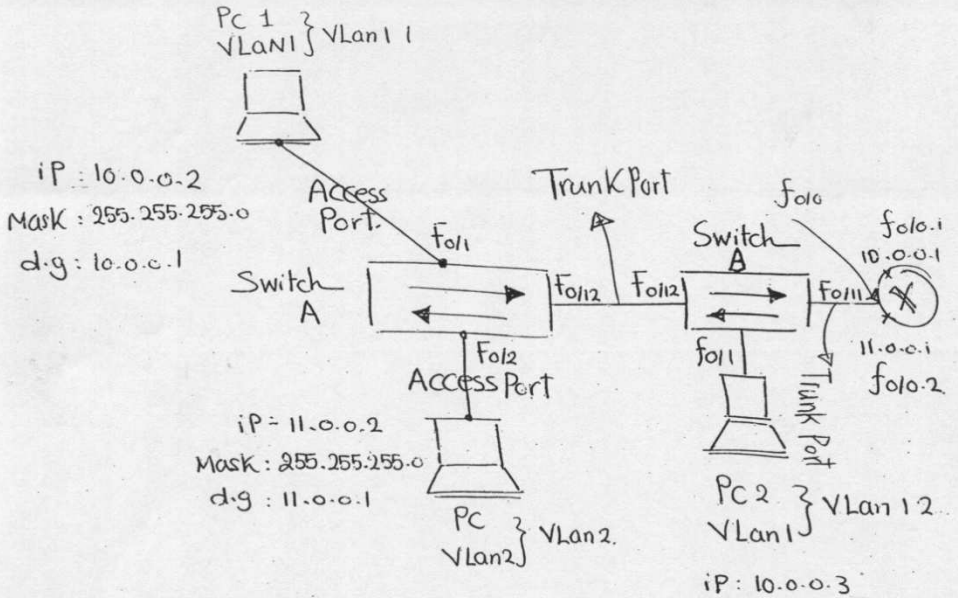
Lab. 3

1

12 - 8 - 2006

Saturday.

new Simulations
updated in pass4Sure V2.6
(lab 3 "cont'd")



⇒ Any Pc ≡ DTE Needs :-

1_ IP
2_ Mask
3_ default gate way.

e-Station ▶

VLAN 1
VLAN 2
VLAN 1 2

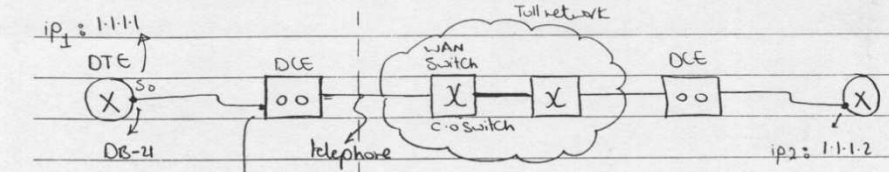
C:> Win iPCFg

then add IP, Mask, d.g
as Shown up...

repeat for all LANs in estation.

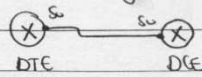
Session (24)
13/06/06

WANs Introduction Layer 2 (L2) In WANs



N.B :- (1) In LANs every thing is auto Synchronized & So we don't need any DCE devices for Synchronization

(2) In LAB we use no DCE devices but instead we connect 2 Routers back to back & configure one of them as a DCE devices



(201)

- WAN technologies :- a hop-to-hop technology
  i.e how we will transfere data from one DTE device to another DTE device

← كل المرسوم بين R1 & R2 هوه عباره عن سلكة ذ L3 , عشان كده
ip1&ip2 هما ذ نفس ال subnet

كل المرسوم يعتبر سلكة ذ L3

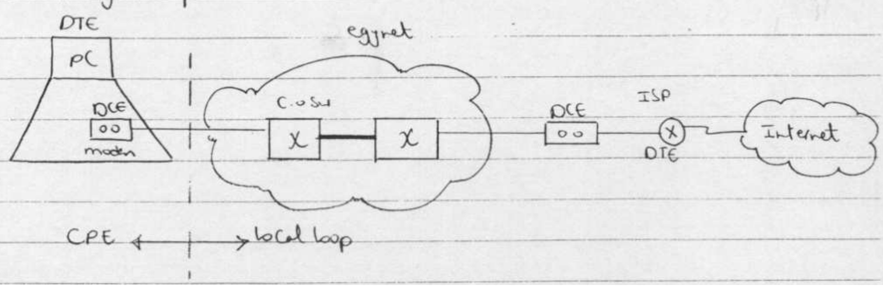
- All WAN technologies work in L1 (physical) & L2 (Data link layer) of OSI
  i.e Network Interface layer (TCP/IP)

- DTE (Data terminal Equipment) : src & dst of information & data.
  DCE (Data control Equipment) : used to adjust clking & synchronization.
  CPE = DTE + DCE (The equipments @ the customer side)

- local loop ⇒ It is the system of Cables that is connected bet.
  (كابينة التليفون) the telephone box @ your home & the central office
  Switch (السنترال)

- The C.O Switches of the service provider (carrier company) forms what is called the Toll network ex: Telecom Egypt

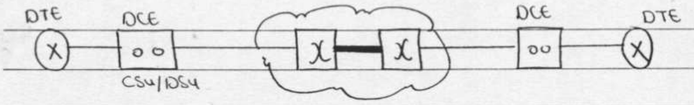
ex: Analog dial up



WAN Connections : how to DTE devices (Router ↔ Router) can be connected
« L2 technologies » to each other on the WAN

(1) Dedicated Circuit Switching

- There is a physical cable from L3 hop to L3 hop & all traffic will pass on the same physical cable which is available all time (24 hours / 7 days) with guaranteed B.W.

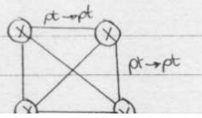


CSU (Channelization Service unit)
DSU (Data service unit)

* example on technology : leased line
* example on protocols (L2 protocols) : HDLC (High level Data link control protocol)
ال protocols اللي ال leased line tech. بتشتغل بيه ⇙ PPP (Point-to-point protocol)

⇐ المصرية للاتصالات بتوفر لل Customer اللي دائماً بيكون شركة ضخمة بتوفر له physical cable شغال طول الوقت ممكن يتم توصيله أو الحفر له من جديد لو مكنش هناك spare cables لربط المنطقتين.

Adv. : High speed up to 45 Mbps
Disadv. : (1) high cost
(2) Support only point → point
ex : to connect 4 Routers we need



(2) On demand Circuit Switching

- Dial up technologies that can request a circuit (cable) to send traffic unit for a certain period of time.

← يعني لا تشغل الخزنة لأنه هناك leased line بينك وبين اللي انت عايز تكلمه

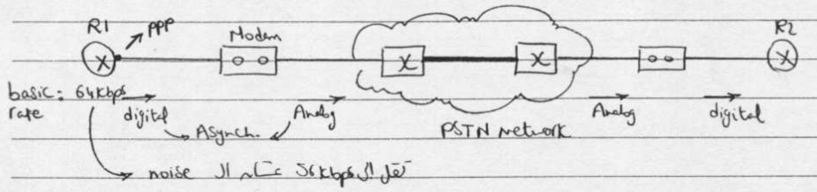
i.e : leased line for a period of time زي مكالمة التليفون.

- If you dial the same dst 2 times, then each time your data will transfere on different wire.

- examples on technologies : (1) PSTN (Public Switched telephone Network) "Analog dialup"
(2) ISDN (Integrated services digital Network) "Digital dialup"

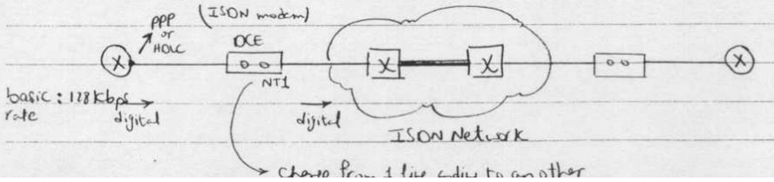
examples on protocols used by these technologys : (1) HDLC only with ISDN
(2) ppp with both PSTN & ISDN

- PSTN ⟹ Analog dial up i.e the core switches predict analog input



If analog transmission exist this means that we've Asynchronous T^X
ppp supports both Asynch. & Synch. T^X , but HDLC supports Synch. T^X

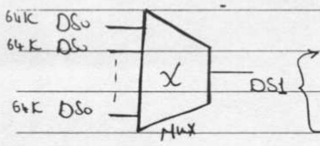
- ISDN ⟹ Digital dial up i.e the core switches predict digital input



Speeds available

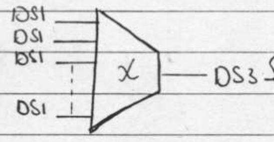
- Analog dial up → 56 Kbps (coz of noise) ≡ ideally
- digital dial up → for a digital voice we need at least 64 Kbps

∴ the least Channel DS_0 = 64 Kbps



T1 (USA) = 24 DS_0 ≡ 1.54 Mbps

E1 (Europe & Egypt) = 32 DS_0 ≡ 2.04 Mbps



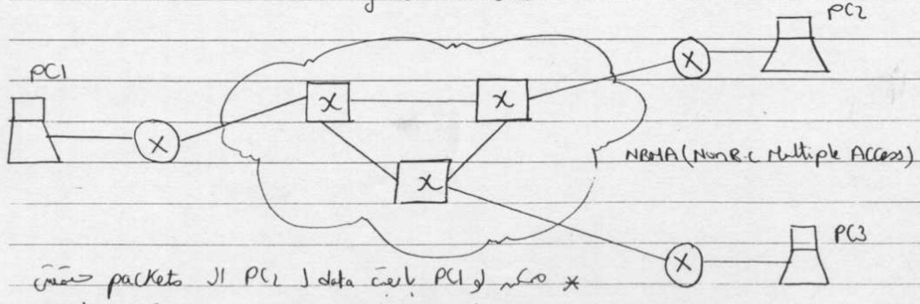
T3 ≡ 45 Mbps

E3 ≡ 34 Mbps

« Standards »

(3) packet switching = . It is a technology that can support point-to multipoint connections using the concept of virtual circuit (VC)

. here we buy from the service provider a guaranteed B.W



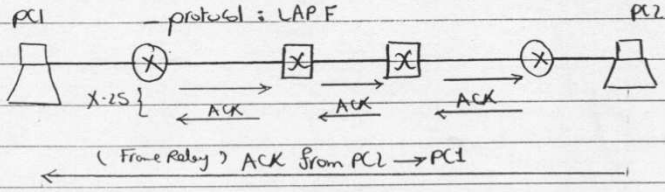
* ممكن لو PC1 بابعت data لـ PC2 ال packets حتمشي في كذا طريق ولو طريق وقع ال pcks حتمشي في طريق تاني

* ممكن PC1 تبعت لـ PC2 & PC3 (multi destinations)

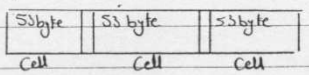
examples on technologies work with pck switching & protocols used by these technologies

(1) X.25 : - Synchronous tech.
- speed 48 Kbps
- low speed for error detection & correction & reliability supported (ACK) each hop on L2
- very much over head
- protocol : LAPB (Link Access procedure Balanced)

(2) Frame Relay : - Synchronous tech.
- speed 45 Mbps
- error detection & correction & reliability is supported only from PC → PC & not from hop to hop
i.e depends on TCP for error correction & Reliability
- protocol : LAPF



(3) ATM (Asynchronous transfere Mode) :
- Asynchronous tech. i.e doesn't transwitt @ fixed clk times
- speed (155 Mbps → 40 Gbps)
- Any pck is divided into small cells of fixed size, each cell = 53byte & so ATM is called Cell Switching tech.
each cell will choose a path to go throgh to the dst.

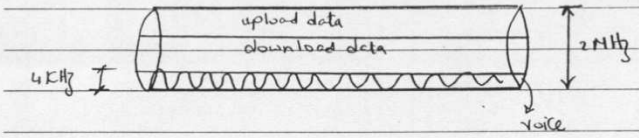


- protocol : ATM

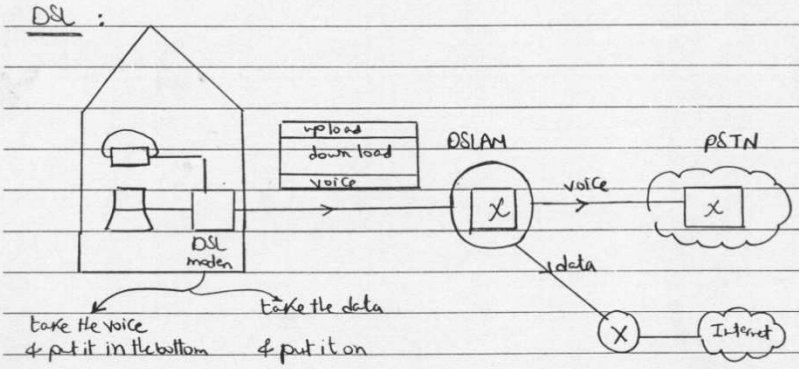
(4) Broadband Technologies

* DSL * Cable TV * Satellite

⇒ our cable can bear up to 2MHz, for voice we use only 4 KHz, so we may make use of the rest of the cable to TX data



DSL :



- DSL is a layer 1 technology
- Should work with all2 protocols PPPoA / PPPoE

Let's Study the L2 protocols that work with circuit & on demand circuit Switching i.e HDLC & PPP

(1) ISO HDLC (not Supported by Cisco) : ISO Invented it

flag	Address	control	Data	CRC	flag
0111 1110 preamble	1111 1111		packet (IP/IPX)		

Address → for nonexisting as we work pt→pt

"ISO HDLC frame"

flag → like the trailer used to Separate bet. frames

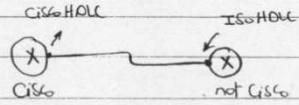
disadv. :- contains no field for the type of the upper layer protocol

(2) Cisco HDLC : Default on Cisco Serial interfaces
"Cisco properiatory"

flag						
preamble	Address	control	type	Data	CRC	flag

"Cisco HDLC frame"

disadv. :- works only with Cisco Routers



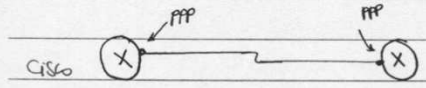
up → L1

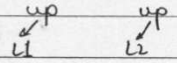
administratively down → L2 is down due to encapsulation mismatch

PPP (Point-to-point) : open Standard Can be used by Any Router

Flag	Address	control	Type	Data	CRC	Flag

PPP Frame





⇒ To configure an interface to work with certain protocol

N.B : by default any Serial interface works HDLC

(config) # int ▼ S0

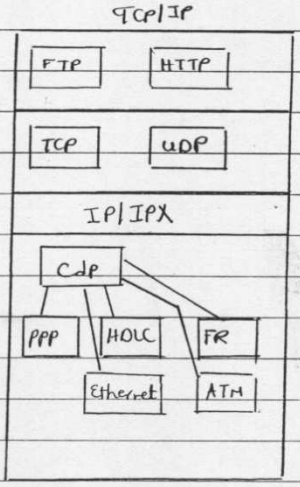
(config-if) # encapsulation ▼ ppp

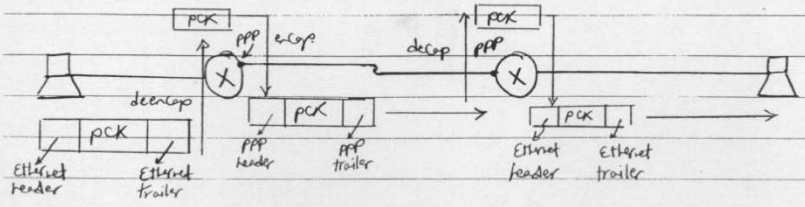
then to make this interface work with HDLC use

(config-if) # no ▼ encapsulation ▼ ppp

or

(config-if) # encapsulation ▼ HDLC





PPP Components : PPP Can be considered no. of protocols work together

(1) **LCP** : "link Control protocol"

It negotiates
- * link establishment → open session
- * link management (options & testing)
- * link termination

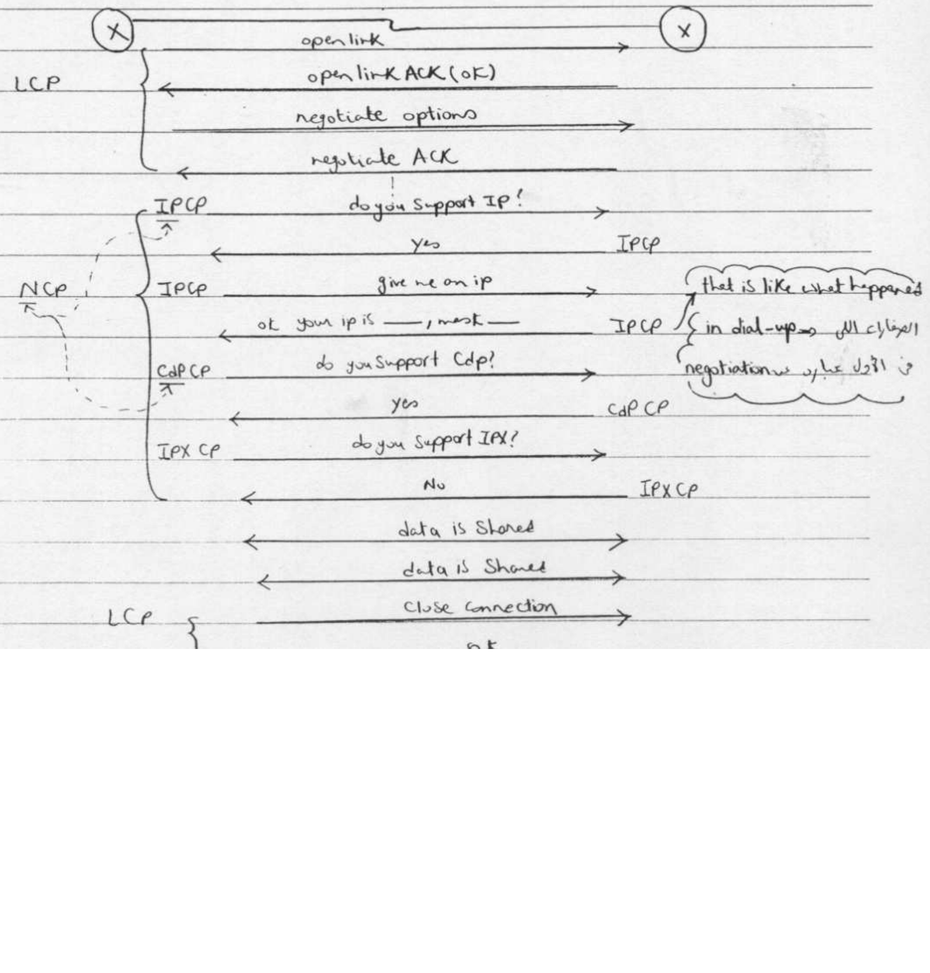
(2) **NCP** : "Network control protocol"

– negotiates the upper layer protocol to be sent on that link

← ال 2 Routers حيتفقوا ماهو نوع ال pckts اللى سيتم ارسالها ← IP, IPX

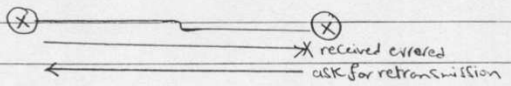
(3) **ppp frame format** : used for hop-to-hop data delivery

PPP operation : * debug ppp negotiation



ppp options In LCP negotiation

(1) error correction ⇒ ask for retransmission if the PCK is received error

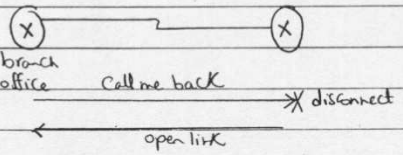


(2) Compression

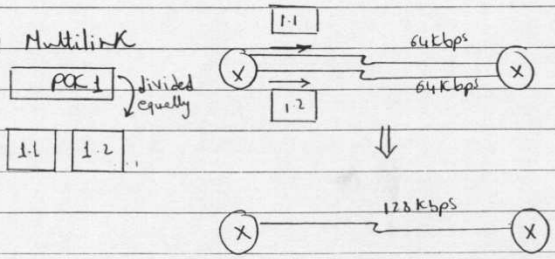
The 2 Routers will negotiate weather to T^x & R^x compressed data or not

(3) Call back ⇒ the branch office will give the center office a ring only & the center office will open the link i.e the center office will pay

(useful for security + money)



(4) Multilink



AS if we increased the B.W

(5) <u>Authentication</u> : put a username & password before accessing the network

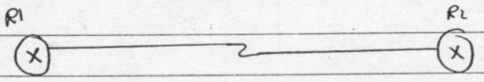
← زي الإشتراك المجاني, بابه كله لازم username & password

(5.1) PAP (5.2) CHAP

<u>Configuration</u> : (config-if) # ppp authentication {chap/pap}

<u>N.B:</u> All these options 're not working by default but only activated by configuration, in CCNA we know only the config. of the Authentication.

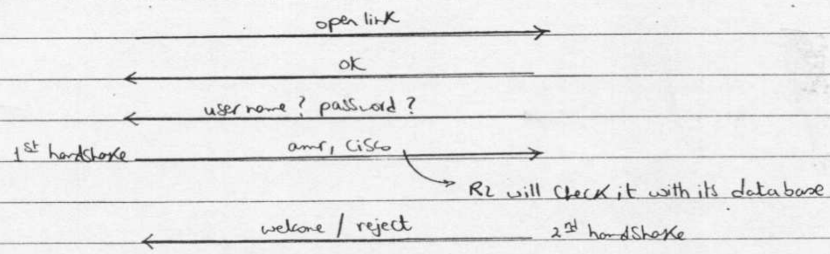
(5.1) <u>PAP (PPP Authentication Protocol)</u> "2-way handshake"



R2 database

username	password
Amr	Cisco

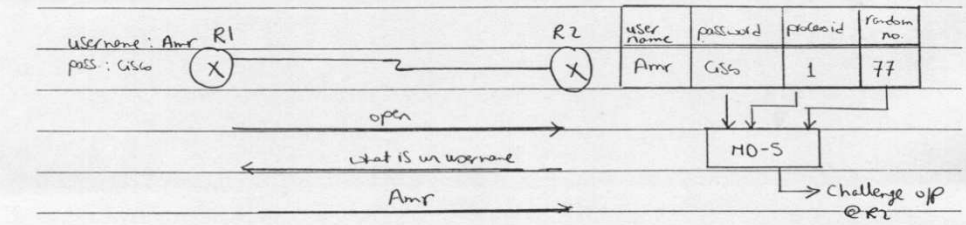
on R1 : (config) # username <u>amr</u> password <u>Cisco</u>



<u>disadv.</u> : the password is sent in clear text & can be easily hacked

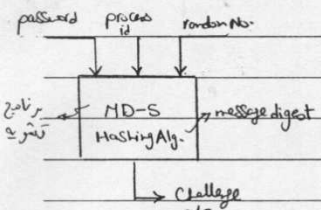
(5.1) CHAP (Challenge Handshake Authentication Protocol)

" 3 way handshake "



R1 will take these inf. ← Challenge (process id = 1 & random no. = 77) 1st handshake

& apply a certain Algorithm on them as follows



2nd handshake — Challenge o/p → R2 will compare this with the previous Calculated Challenge o/p

3rd handshake ← welcome / reject

N.B :- to get the right Challenge o/p we should know 3 inf.

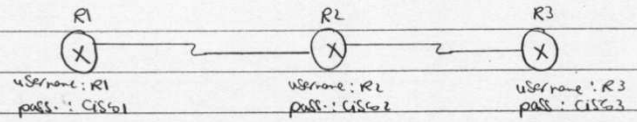
pass. processid random no.

let's summarize the configurations

(config) * int ▼ S0
(config-if) * encapsulation ▼ ppp
(config-if) * ppp ▼ authentication ▼ { chap / papf

To put a username & password on the Router use
(config) * username ▼ username ▼ password ▼ password

ex :



⇐ لازم كل Router يعرف الـ password بتاعت الناس الـ جنبه

on R1
(config) * hostname ▼ R1
(config) * username ▼ R2 ▼ password ▼ Cisco2

on R2
(config) * hostname ▼ R2
(config) * username ▼ R1 ▼ password ▼ cisco1
(config) * username ▼ R3 ▼ password ▼ cisco3

on R3
(config) * hostname ▼ R3
(config) * username ▼ R2 ▼ password ▼ cisco2

Trouble Shooting on L2

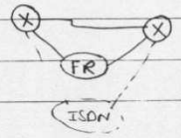
* Sh ▼ ip ▼ int ▼ brief

Session (25)
15/06/04

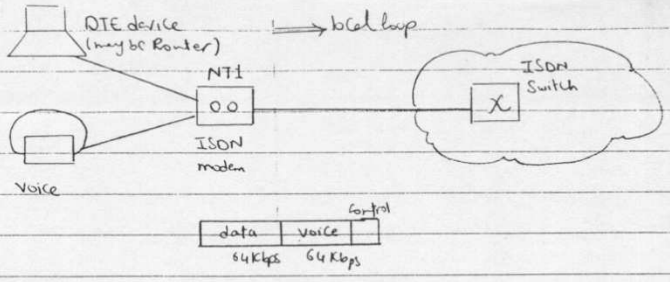
WANS
- Circuit Switching
  - Dedicated
    - tech. : leased line
    - protocols: HDLC & ppp ✓ (last lecture)
  - on Demand
    - tech. : PSTN – ISDN (this lecture)
    - protocols: HDLC & ppp
- packet Switching (virtual ct.)
  - tech.
    - FR its protocol ⇒ LAPF (next lecture)
    - ATM its protocol ⇒ ATM
    - Broadband ex : DSL, Cable Tv, Satellites
    - X.25 its protocol ⇒ LAPB

ISDN (Integrated services digital networks)

- It is a pure digital on demand Circuit Switching
  i.e if you close the connection & open it another time you may transmitt on different cable
- For large companies, ISDN is used as a backup technology for main technologies like leased line & FR
  ⇒ ISDN works only when leased line is down for only small time & so it is more cheaper



  ⇒ for small companies (in an home) ISDN may be used as the main tech.
- ISDN depends on TDM (Time Division Multiplixing)
- It supports voice, video & data



Types of ISDN

(1) BRI (Basic Rate Interface)

2B (Bearer Channel)
- Channel that carry voice, data or video
- 2 Channels each 64Kbps
- protocol that is responsible to T^{x} the data hop-to-hop is PPP/HDLC

1D (Delta) 16Kbps
- Carry control/signaling information like setup & tear down
- 1 CH 16Kbps
- protocol that is responsible to T^{x} control information is LAPD (Link Access procedure for D channel)

$BRI = 2*B + 1*D = 2*64 + 1*16 = 144\ Kbps$

D	B1	B2	D	B1	B2	D	- - -

(2) PRI ISDN (Primary Rate Interface) ⇒ used by large companies

PRI (E1)
30B + 1D
64 Kbps, 64 Kbps

PRI (T1)
23B + 1D
64 Kbps, 64 Kbps

PRI (E1) Rate = 31 * 64K
≅ 2 Mbps

PRI (T1) Rate = 24 * 64K
= 1.5 Mbps

ISDN protocols:

Signaling & control msg → Q.931

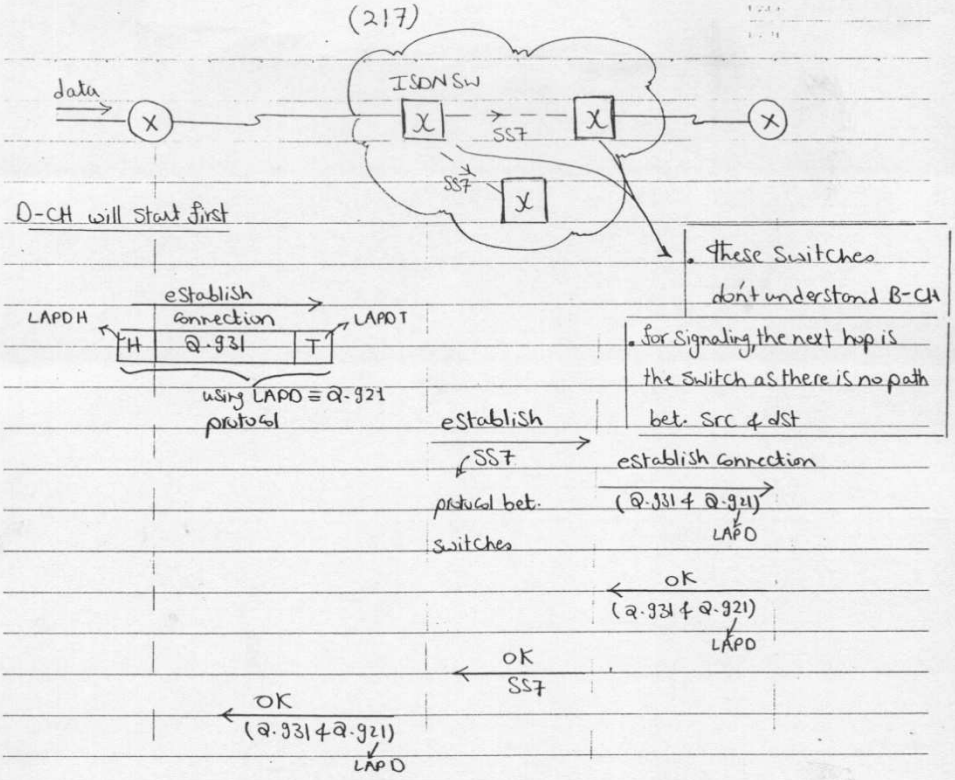
Encapsulate the Q.931 msg which is the upper layer protocol for D-Channel

ITU → I-Series
→ Q-Series

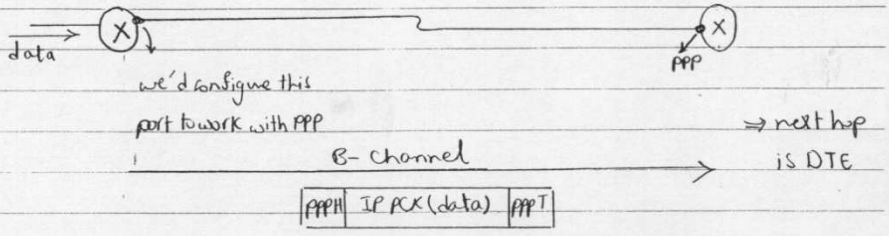
	D-Channel	B-Channel	OSI
	Q.931 (→ L3)	IP, IPX, Apple talk	L3
	Q.921 (LAPD) (→ L2)	ppp or HDLC	L2 (PPP H | IP | PPP T)
	I-Series		L1

ISDN operation:

- At first the D-Channel begins & the protocols that work with the D-CH is Q.931 (L3) & LAPD (L2) that share signaling & control information with the ISDN switch & up till now there is no path bet. scr & dst
- When a connection is established, B-CH will start working using for example IP (L3) & PPP (L2) that help sharing data bet. scr & dst.



Now a connection is established & as if we operate Circuit switching, now B-channel will work to carry data information using for example IP(L3) & PPP(L2) protocols



PAGE
DATE

- SS7 is the protocol that is used between ISDN switches. It specifies which dst phone no. corresponds to which interface i.e every switch keeps a table of dst phone numbers & the interface on this switch in order to reach this dst, so it is somehow similary to the routing protocols between routers

- SS7 stands for System Signaling number 7

switch port	Tel. no.

- ISDN is a technology used some protocols to know how a router will establish a connection to talk to another router

- ISDN basic speed is 128 Kbps

ISDN Configuration

⇒ All what we want to do is to configure our Routers to deal with a System of ISDN Switches.

(1) Define ISDN Switch:

(config) * ISDN ▼ Switch-type ▼ Switch type
ex: Basic-5ESS

- the Router has a database of many ISDN Switches but you should tell him what is the type of the Switch that you're going to deal with
- this configuration will be for all serial/BRI Interfaces exist on the Router

"OR"

(config) * int ▼ S0/BRI0 ? → depend on the interface
(config-if) * isdn ▼ switch-type ▼ switch type

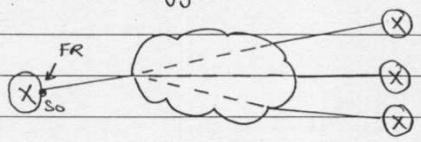
- this method of configuration is used if each interface is connected to a different type of Switches.

Some Switch types: Basic-5ess vendor → AT&T
Basic-ni1 vendor → national
Basic-dms100 vendor → Nortel

Session (26)
18/06/06

Frame Relay (FR) ~> like X.25 & ATM but with some differences

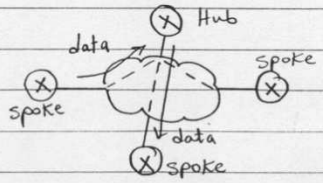
- It is a packet switching technology
- It depends on the concept of virtual circuit (VC)
  - PVC (permenant VC)
    - Simulates the leased line 24h/7days
  - SVC (Switched VC)
    - Simulates the on demand Circuit Switching
    - not commonly used
- It is considered a NBMA technology
  ⇒ to send B-C msg we'll Send replicate unicast



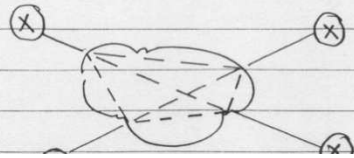
- FR has many topologies

pt-to-pt

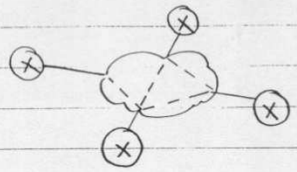
Hub & spoke (star)
- all data is directed to a central Router & it will direct the data to the proper dst
- commonly used



Full mesh
- very high cost



partial mesh
- not full mesh



FR Encapsulation

- FR uses LAPF (Link Access procedure for FR) encapsulation
  N.B : X.25 uses → LAPB & ATM uses → ATM

- LAPF Frame is as follow

Flag 0111 1110	Address DLCI	control	Data	CRC	Flag 0111 1110

DLCI ≡ Data Link circuit Identifier

⇒ LAPF is not used now because it has no "type" field to show the type of encapsulated data (IP, IPX, ---)

. to notify the end of frame, i.e no idle time as in Ethernet.

- Improvements

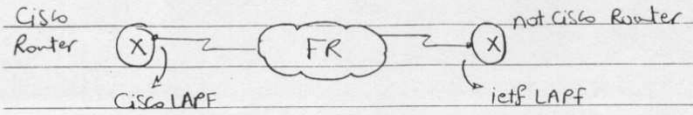
↓ Cisco LAPF
(for Cisco Routers only)

↓ ietf LAPF
(for Cisco & non Cisco Routers)

Flag	Address DLCI	control	Type	Data	CRC	Flag

Type → IP, IPX, Cdp, ---

→ Cisco LAPF & ietf LAPF are not compatible to each other

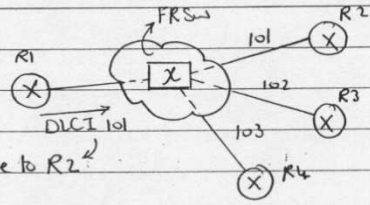


⇒ L2 is administratively down
encapsulation mismatch

⇒ L2 is up

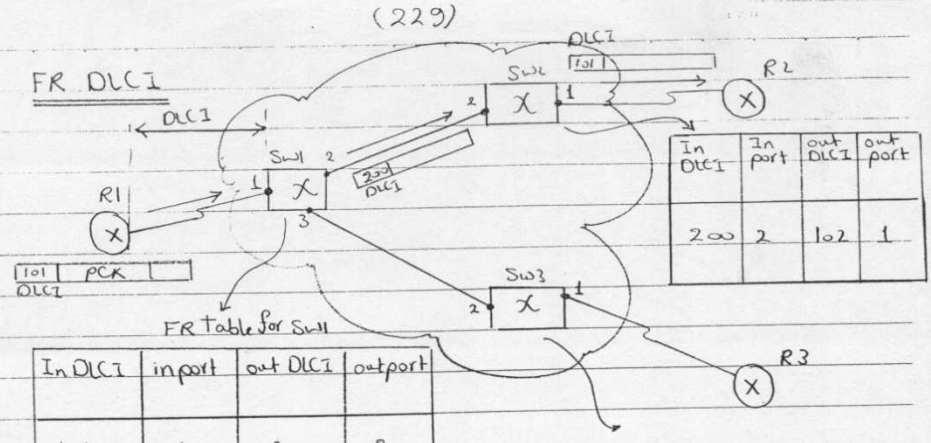
DLCI (Data link Circuit Identifier)

. It is the virtual circuit ID → عنوان السلكة التخيلية . اللي إنا عايز الـ FR يوصلني عليها



. FR → DLCI but ATM → VPI & VCI (virtual circuit Identifier)
↓
virtual path Identifier

FR DLCI



In DLCI	In port	Out DLCI	Out port
200	2	102	1

In DLCI	in port	out DLCI	out port
101	1	200	2
102	1	300	3
200	2	101	1
300	3	102	1

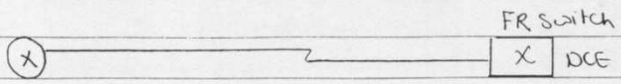
In DLCI	In port	out DLCI	out port
300	2	102	1

FR Table for Sw3

→ It means that: if data enters port 1 with DLCI 101, it goes out from port 2 with DLCI 200

- The FR tables are constructed by vendors like Alcatel, AT&T
- DLCI is full local between the Router & the FR Switch
- R1 can be connected to upto 1024 sites (0 → 1023) i.e the Router Serial physical interface can learn up to 1024 DLCIs
- But how R1 will know about the DLCIs ?
  ⇒ this is using LMI (Local Management/Signaling Interface)

LMI

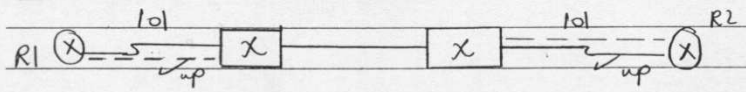


every 10sec — LMI inquiry msg
What is my DLCIs & what're there status (up/down)

LMI reply
you have DLCI 101, active
" " " 102, in active
" " " 103, deleted

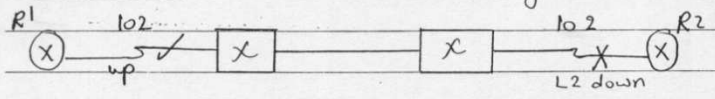
see using
debug ▽ Frame-relay ▽ LMI
Sh ▽ Frame-relay ▽ PVC

101 active : 2 sides are active

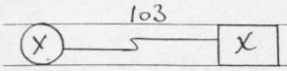


AS if R1 & R2 are connected to each other

102 in active : remote end failed but my side is active



103 deleted :



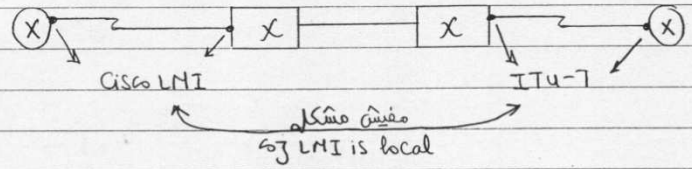
↳ DLCI 103 doesn't exist in the FR table

LMI types :

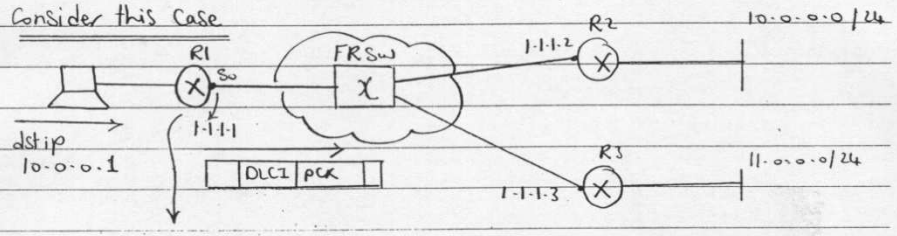
(1) Cisco LMI
(2) ITU-T (Q.933a)
(3) ANSI (Annex-D)

} The Router will work with the LMI type supported by the FR Switch

ex :



Consider this case



FR Map for R1

next hop ip	DLCI
1.1.1.2	101
1.1.1.3	102

RTG Table of R1

Network	o/p interf.	next hop ip
10.0.0.0/24	S0	1.1.1.2
11.0.0.0/24	S0	1.1.1.3

* Sh frome-relay map

← الـ FR Switch مبيعرفش غير DLCI ، عن طريق الـ Router الـ RTG Table
يشوف الـ next hop ip وعن طريق الـ FR Map يشوف هذا الـ ip
الـ DLCI المقابل له وبعت هذا الـ DLCI للـ FR Sw
← R1 يقدر يعرف كل الـ DLCIs اللي عنده عن طريق LMI ولكنه يعرف منين
أن 1.1.1.2 الـ DLCI تابعة هو 101 ؟؟ ← هنالك طريقتان

In order to form the FR Table we've 2 methods

- Static
- Dynamic (IARP) → Inverse

- IARP: is a protocol used to know the unKnown ip for known DLCI (from LMI)
- The SCR will send a B.C msg & only the dst will reply with his ip

(B.C ≡ replicate unicast)

FR Configuration

(config) # int s0

(config_if) # encapsulation frame-relay [cisco/ietf] (default / optional)

(config_if) # frame-relay lmi-type {cisco/ansi/q933a} (according to FR Switch)

- this command may be not written on Cisco routers coz there is automic lmi type detection (see later)

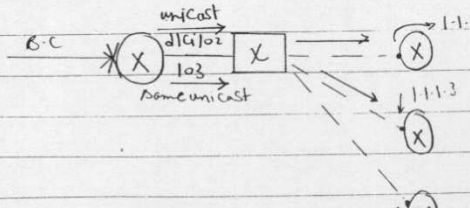
(config-if) # frame-relay map ip nexthop ip local dlci [Broadcast] (By default)

(i) Static method to control the B.C

ex: (config-if) # frame-relay map ip 1.1.1.2 102 broadcast | By default any FR interface doesn't FWD B.C

(config-if) # frame-relay map ip 1.1.1.3 103 broadcast

(config-if) # frame-relay map ip 1.1.1.4 104

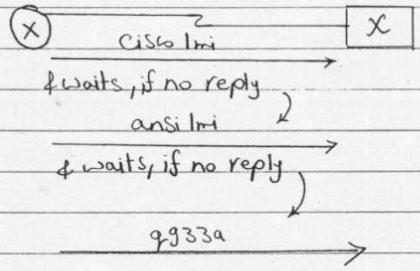


(ii) dynamic method using IARP to form FR Map, but in this case we can't control the B.C i.e the replicate unicast msg will reach all routers in the FR Network
(B.C is supported by all DLCIs)

- on Routers, IARP is used by default & is deactivated only if we configure the static way

---

- on Cisco Routers there is Automatic LMI type detection?



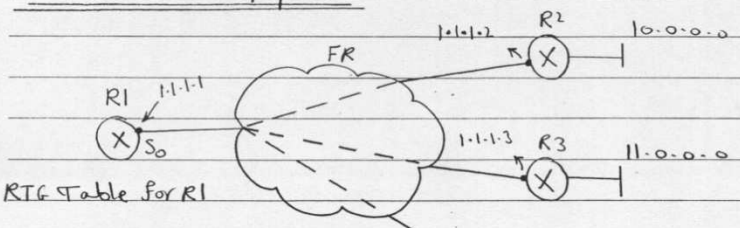
Trouble Shooting Summary

* Sh▼ int → Show the Status of the interface
* Sh▼ frame-relay ▼ PVC → Show the Status of VCs (active, inactive, deleted)
* Sh▼ frame-relay ▼ map → Shows the FR map (DLCI vs next hop ip)
* debug ▼ frame-relay ▼ lmi → debugs the lmi requests & replies to the router

---

FR problems with Routing -

In case of Hub & Spoke



RTG Table for R1

Network	port	next hop
10.0.0.0	S0	1.1.1.2
11.0.0.0	S0	1.1.1.3
12.0.0.0	S0	1.1.1.4

FR - map

⇒ Split horizon will cause a problem, why?
Any update sent from R2, R3, R4 to S0, will not be sent again from S0 i.e R2, R3 & R4 will no nothing about each other

Solution

(1) use Static Routing (default route & static route)

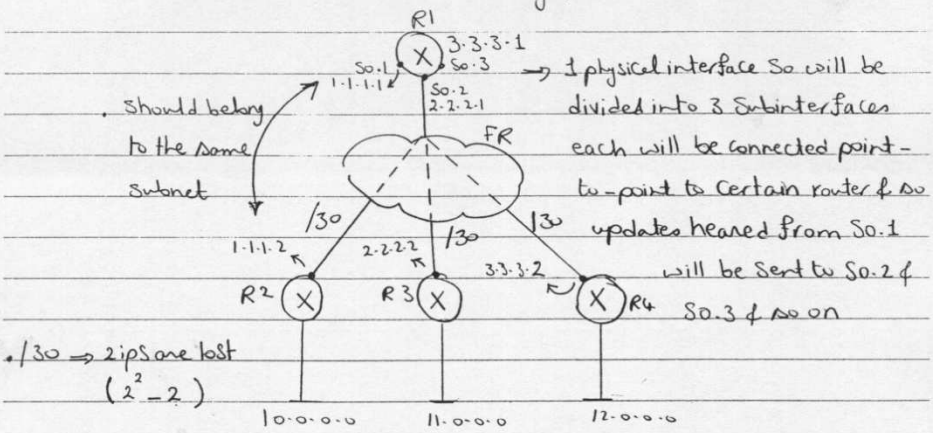
(2) Disable the split horizon feature
(config-if) # no ip split-horizon

(3) use Full mesh FR topology

(4) Configure point_to_point Subinterface

→ adv. : Solve the split horizon problem

→ disadv. : will consume many ips



- Should belong to the same subnet

→ 1 physical interface S0 will be divided into 3 subinterfaces each will be connected point-to-point to certain router & so updates heared from S0.1 will be sent to S0.2 & S0.3 & so on

- /30 ⇒ 2 ips are lost ($2^2 - 2$)

(config)# int ▽ S0

(config-if)# no ▽ ip ▽ address

(config-if)# no ▽ shut down

(config-if)# encapsulation ▽ Frame-relay

(config-if)# int ▽ S0.1 ▽ point_to_point

(config-subif)# ip ▽ address ▽ IP ▽ mask

(config-subif)# frame_relay ▽ interface-dlci ▽ dlci #

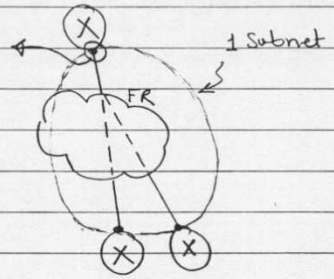
This command is used to assign each sub-interface a dlci #, to be able to receive correct LMI replies.

Case in exam: To reserve ips but it doesn't solve the split horizon problem use:

(1) point-to-point subinterface

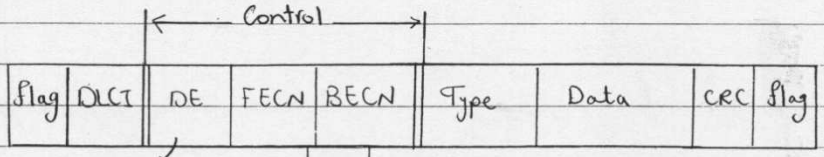
(2) point-to-multipoint subinterface (✓)

- Configure this interface as pt→multipoint only to reserve ips



FR congestion management

Cisco LAPF & itef LAPF Frame is as follow



DE ← Discard Elligibility

Frame لو discard as DE↑ ∴ discard elligibility ↑

BECN → Backward Explicit congestion notification

FECN → forward Explicit congestion notification

we've 2 definitions

CIR (Committed Information Rate): يعني بيضمن SP الـ rate ده

↳ guaranteed B.W ex: 512 Kbps

EIR (Excessive Inf. Rate): extra rate/B.W given in case of non-congestion

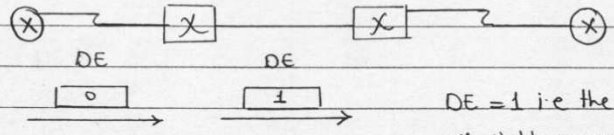
If the Rate of communication R is :

(1) $R \leq CIR$

∴ your frame will be surely delivered

(2) $CIR < R < CIR + EIR$

∴ your frame will be marked & will be dropped in case of service provider congestion

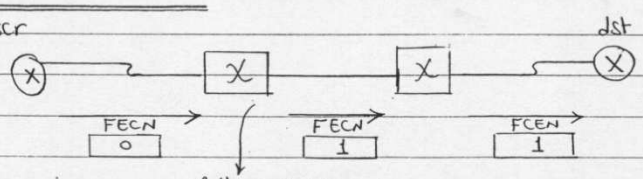


DE = 1 i.e the discard elligibility increased

(3) $R > CIR + EIR$

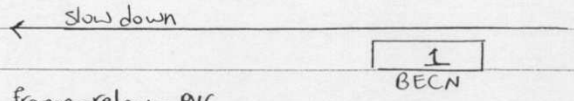
∴ your frames will be dropped

FECN & BECN :



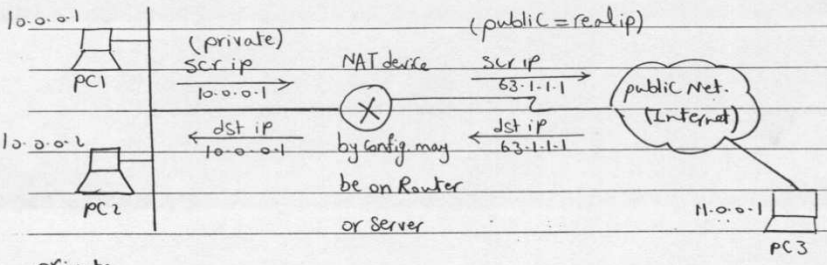
if the switch sensed very high rate then it will make FECN = 1

When dst receive FECN = 1, he'll send a frame to the scr with BECN = 1, asking the scr to slow down.



※ Sh ▼ frame-relay ▼ PVC

NAT (Network Address translation)



Private IPs assigned by IANA

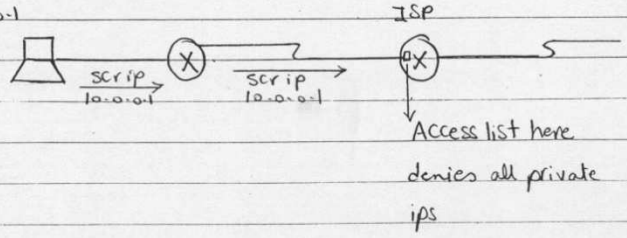
ClassA : 10.0.0.0 → 10.255.255.255

Class B : 172.16.0.0 → 172.31.255.255

ClassC : 192.168.0.0 → 192.168.255.255

- The main concept of NAT is that, when a pck is sent to the public Network (Internet), the NAT device (Router) will change the private address into a public (real) ip.

If there is no NATing :



- NAT is a software loaded on Routers or Servers.

NAT Terminology =

(1) Inside local ip: Internal device with private ip
i.e the local ip of a device exist in my Network
ex: 10.0.0.1

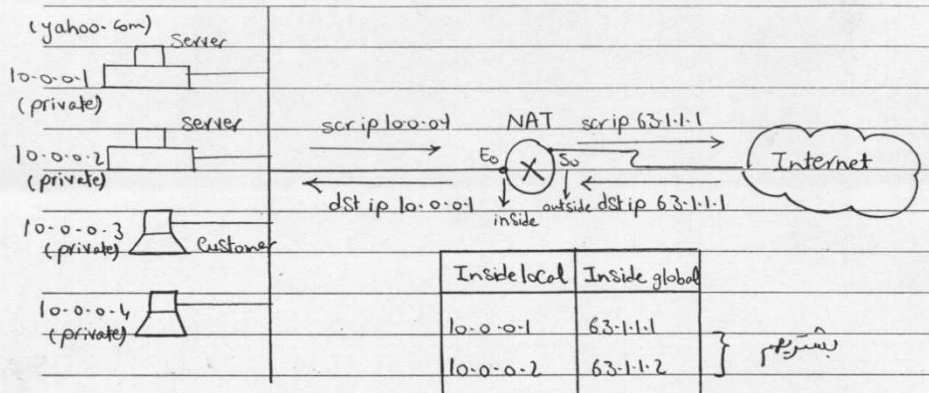
(2) Inside global ip: Internal device with public ip
i.e the global ip of a device exist in my Network
ex: 63.1.1.1

(3) outside local ip: external device with local ip
i.e the local ip of a device doesn't exist
in my Network

(4) outside global ip: external device with public ip
i.e the global ip of a device doesn't exist
in my Network

(240)

(1) Static NAT : 1 public → 1 private
↳ for "Servers"



Inside local	Inside global
10.0.0.1	63.1.1.1
10.0.0.2	63.1.1.2

بشروط

- The NAT Table is filled manually
- Static NAT is used if your devices are accessed by others for getting benefits from thier services (i.e Servers should have well known unchangable public ips)
- But why we don't give the servers a public ip only ?
  because Routers & Customers lie in the same Network with the Server should be in the same Subnet & so we will consume many public ips which is not desirable & so we use private ips even with servers

Configuration for Static NAT

(config)# ip nat inside source static Inside local ip Inside global ip

يعين ال pcks اللى جايه من جوه الشبكة

يعين ال nat محول ال Scr ip

⇒ Automatically will change the dst global ip → local ip

ex: (config)# ip nat inside source static 10.0.0.1 63.1.1.1

(config)# ip nat inside source static 10.0.0.2 63.1.1.2

- we've to assign NAT directions to interfaces in order to work as follow

(config)# int E0

(config-if)# ip nat inside

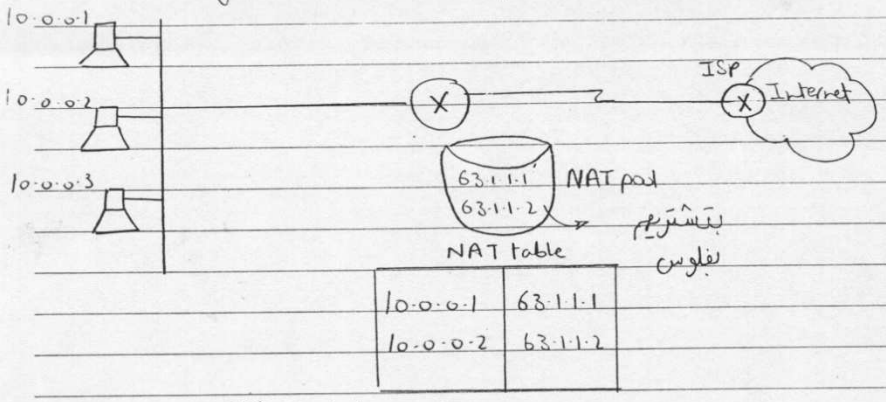
(config)# int S0

(config-if)# ip nat outside

- Trouble shooting: # Sh ip nat translation → Show NAT & PAT Tables

(2) Dynamic NAT : 1 private ip → 1 public ip

- It is used for clients that want to access a public Network
- NAT Table is filled dynamically
- NAT pool, is a pool of ips used to distribute real ips on PCs having private ips when they want to access the Internet



10.0.0.1	63.1.1.1
10.0.0.2	63.1.1.2

pck scr ip 10.0.0.3 →

this pck will be transmitted without translation & it will be dropped at the ISP Router

Configuration

(config)* ip nat pool pool name start ip end ip netmask subnet mask

↳ تعريف جروب و بديله اسم و تعريف ال ips اللي جوه

(config)* ip nat inside source list ACL# or name pool pool name

↳ بقول ACL جيب العنوان اللي أنه يأخذ ip

↳ انظر لل ip بتاع ال scr ولو معنوان ده ال ACL أنه يأخذ public ip

إديله public ip من ال pool اللي اسمها كذا

⇒ The Access list should be configured

(config)* access-list no. {permit} ip mask

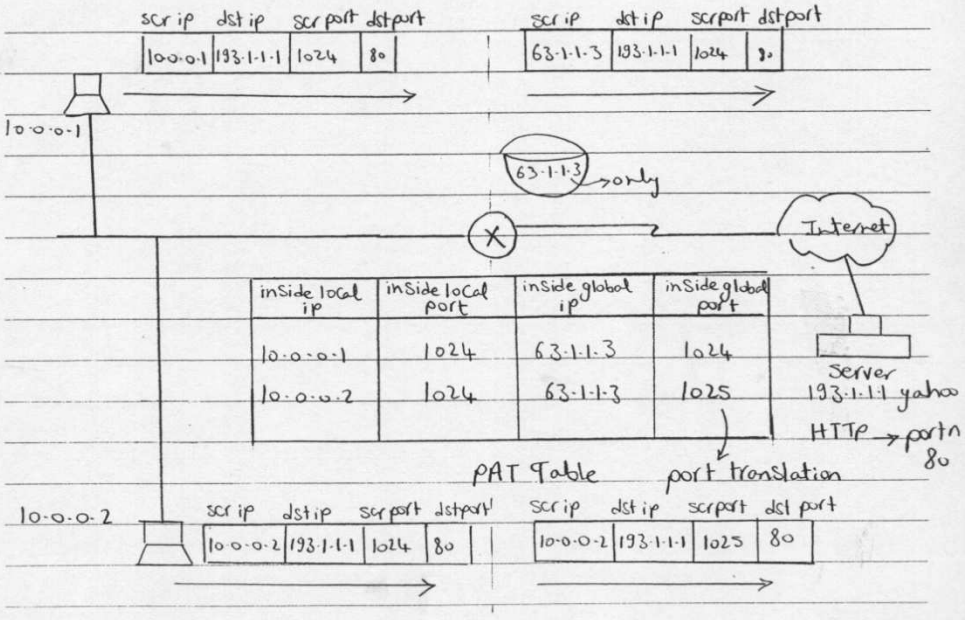
& also don't forget to assign NAT directions to interfaces

(config) # int ▼ E0
(config-if) # ip ▼ nat ▼ inside

(config) # int ▼ S0
(config-if) # ip ▼ nat ▼ outside

(3) Dynamic NAT with overload (PAT) : 1 public → many private

PAT ≡ Port Address Translation



port no. 0 — 65535

0 → 1023 1024 → 65535

Configuration

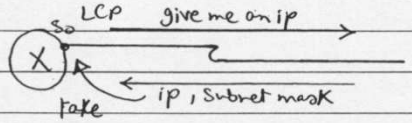
(config) # ip nat pool poolname startip endip netmask subnetmask
↳ define a pool

(config) # ip nat inside source list acl# pool poolname overload

ex: (config) # ip nat pool FM 63.1.1.1 63.1.1.1 255.0.0.0
(config) # ip nat inside source list 3 pool FM overload

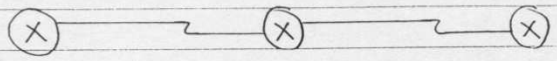
now used in DSL

(config) # ip nat inside source list acl# interface ex:so overload



Simulation(Lab3) (245) Session(27)
20/06/06

File → load Netmap → Routing, ACL, hdlc, ppp
File → load multidevices config. → Routing, ACL, hdlc, ppp



(only accessable)

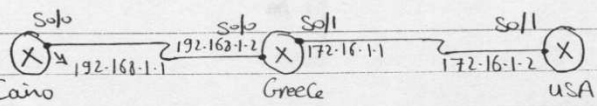
← إفترضه إنك في الإمتحان ومتعرفش أي حاجة عن الشبكة اللي قدامك وكل اللي Greece هي الوحيدة الـ accessable والمطلوب معرفة كل حاجة عنك وعن جيرانك في بساطة!

On Greece

Sh run ↵
- int So/0 has ip = 192.168.1.2 255.255.255.0
- int So/1 has ip = 172.16.1.1 255.255.0.0 & clk rate 64000
- we've 2 active RTG protocols Ripv2 & Eigrp
- password Cisco
- your host name is Greece

Sh cdp neighbors ↵
- USA capability Router, connected to Greece through int So/1 that has ip 172.16.1.2
- Cairo capability Router, connected to Greece through int So/0 that has ip 192.168.1.1

Now we can redraw the Network with all Labels



Access list (1) Standard (2) Extended (more reliable)

N.B: desired port على الـ Router اللي جاي ACL اعمل

ex: Deny ping only on port S0/0 of Greece from any other port
(↳ icmp)

Greece (config)# access-list 100 deny icmp any (scr) host 192.168.1.2
Greece (config)# access-list 100 permit ip any any

Greece (config)# int S0/0
Greece (config-if)# ip access-group 100 in
Greece (config-if)# ip access-group 100 out

Showing: # Sh access-list
deny → 5 matches (5 ping pcks were denied)
permit → 37 matches (ping to USA + updates) (hide in ip pck)

Sh ip interface
to know directions inbound/out bound
In bound access list is 100
outgoing access list is 100

Lab(4) (247)

let's strike WANs

on Cairo

\# Sh int S0/0 → أهم أمرز ال WAN

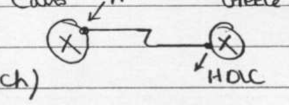
L1 up L2 up

encapsulation HDLC (default)

\# conf t

(config)# int S0/0

(config-if)# encapsulation ppp



\# Sh int S0/0

L2 up L2 admin down (encaps. mismatch)

on Greece

\# conf t

(config)# int S0/0

(config-if)# encapsulation ppp

if you write # Sh int S0/0

up up

also you can see LCP open

open IPCP, CDP, CP

to see the negotiation

use # debug ppp negotiation

we've No

\# Sh ppp

\# Sh ppp status

only

\# Sh int ___

⇐ اعمل Shutdown وبعد كده no Shutdown

لل int. علشان تشوف ال debugging

"O" outgoing , "I" Ingoing confrequest ⟶

⟵ ConfACK

IPCP : State is open

ppp Authentication

on Cairo (config)# int s0/0
(config-if)# ppp authentication chap

on Greece (config)# int s0/0
(config-if)# ppp authentication chap

⇒ Still if you write # sh int s0/0
up down ?
Coz we should assign a username & password

on Cairo
(config)# username Greece (≡ host name) password Cisco

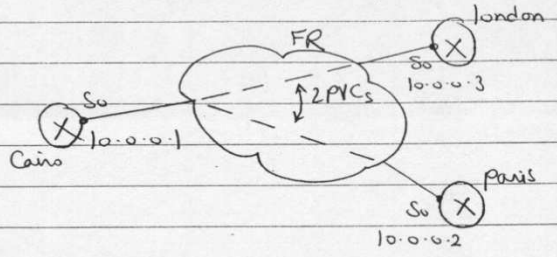
on Greece
(config)# username Cairo (hostname ≡) password Cisco

Now up up

Lab (4) (249)

Frame Relay

load Netmap → Frame Relay
load multidevices config. → Frame Relay



Trouble Shooting
Sh ▽ int ▽ S0
Sh ▽ frame-relay ▽ map
Sh ▽ frame-relay ▽ PVC
Sh ▽ frame-relay ▽ lmi

(config) # int ▽ S0
(config-if) # no ▽ shutdown
(config-if) # encapsulation ▽ frame-relay } on all Routers (Cairo, Paris & London) * Imp

default
encapsulation is CiscoLAPF
& not itef LAPF

Sh ▽ int ▽ S0
up up
encapsulation frame Relay
LMI type is Cisco (default)

N.B : LMI → Cisco
Ansi
q933a

Sh ▽ frame-relay ▽ map

ip of next hp	DLCI	B.C	State	static/dynamic
10.0.0.2	102	B.C	active	dynamic
10.0.0.3	103	B.C	active	dynamic

} use IARP

Sh frame-relay PVC

2 PVCs

BECN & FECN

PVC Status = active