

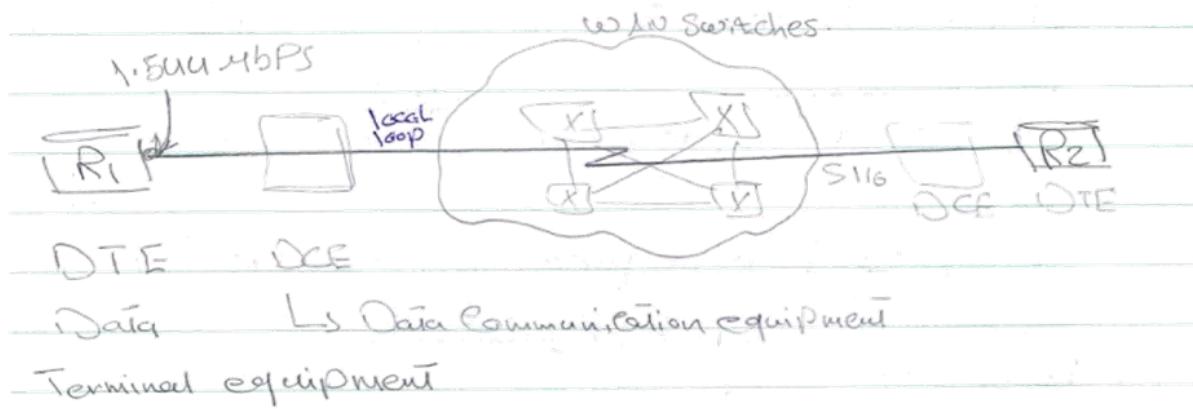
2018



*WAN Technology
papers
Written by:
Eng.
Amgad M. Mesallam
Edited by:
Eng. Abeer Hosni*



WAN introduction



DCE $\xrightarrow{\text{analog}}$ analog \rightarrow Modem
 $\xrightarrow{\text{digital}}$ digital (CSU/DSU)

Communication Co.
Carrier Co.
Teleco

Local loop \Rightarrow Customer (جیزیول، اینترنت)
 ISP (انترنت، ISP)

Demarcation point:

a physical point that defines the responsibilities of the Customer and the responsibilities of the ISP

النقطة الديارقة، ISP هي النقطة الفيزيائية التي يتحملها ISP وتحمّل مسؤولياته، وتحمّل مسؤولياته customer. DSL splits the ISP into two parts.

CPEs Customer Premises equipment

1G.0.0.2

10.0.0.0

11.0.0.0

12.0.0.0

PC1

RI

R2

PC2

Path A

Ethernet header

IP Header

TCP Header

Data

Source MAC = S1X1

Destination MAC = R1

L2 header

IP header

TCP header

Data

Ethernet header

IP header

TCP header

Data

Source MAC \rightarrow R2

Destination MAC = S2X2

(Wan Technologies)

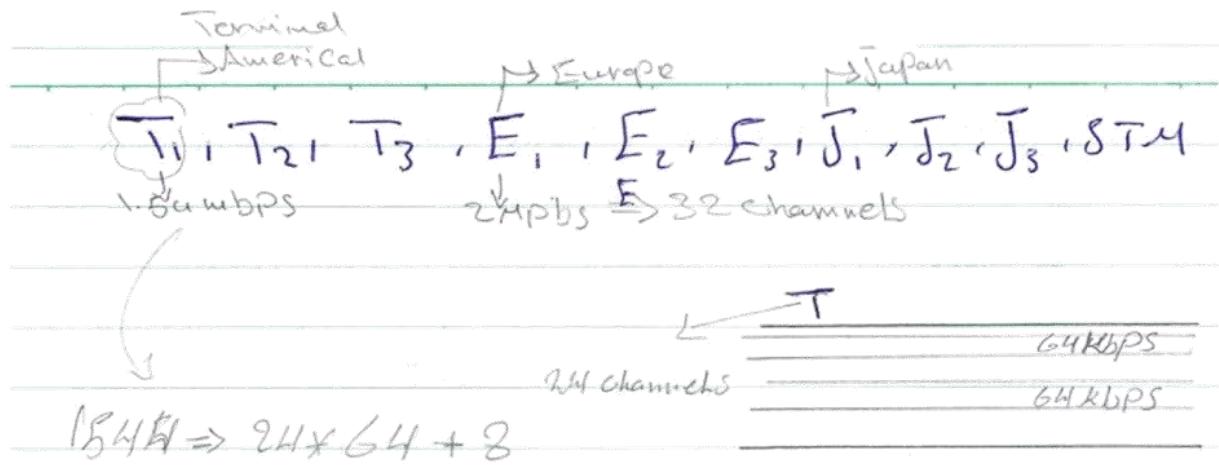
- * Dedicated Circuit Switching (leased line)



The data always travel from source to destination using the same path

Bandwidth, جودة الخدمة ونوع الاتصال ثابت

ويتم التحكم في الأمان



$$STM \Rightarrow 155 \text{ Mbps}$$

ISP جزء من

+ on-demand Circuit Switching -

It is a leased line for a short period of time

e.g. dial-up

لابتك لفترة معينة بحسب اتفاقية

• ISDN

one-to-one Data connection 30 channels 64Kbps per channel
Voice traffic

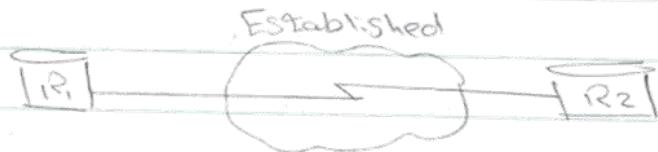
Voice 64Kbps

Data

. DSL هي إحدى تطبيقات ISDN

- Packet switching :-

Packet switching \rightarrow Circuit switching \rightarrow الاتصال



Source \rightarrow Connectivity \rightarrow Circuit sw. \rightarrow It's data \rightarrow Established. until destination, destination \rightarrow Source \rightarrow network

Packet switching



destination \rightarrow Source \rightarrow packets \rightarrow Data \rightarrow Destination

MPLS:

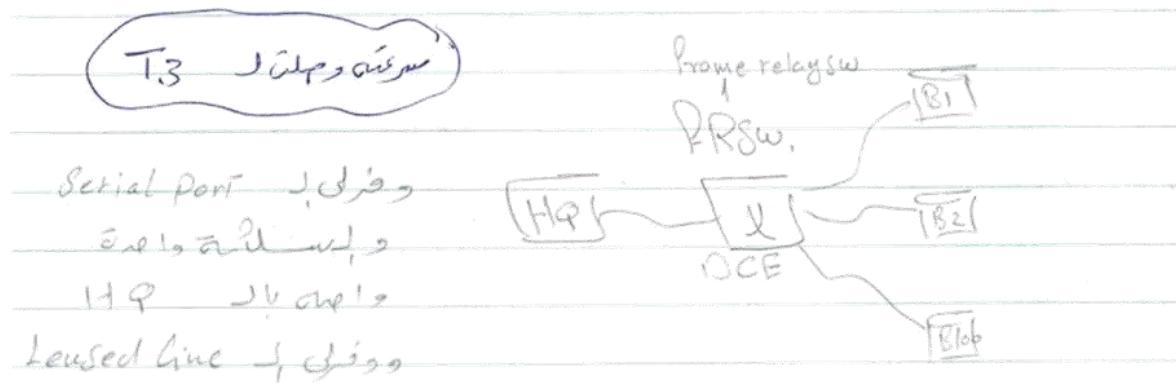
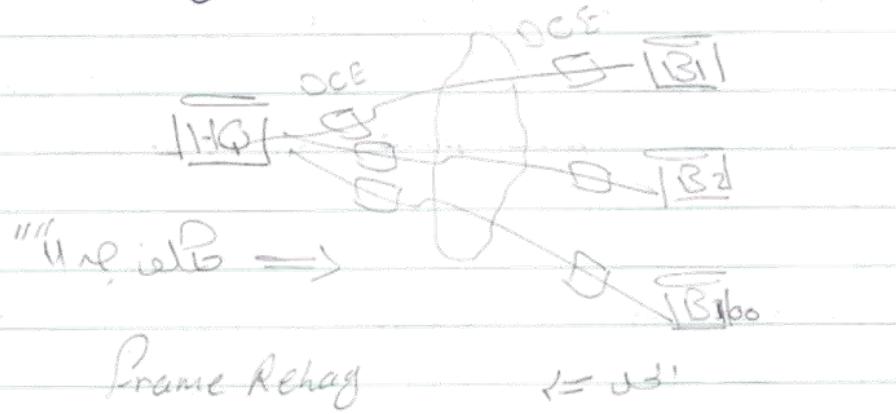
A WAN technology serves as the underlying network to carry multiple types of network traffic such as IP, ATM, Ethernet, and DSL

* Packet Switching انواع من

• X.25

(reliable - error correction) على الـ **Frame**
لـ **جودة بث** ، **نهاية محددة** ، **نهاية**

• Frame relay **بروتوكول لـ "الفرم"**



① Shared Bandwidth ← **أمثلة**
② low security.

CIR \Rightarrow ISP و بين Customer **لـ "النفاذ"**

و **Minimum Bandwidth** **لـ "النفاذ"**

(Committed info rate)

Frame relay \Rightarrow Packets (1500 Bytes) MTU

- Cells are ATM cells packets are ATM FR cells
- ATM is divided into Cells and header
(Cells = 53 bytes = 48 bytes data + 5 bytes header)

Congestion happens when a cell is lost
No Gbps throughput and low latency
between cells and between frames

- Broadband technologies-

- DSL (Digital Subscriber Line)
- Satellite
- Cable TV (DOCSIS)

DSL

voice

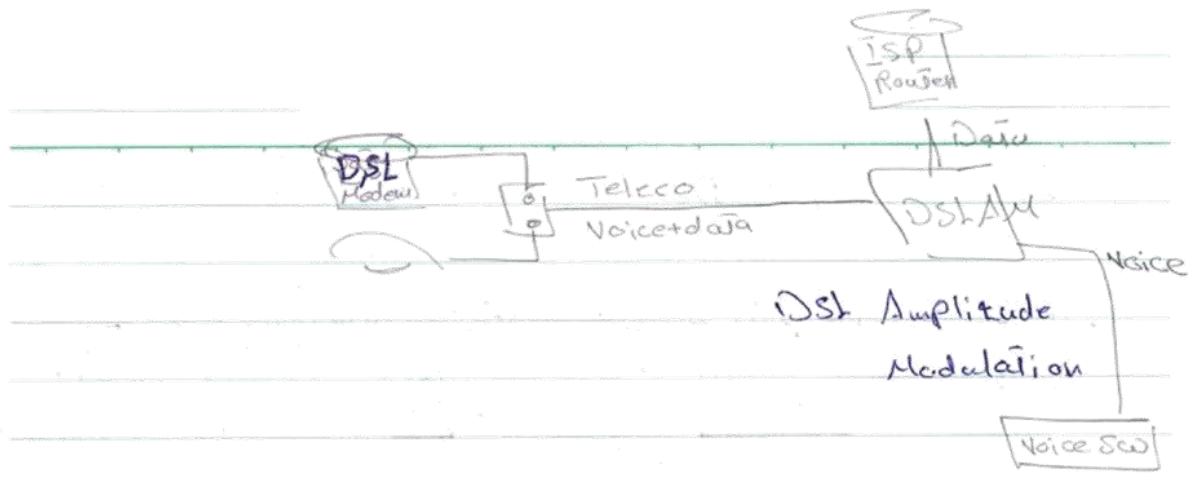
data

\hookrightarrow ADSL (asymmetric DSL)
asymetric

\hookrightarrow SDSL (symmetric DSL)
symmetric

ADSL \Rightarrow upload 1 Mbps Download 8 Mbps
1 : 8 ratio

SDSL \Rightarrow upload 1 Mbps Download 1 Mbps
1 : 1 ratio



PPP Protocol

Point-to-Point Protocol

لهز في الإغراق داخل بروتوكول

وذلك لأن بروتوكول

- Standard HDLC

" High level Data link Control)

Flag	Address	Control	data	FCS	Flag
------	---------	---------	------	-----	------

بروتوكول بروتوكول Cisco

- Cisco HDLC

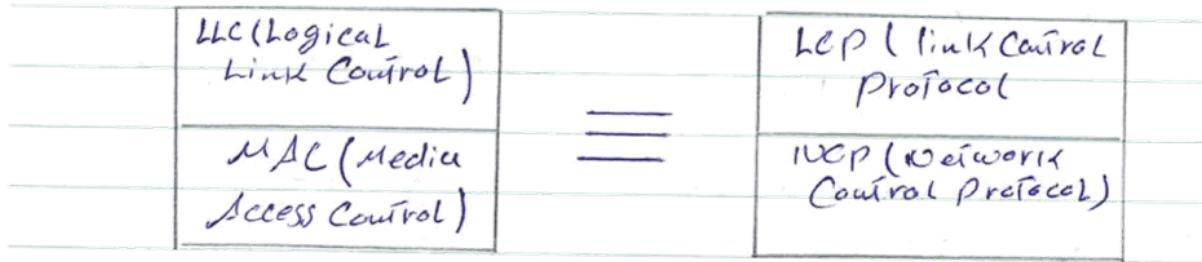
Flag	Address	Control	Protocol type	data	FCS	Flag
------	---------	---------	---------------	------	-----	------

بروتوكول Cisco بروتوكول Cisco بروتوكول Cisco

PPP على

L2

WAN



Ncp, LLC \Rightarrow يخواضون مع Layer Addressing لـ نوع ما يدعى بـ

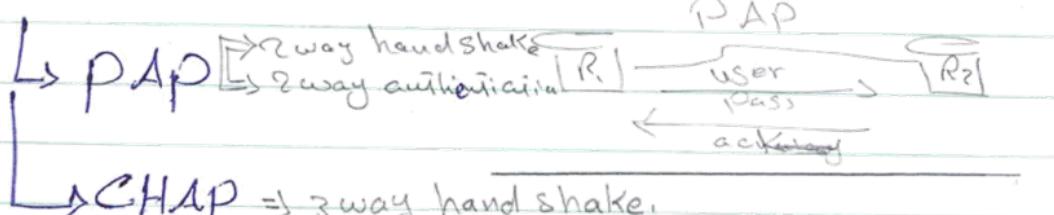
Lcp \Rightarrow RVR de Connect \rightarrow R ويكون له Properties مثل امتداد ونقطة الاتصال.

PPP properties



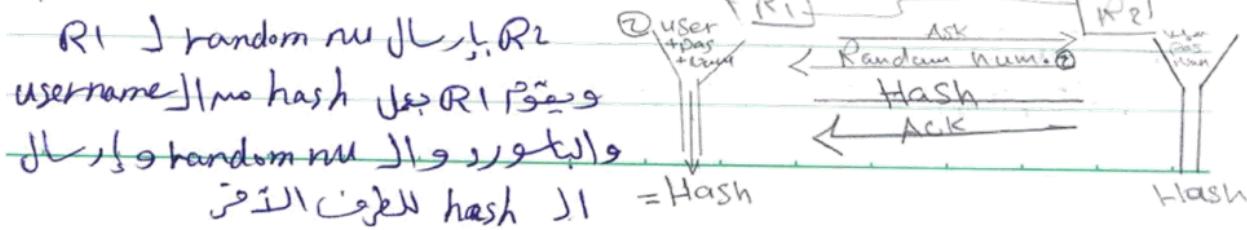
+ authentication

Routers \leftarrow two include Password & Username بخط يد
لـ RVR de Connect



CHAP \Rightarrow 3 way handshake.

ف يقوم R2 بـ الدخول في R1



والهدف آخر يقوم بنفس العملية فإذا اعزى سرقة سرقة
فلا يحصل على nothing user name والPW ونحوه بارسال الـ ACK

- Call back :-

يقوم الراوتر بفضل الـ Connection L1/L2 - [R1] --- [R2] --- [PC]
الذي يبدأ في الـ user ويعود بعمل الـ Connection بفضل الـ ACK

- Multi link :-

int ركيز link مع الـ IP
وأحد واعطاهم IP واحد لزيادة BW

one, all IP



Compressions:-

- ↳ predictor
- ↳ SACK
- ↳ MPPC

8sec



8sec 8sec 8sec



اقصر

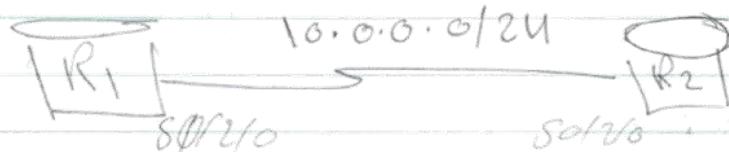
Compression

high load level

Microsoft Point-to-Point Compression

Lab

clock rate



R1 show controllers

R1 Config & 0

R1(Config) in 50/20

R1(Config-if) encapsulation ?

R2 (Config-if) # encapsulation PPP ↴
R2 * show ip int br

authentication



Usernames R2

Pass CC10A

Usernames R1

Pass CC10A

r1 (Config) # username R2 Pass CC10A

r2 (Config) # username R1 Pass CC10A

r1 (Config) # int s0/2/0 ↴

* PPP authentication ?

* If " " → CHAP

(LCP open)

R1 # show ip int br

-> (is up/down (o int)) اذالات حالة البروتوكول

① encapsulation mismatch

② authentication failure

وهي تك اذالات يكون حالة البروتوكول

R1 # show int s0/2/0 كا يفتح open (نافر)

* مفتوحة

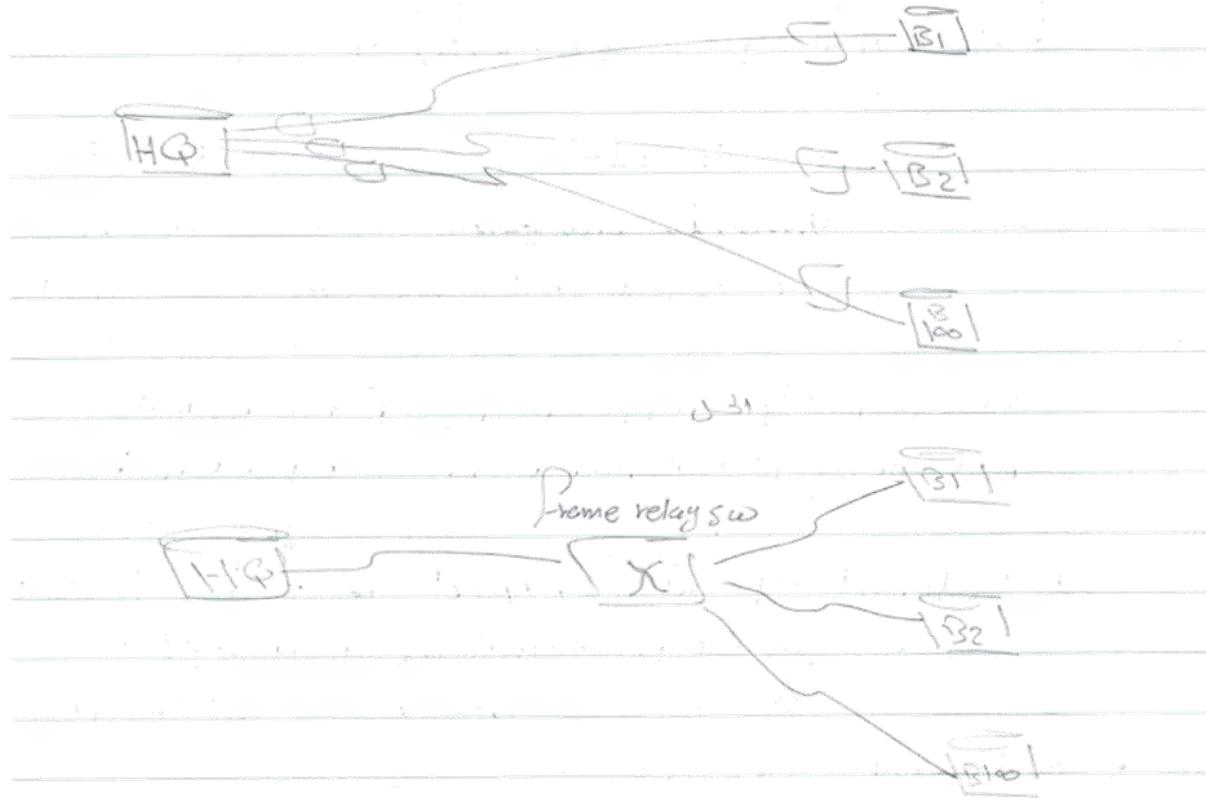
الراوتر اذالات (clocking configured by default) اذالات net اذالات clock rate اذالات

-> clock rate اذالات

R1 (Config-if) # clock rate ↴ ← s0/2/0

└ DCE router

((Frame relay))

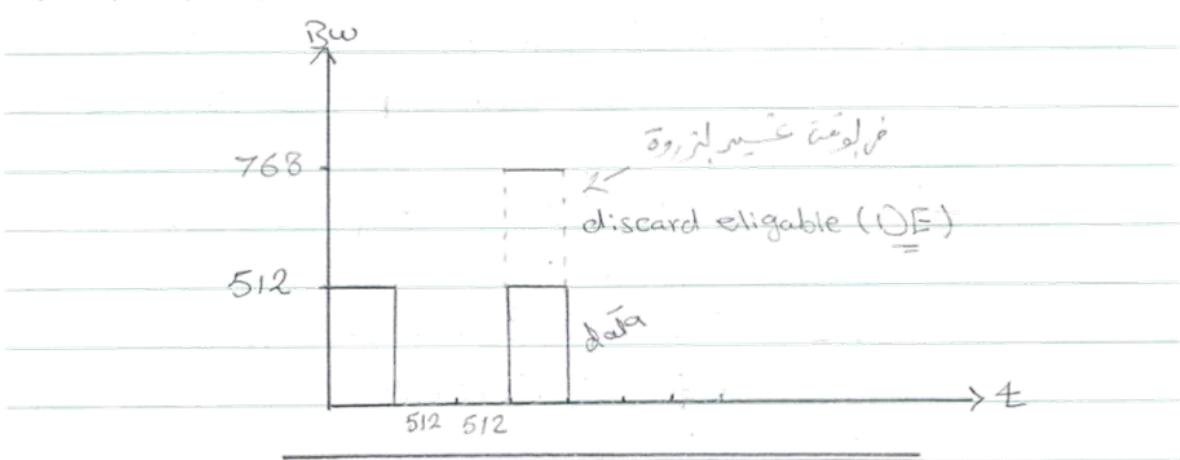


(Security) \rightarrow ① \leftarrow \rightarrow \leftarrow \rightarrow \leftarrow \rightarrow
shared. \leftarrow \rightarrow \leftarrow \rightarrow \leftarrow \rightarrow
نحوه في المحيط \rightarrow \leftarrow \rightarrow \leftarrow \rightarrow \leftarrow \rightarrow
Relay sw

CIR \rightarrow ISP مع الفاقيحة! ISP \rightarrow ولـ
Committed information rate

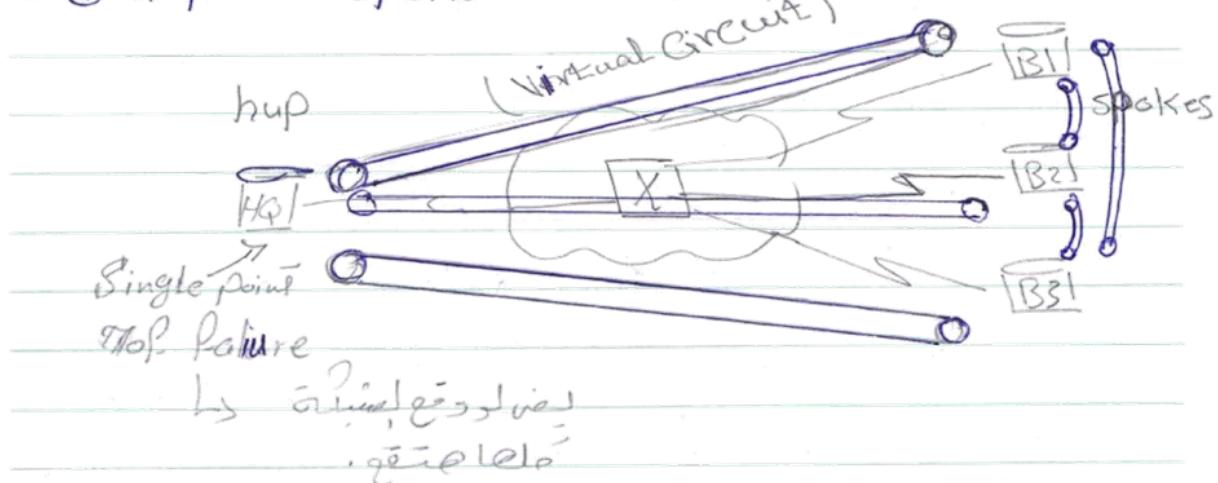
mini. Bw \rightarrow ISP \rightarrow \leftarrow \rightarrow
متحدة معاً في وقت المزدوجة مثل "512"

Frame Relay Technology \rightarrow \leftarrow



Frame Relay Topologies:-

① hub and spoke (loop cast)



② Partial Mesh

$B_2 \rightarrow B_1$ \Rightarrow أطول مسافة بين الأفرع \Rightarrow branches \Rightarrow VC \Rightarrow تحميل ثقيل *

③ Full Mesh

أقصى مسافة بين الأفرع \Rightarrow $B_1 \rightarrow B_3$ \Rightarrow Direct \Rightarrow Destination \Rightarrow Source \Rightarrow Data

يعنى \Rightarrow معندهم أي فرع

لهم لو عاوز اعرف عى كام Full mesh معاً كل طرada
فلا ينفعك إلا Virtual Circuit

$$NC = n(n-1)/2$$

$n = \text{No. of R}$

Virtual Circuit

SVC
Switched VC
Data link, physical
in Circuit Layer
Established

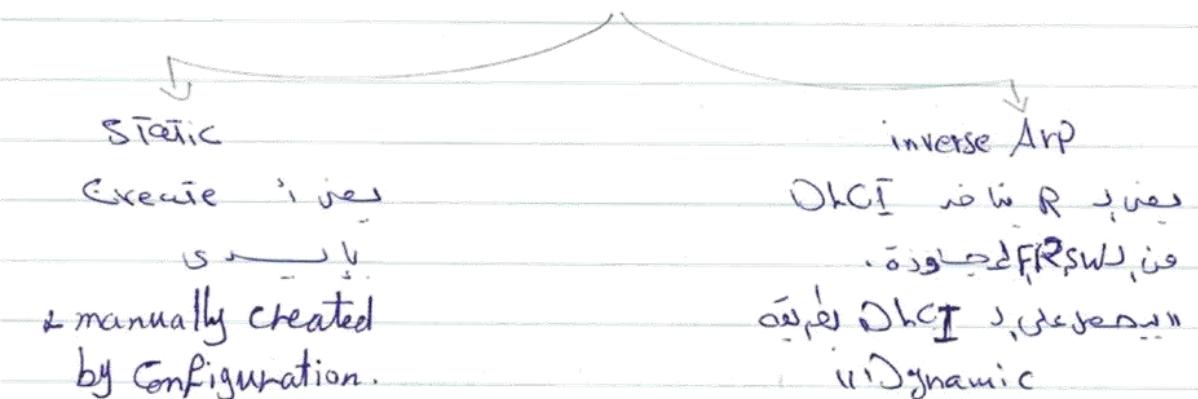
PVC
Permanent NC
دائم الاتصال، دائمة

MAC Layer، او راجييس Frame Relay ،
Serial int. ، DLCI
DLCI ،
Data link ، Connection Identifier
L2 addressing.

لهم لو عاوز اعرف عى كام Create Virtual VC
Source DLCI، Destination DLCI
Lateral Configuration

DLCI \Rightarrow Locally Significant Per Segment.
Router's has unique set of DLCI from

DLCI



Active إن دلولين شائعة لتعريف الاتصال

LMI Protocol

(Local Management Interface)

Destination, Source مابين دلولين
Signal إشارة

يعلم لطرف من صنف دلولين

① Active

يعلم لطرف بعنوان فيه

② In Active

③ Deleted

(DLCI is deleted
on my side)

يعلم لطرف

DLCI دلولين

LMI Types:-

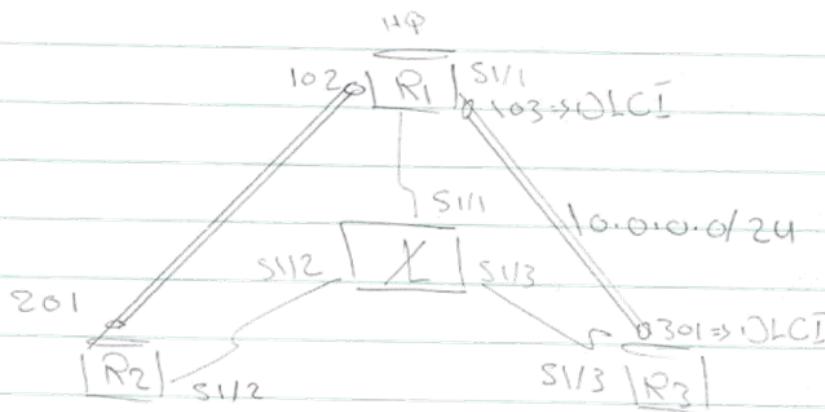
- Cisco (default)
- ANSI
- Q.933a



(locally significant per segment)

نقطة، في الـ LMI تدعى mismatch (رسالة up/down)، حيث إنها تؤدي إلى خطأ

11 Frame relay Configuration



hub and spoke

GN5 \Rightarrow R3700

Rc \Rightarrow hostname Frsw

line console

\rightarrow First, Configuring router Cisco as a frame relay switch.

Frsw ~~*~~ Config & t

FRSW(config) ~~*~~ Frame-relay & switching

FRSW(config) ~~*~~ int S1/1

(Config-if) ~~*~~ no ip address

(Config-if) ~~*~~ encapsulation frame-relay

(Config-if) ~~*~~ frame-relay ?

(Config-if) ~~*~~ frame-relay InP-type

(Config-if) ~~*~~ clock rate 64000

(Config-if) ~~*~~ no frame-relay inverse-arp

PVC ~~*~~ frame-relay route 102 int S1/2 201

~~*~~ frame-relay route 103 interface S1/3 0.3.0.1

~~*~~ no shutdown

~~*~~ end

* show run int s1/1 ← Running Config لغات
Paste, Copy ← Data tab
جاء من الملفات ← int لغات
Frame-relay route 301 int s1/1 102

* int s1/2

* Paste ↴

* int s1/3

* Paste ⇒ Frame-relay route 301 int s1/3 103 ↴

* show frame-relay route ↴

r1(Config) * int s1/1 ↴

r1(Config-if) * ip add 10.0.0.1 255.255.255.0 ↴

* encapsulation frame-relay ↴

* no frame-relay inverse-arp

* frame-relay map ip 10.0.0.2 102
broadcast ↴

* frame-relay map ip 10.0.0.3 103

broadcast ↴

* no shutdown ↴

R2(Config) # S1/2

R2(Config-if) # ip add 10.0.0.2 255.255.255.0 ↵

* encapsulation frame-relay ↵

* no frame-relay inverse-arp ↵

* frame-relay map ip 10.0.0.1 201 ↵

* frame-relay map ip 10.0.0.3 201 ↵

* no shut ↵

R3(Config) # S1/2 ↵

* ip add 10.0.0.3 255.255.255.0 ↵

* encapsulation frame-relay ↵

* no frame-relay inverse-arp ↵

* frame-relay map ip 10.0.0.1 301 ↵

* frame-relay map ip 10.0.0.2 301 ↵

* no shut ↵

R1 * show frame-relay map ↵

R2 * trace route 10.0.0.3 ↵

R3 لا يوجد رute من هنا! ↵

Broadcast :- Broadcast is used in R.I, the interface
 R.I is a full duplex link and uses Multicast I.L, it
 has a specific Routing Protocol decision rule.
 Multicast Broadcast \Leftarrow update

Point-to-Point Broadcast with its Recommended
 and some features

* split-Horizon issue

It is a problem in which update is received
 from a neighbor in split horizon, or in EIGRP & RIP \Leftarrow Routing Protocol
 to avoid sending update to the same port

- No IP split-horizon eigrp &
 Routing Loop \Leftarrow It is not present in EIGRP

- Full mesh

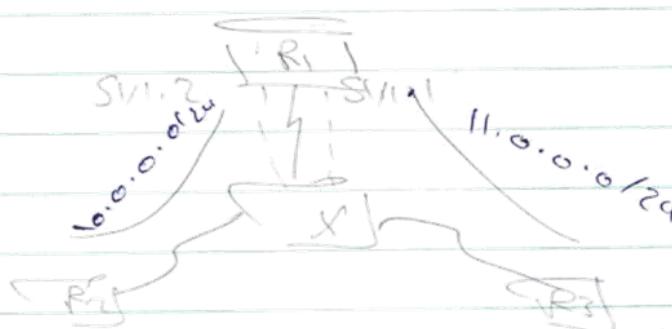
• Across the Cost

Same in!

This is full

* vr = sub interfaces

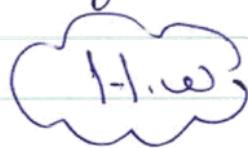
(Point-to-Point sub interfaces)



وَمَا هِيَ سَلْكٌ ؟

* int S11.1 Point-to-Point ↪

* Frame-relay interface-Dcls 102 ↪



RJ, DLSW, PPs,

LMI لـ مـاـجـيـكـاـلـ

r(Config) * int S11 ↪

r(Config-if) * Frame-relay LMI-tg ?

Frame Relay Congestion management

Congestion (steps)

- Backward Explicit Congestion Notification ((BECNU))

- Forward Explicit Congestion Notification (FECNU)

- Discard Eligibility



Network attacks

To understand Network Security

Network attack \rightarrow هجوم على الشبكة

① Physical Network attack

Physical Installations-

Mitigation \rightarrow Secure equipment physically in a separate room

\rightarrow Using Video Monitoring or wireless webcam.

② Reconnaissance attack

هدفها جمع المعلومات عن الأنظمة والخدمات

- a) packet sniffers
- b) ping sweep
- c) port scan
- d) using internet database
- e) google hack

③ Access Attack

- a) Password attack (brute-force & dictionary attack)
- b) Trust exploitation
- c) man-in-the-middle

Dos attacks-

① Ping flood.

② Mail Bomb "رسالة لسرقة E-mails involves Destination جهت اوجه الى destination جهت اخراجها من البريد" .

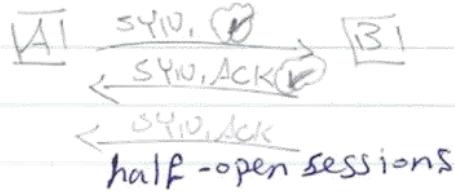
③ SYN Flood

attack on Destination source

، بعـض SYN \leftrightarrow TCP

خراج

④ IP spoofing



Distributed Dos - DDoS

الى IP بث ، PCs جهات
attack tools

Server side PC1 PC2 PC3 PC4

server

attacker

R1 (Config) Security passwords min-length 10

Password length \geq 8 includes

(Auto secure)

CDP → Cisco Discovery Protocol
Enabled by default

Finger → يُعرف في الموجة التي تصل إلى نظام التشغيل
Enabled by default.

Configuration
الإعدادات التي تجعل Auto Secure مفعلة
عن طريق Router التي تفتح
خدمات غير مرغوب فيها
un-wanted services

(Auto secure)

Full
=
يُفتح جميع خدماتها
عما، افتح، ابْرَدْهار، افتح، افتح

No-interact
=
عن طريق تعامل معها وفقاً
ووجهة نظر Cisco
فقط على التي تفتح
ويفتح كل شيء
من وجهة نظرها.

Labo- Cisco



Router # auto secure? Enable J.
mode

Router # auto secure Full *

=

Router # auto secure ibo-interact<

في حالات العذرية interactive mode full
الذى تتم عمله من دون حالة لتجاهة
هذا سيف تم بدل 1024، كذلك سيف
6 character كحد أدنى لـ min length

Router # show run

تحت المدى no all services
enable لتجاهة سيف لـ Cisco service

ex) R(Config) # ip http server

ip http secure-server

((VPN))

Virtual Private Network

VPN gives us leased line between LAN LAN no real traffic - لجعل اتصال LAN LAN مجازاً



- Private is Tunnel data, which is also Private
- برمجة بطرقة ان تذهب بعدها Data encapsulation
- veip

VPN وظائف

Tunnel \Rightarrow Clear text
SSTI \Rightarrow Encrypted
VPN \Rightarrow Tunneled.

① Confidentiality \Rightarrow data or

encryption

data

نقطة الى

ومني نوعين من

symmetric

data key

key different

data key

R1
Key

R2
Key

Security, privacy, authentication
in route tunneling

key

Asymmetric

R1

R2

Public Key

Public Key

Private Key

Private Key

Public \Rightarrow data, same

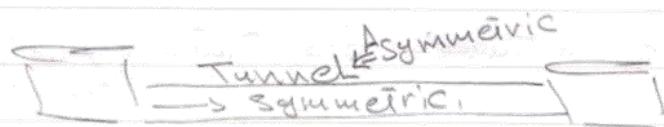
Private \Rightarrow private key

symmetric

- * DES (56 bit)
- * 3DES ($3 \times 56 = 168$ bit) (112 bit active)
- * AES (128 bit) subset
(192 bit)
(256 bit)

Asymmetric

- * RSA (SSH negotiations)
- * Diffie-Hellman
public key exchange
 - Group 1 (768 bit)
 - Group 2 (1024 bit)
 - Group 5 (1536 bit)



Asymmetric \leftarrow Key exchange
symmetric \leftarrow Data exchange

Negotiation protocols:-

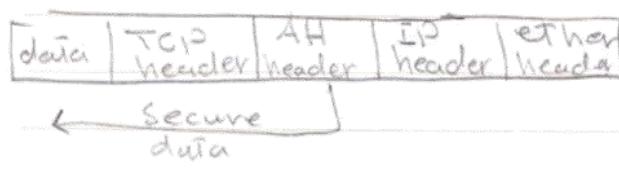
2 protocols

AH

auth header

فقط للتحقيق

- Security by auth.



ESP

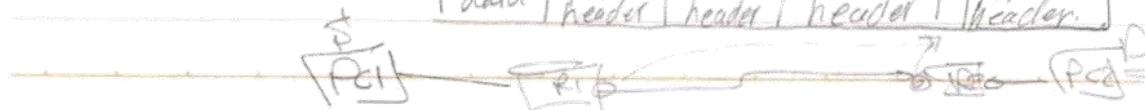
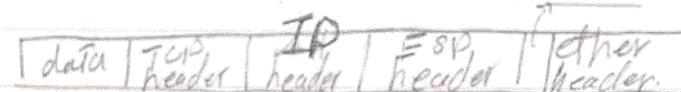
encapsulation

Security payload

فقط للتحقيق

- Security by auth

- encryption



* طريقة عمل الـ Asymmetric



يقوم الـ public key من source بإرسال الـ destination
يستخدم في تشفير الـ private key الخاص به والذي يملك به المستلم
ثم يقوم بإرسال الـ encrypted private key إلى destination
وبالتالي حماة حمل message key لا sniff
. digital certificate يكون داخل الـ public key وارسل إلى source

② authentication

التحقق

pre-shared key

PKI

public key infra

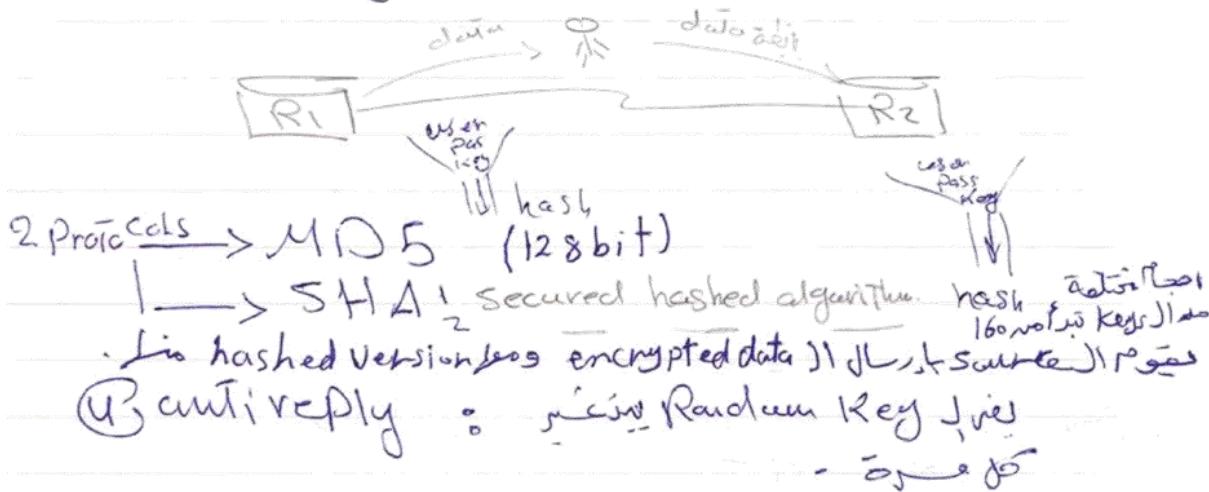
- يتم كتابته على الروتير ويتم تبادله
بعد تشفيره ولكن يفضل تغييره كل
فترة كنوع من الـ security

- عن المعدودات الكثيرة
يحسب تفاصيل key كل فترة
ويحصل على CA لدعائه
الـ Key وCertificates

(The data is not altered).

③ Integrity

data is not altered



* How to create a tunnel -

- GRE (generic routing encapsulation)

جهاز امني يرسل بروتوكول

وقد يوجد بـ

- PPTP (Point-to-Point Tunneling Protocol)
Microsoft provides GRE and PPTP

- L2TP (Layer 2 Tunneling Protocol)
[L2F + PPTP]

- IP SEC & Tunnels, create VPN

IPsec will GRE will Cisco's Cisco's tunnel will -

Lab ② Configuring a basic GRE Tunnel.

- EIGRP ١٢٣ IP بروتوكول ١

ـ R1, R2, R3 three sites مثل R1, R2, R3

ـ VPN ١٢٣ لـ agency ١٢٣

- GRE encapsulation is not encrypted by default, but can be encrypted through simple configuration techniques

ـ private ١٢٣ R3, R1 ١٢٣ R2

ـ will fit IP ١٢٣ ١٢٣ networks

ـ private network ١٢٣ encapsulation

ـ it uses its logical (virtual) interface & loopback ١٢٣ tunnel ١٢٣ tunnel ١٢٣ ١٢٣ routers ١٢٣

R1(config)# int tunnel 0

R1(config-if)# ip add 172.16.1.3 255.255.255.0

R1(config-if)# tunnel source s0/0

R1(config-if)# tunnel destination 192.168.23.3

R3(config)# int tunnel 0

R3(config-if)# ip address 172.16.13.3 255.255.255.0

R3(config-if)# tunnel source s0/0

R3(config-if)# tunnel destination 192.168.12.1

ـ successful config

R1, R3 ١٢٣

ـ A ١٢٣ eigrp ٤٥٦ R3, R1 ١٢٣ routing protocol ١٢٣ eigrp ٤٥٦ ١٢٣

R1(config-router)# network 172.16.0.0, no auto-summary

R3(config-router)# network 172.16.0.0, no auto-summary

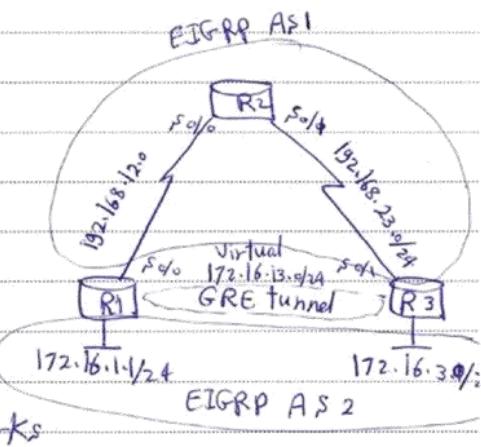
R1, R3 # show ip eigrp neighbors 2

ـ tunnel interface ١٢٣ EIGRP adjacency ١٢٣ ١٢٣

R1, R3 # show ip route

ـ R2 config ١٢٣ loopback int ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣

ـ Virtually ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣ ١٢٣



Another situation:

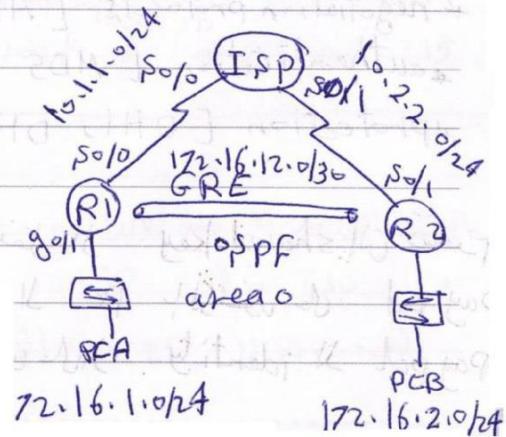
Lab GRE (generic routing encapsulation)

جهاز ISP يرسل بث إلى R1

R1 يرسل بث إلى ISP

و OSPF لـ multicast packets

، streaming applications & EIGRP



نقوم بعمل static route في ISP

R1(config)# int tunnel 0

R1(config-if)# ip add 172.16.12.1 255.255.255.252

tunnel source S0/0

tunnel destination 10.2.2.2

R1, R2 # show ip int br

R1# show int tunnel 0

 tunnel source 10.1.1.1 , destination 10.2.2.2

 tunnel protocol/transport GRE/IP

R1# ping 172.16.12.2 successful

- نقوم بتنفيذ الـ OSPF على LAN int و tunnel int

R1(config-router)# net 172.16.2.0 0.0.0.255 area 0

net 172.16.12.0 0.0.0.3 area 0

ونفذ على LAN int و tunnel int على R2

، executes OSPF on R2 on LAN int and tunnel int

* مسارات إلى ISP

نقوم بعمل static route على WAN links (EIGRP) two processes

، وننكر اتصاله أولاً فإن ISP لن يرى

الـ LAN int بـ static routes

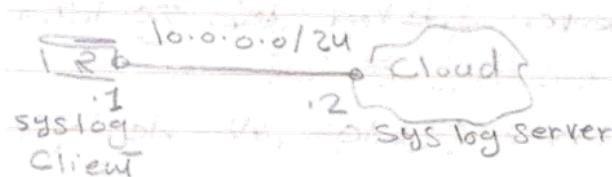
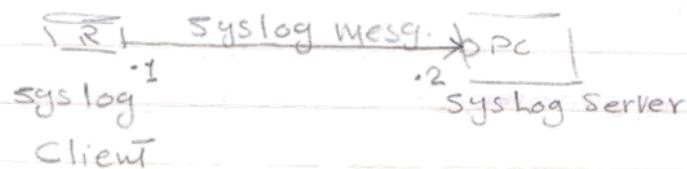
Syslog

عَنْ أَبْعَدِ مَسْتَوَىٰ وَمُعْدَنِيَّةٍ وَمُسْتَوَىٰ أَكْلَمِيَّةٍ

S.W. 3, S.R. 3, Jessie

CiOS => Run as admin

10.0.0.0/24



Router Config

* int R0/0

* IP add 10.0.0.1 255.255.255.0 ↘

no shu

* Ping 10.0.0.2 ↗

(Setup Kiwi Syslog Server)

Kiwi syslog server

Router (Config) * Logging on => log if enable new
enabled by default

(Config) * logging = ?

* logging = 10.0.0.2 <

* end

Kiwi لogging على برنامج

Time Stamp => الوقت المدخل في log
R جهاز clock لـ نظام اخطاء النمل

(Config) * line Console

(Config-line)

login local

* exit

(Config) * username Abeer pass 123

* username Ahmed pass 456

* login on-success log

Server log file لـ login successful

* login on-failure log

Server log file لـ login failed

Exit - Exit

* username: abeer

Password: 123

% Sec-log - 5-log

↳ Severity num.

Severity numbers

- Emergency (Severity 0)
- Alert (Severity 1)
- Critical (Severity 2)
- Error (Severity 3)
- Warning (Severity 4)
- Notification (Severity 5)
- Information (Severity 6)
- Debugging (Severity 7)

(config) ✘ logging console 6 ↪

sys log ينبع من severity 6

(config) ✘ logging buffered ✘

يُسجل الأحداث في ذاكرة Ram، حيث يتم حفظها

✘ logging buffered 5000

5000 byte ↪ ذاكرة ١,٢٠٠٠٠٠

R ✘ debug IP packet ↪ IP، de bug dev

✘ show logging ↪

log تأثيراته

✘ clear logging ↪

清除 logs ✘ Clear كل الأحداث

buffer ✘

(Config) ✘ Logging origin-id ?
R معلومات المتصفح تدخل في id log . اي عنوان المتصفح

(Config) ✘ Logging origin-id > hostname

(Config) ✘ Logging origin-id > IP

IP → R يأخذ IP المدخل في id log

(Config) ✘ Logging source-interface f0/0

0.0.0.0 → syslogserver || يأخذ source int f0/0

(Config) ✘ Logging origin-id > string MY-ROUTER

Logging trap 6 severity 6 to syslog Server
6 → by default

File → import Export setting from INI file.

Kali viewer . لفتح الملفات والصور .
وأفتح الملفات التي تم إنشاؤها .

summary

Logs can be on :-

- Console
- terminals (R # terminal monitor)
- SNMP
- syslog servers
- buffer

syslog

R(Config)# security authentication failure rate 2 log

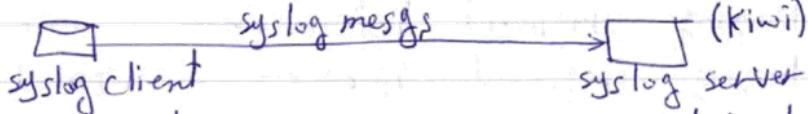
التي حدثت أثنتين أو
user log يجيء من جهاز auth لـ console the logs -
.auth

.buffer size 1000 لـ messages و كل لـ 1000 messages

R(Config) # logging buffered 5000

R# show logging

syslog server (logs) 10 messages



- syslog [timestamp + log msg name + severity level + text]

level	name	description
0	emergency	router unstable
1	alert	immediate action required
2	critical	condition critical
3	error	" error
4	warning	" warning
5	notification	normal but important event
6	info	info msg
7	debugging	debug "

.int interface no shutdown interface 5 .Logs will be sent to interface 0

lab

R(F0)

192.168.1.1

Kiwi

192.168.1.2

① install Kiwi on the server

② R(Config) # logging on ← enable logging

③ # logging 192.168.1.2 ← Configure log host

④ # logging trap 0 ← (optional) defines the severity level

⑤ # logging source int F0 ← (optional) defines the src int

⑥ # logging origin-id 192.168.1.2 ← (optional) define the router name or IP

جاءت مساعدة في kiwi syslog ومهم desktop على 2 short cuts هي kiwi cube و kiwi cube viewer . وبجانبها avereage . والتي تظهر رسائل الأرولوج . kiwi log viewer & daemon .
أيضاً kiwi log viewer إذا استلم المارز رسالة log .
ويظهر log على الراوتر تحت logs وفقط على Consolle .
فيما يلي يظهر رقم ال severity في viewer message .
يظهر في ال priority .
يظهر في ال severity .

في حالة وجود أكثر من راوتر في الشبكة ونريد ما إن تظهر على viewer بالـ IP .
وليس بالـ IP منفصل لآخر .

R(Config)# logging origin-id hostname يظهر باسم الماوتر
logging origin-id ip ← IP ← IP

logging origin-id string ← ← ← يظهر اسم الماوتر

. messages viewer أو الـ IP أو text في خانة

إذا استخدمنا لهذا بحث يظهر كـ IP فإنه يظهر . حتى يتم تحديد الـ source-int

R(Config)# logging source-interface fo

في برنامج kiwi يوجد icon داخل علامة الماوتر

أيضاً severity tab تظهر احصائيات على logs بر

kiwi-log viewer لـ logs في برنامج kiwi logs save عمل file → export settings to ini file

وسيتم عمل file ini في logs لـ save يوجد

داخله مسار لـ cache file الذي هو الـ

C:\prof files\syslogd\logs\syslog\catchall.text

وهذا الملف هو الذي يتم فتح him

log viewer → file → open → بـ viewer

View → clear display

logs لـ view

- R(Config)# logging on (enabled by default).

R# show log (to check if it's enabled)

syslog destinations [Consolle - monitor (Vty, AUX)]

memory buffer - SNMP trap - Flash]

R(Config) # logging 3 [means from 0 → 3]
R(Config) # logging Console debugging = Logging Console 7
disabled by default

R(Config) # service sequence-numbers ← enables seq no of the log

R(Config) # service timestamps ← enables time stamp of the log
service timestamps log ←
<cr> datetime uptime ← time only not date
since last reload

R # terminal monitor ← enable logging to telnet

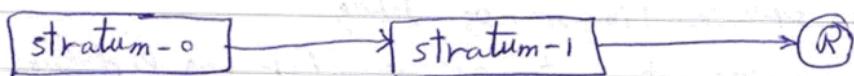
, syslogserver) (1 severity 6) (1) by default -
syslog set N (fei W) logs N filters N (rins) logging facility rnf -
. logs N format N (E) rns si

R(Config) # no service timestamps log
no service timestamps debug
no service timestamps ← for log & debug

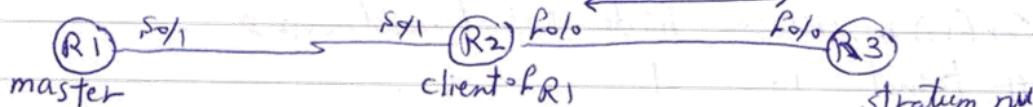
NTP (UDP 123)

المحاجع synchronized في الشبكة بتوقيت العالم time servers digital certificates NIS, syslogs authentication

atomic clocks stratum-0 موجوداً NTP top hierarchy هي stratum-0 no time synch يدعى Cisco (روتيرات نسبية)، clock public NTP servers يحصلون على جملة



- NTP v3 is more secured than v1, v2 - Peer to each other



R1(Config) # ntp master (or) ntp master 5

لتحقيق ذلك أو وضع رقم أو stratum number

- every next tree level has less accuracy.
- levels are known as stratum in NTP
- time always passed in UTC. (universal time coordinated)
- NTP roles (server - client - peer)
 - server → supplies time but not adjust local
 - client → only adjusts to clock info
 - peer → synchronize each other - but must be in the same stratum,
- peers always public NTP client always edge router
- router is not synchronization

- Key num must match in NTP authentication.
- The client authenticates the server not the opposite because the server doesn't care who will get the clock.

lab R2(config)#ntp server 10.0.0.1
 رجاءً من R1 لا يُعرف R2 كل نصف كل ملء ونحو synchronization هو المطلوب

R2# show ntp status

clock is synchronized, reference is 10.0.0.1

R2# debug ntp packet , debug ntp authentication

R2(config)# ntp authenticate enable authentication

#ntp authenticate-key 1 mds ccIE

#ntp trusted-key 1 (Key must be present) (في حالة وجود خلل في المفتاح)

R2(config)#ntp server 10.0.0.1 key 1

R2# show ntp associations detail

Configured, authenticated.

رسالة client clock will be synchronized by default -

→ BWR ACL number 1 is used

R1(config)#ntp access-group SERVERONLY_1

R2(config)#ntp source loop1

multicast group) clock of client will be

R1(config-if)#ntp multicast 224.1.1.1

R2(config-if)#ntp multicast client 224.1.1.1

123 is NTP port 119 will debug ip packet no

R2# show clock detail

NTP no delay time source is وقت الملاحة

R2# show ntp associations

* 10.0.0.1 ← synchronized ntp clock (ntp will go to the gateway)

R2(config)#ntp peer 11.0.0.3

R3(config)#ntp peer 11.0.0.2

- إذا لم يوجد أي مفتاح اضطرارياً يُخزن في ntpserver

```
R(Config)# ntp server 192.168.1.1 prefer
```

- إذا كان يوجد مفتاح key من اختيار المدير

```
R(Config)# ntp trusted-key 1
```

- لـ association يتم تعيينه على المفتاح key

```
R(Config)# ntp max-association 1
```

- R(Config)# clock ?

summer-time time-zone hours offset from UTC
ex) R(Config)# clock time-zone EST 5
 # clock summer-time EST recutting

NetFlow (UDP)

- وظيفته مراقبة الشبكة وإلـ BW وتحليل traffic على مستوى حركة بيكو

- وكم شركات مثل alcatel و Huawei و H3C و juniper و Mikrotik

- ويقوم البروتوكول بجمع المعلومات وتخزينها في Flow Cache

- ثم timeout لها في Network Analyzer

- والغرض من push Netflow إلى SNMP والمراقبة

- بينما الثاني يقوم بعمل pull للبيانات

- والفرز الناتج من push يعتمد على العناصر نفسه مثل IP

- CPU RAM utilization traffic counts و resource errors

- traffic line areas classes Netflow

- ويعد الـ Netflow بمثابة محرر لبعض معايير التصفية

- src IP add Dest IP add

- src port for UDP or TCP Dest port for UDP or TCP

- IP add Ingress int IP Tos

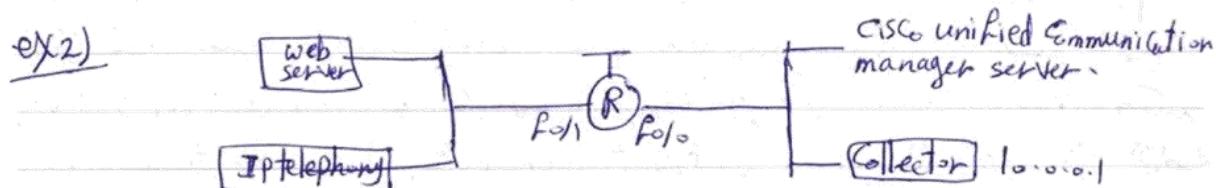
- ويعتمد على Netflow Versions

Ex 1



R2(Config)# int f0/0
 R2(Config-if)# ip route-cache flow
 R2(Config)# ip flow-export version 5 ← version 5
 R2(Config)# ip flow-export destination 10.0.0.1 2000
 النسخة لتحديد IP Collector الـ . وكذلك البوت الذي نستخدمه للدردشة
 لبيانات Netflow له يوجد له بورت معين

R2(Config)# ip flow-export source f0/0
 النسخة لتحديد source الذي ينبع منه المعلومات (Router/switch)



R (Config-if)# ip flow ingress ← F0/0, F0/1
 R (Config)# ip flow-export source loop 0
 #ip flow-export version 5
 #ip flow-export destination 10.0.0.1 5000
 في الحال السابقة تقوم برعاية كل فرقة من فرقة

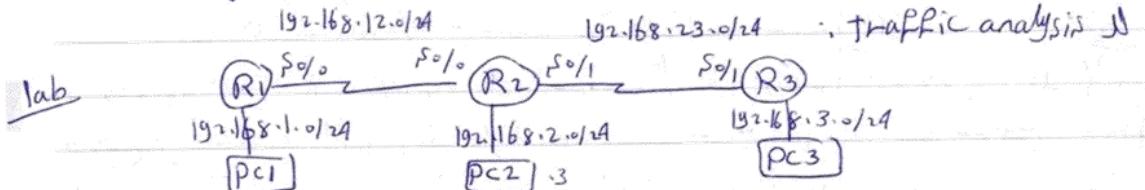
R (Config)# ip flow-cache timeout active 5
 النسخة لتحديد قيمة الـ timeout التي سُئل في
 timeout قبل أن تحدث

R (Config)# ip flow-cache timeout inactive 30
 R# show ip flow export
 R# show ip cache flow
 R# show ip cache verbose flow
 البرامج التي تدعم Netflow
 - sFlow Trend
 - Solarwind Netflow analyzer
 - Plixer Scrutinizer
 - Manage engine Netflow analyzer

int 11mz will traffic info to collect لبيانات Netflow
 int 11mz اول

Netflow

- * monitors the traffic through the router.
- IP accounting مراقبة L3 SW يرجع الى اوتوكور (will traffic line number) - ملخصات حركة النسخة
- customize ل CUSTOMIZE netflowing traffic و more flexible netflow و يوم



R2 (Config-if) # ip flow ingress { S0/0 & S0/1
ip flow egress

R2 (Config) # ip flow-export destination 192.168.2.3 9996

روزنه (روزنه) . standard portnum el (netflow) !!

R2 (Config) # ip flow-export Version 5g

R2 # show ip flow interface

. netflow (L1 لـ L2) int (النظام بالإنجليزية)

R2 # show ip flow export

Destination (1) 192.168.2.3 (9996)

Version 5g flow records

R3 → R1 new traffic for n (رسائل)

R1 # telnet R3 R3 # ping R1 repeat 1000

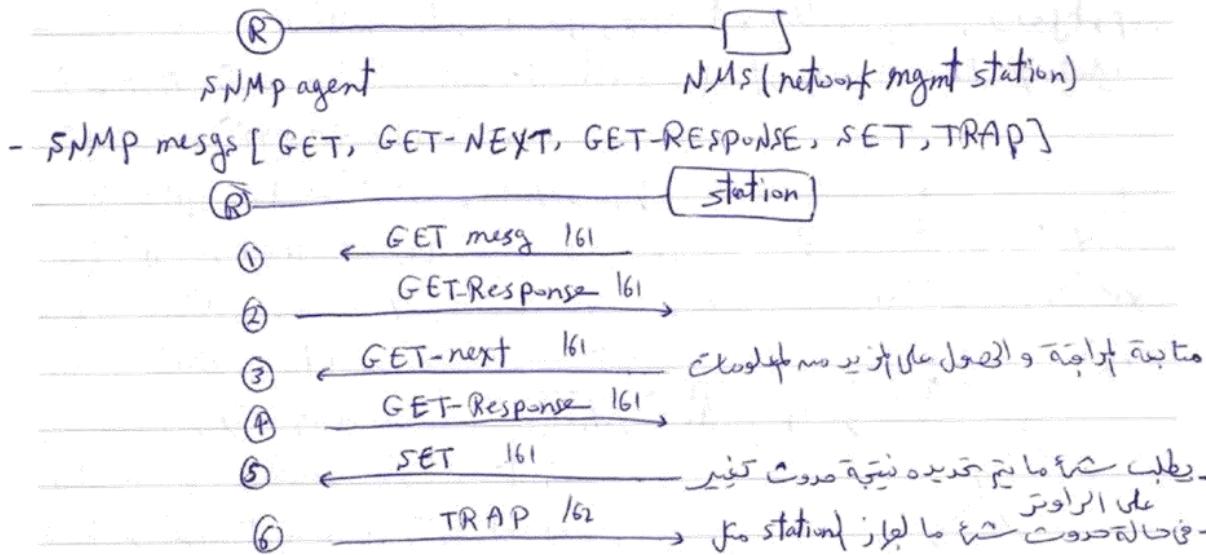
PC1 (browse to R3 (HTTP server))

R2 # show ip cache flow

R2 # clear ip flow stats

SNMP [L7 - UDP - port(161, 162)]

- بروتوكول لمراقبة الأجهزة وكماءد راسه بعد ذلك عمل
 (simple gateway mgmt protocol) SGMP
 (Secure Common mgmt info protocol) CMIP
 وجاء بعده بروتوكول آخر وهو
 وكتبه لم يسر على إنشاء SNMP .



- وفي البداية يعمم الرؤوس بوضع الـ (mgmt information base) MIB (info)

قبل ارسال الـ (management station)

(V1, V2C, V3)

- دينج جر SNMP 3 Versions

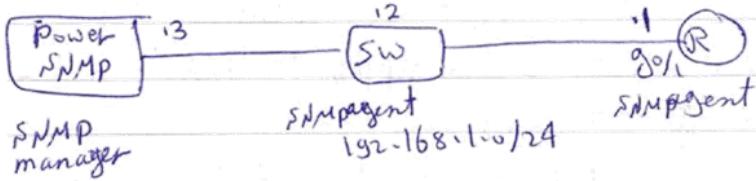
ما ينفع كل معلومات تكون بالخطأ
 Get-next في V2C
 authentication ، security في V3
 (V3 has authentication & encryption capabilities) ، access control و privacy و
 lab.



SNMP lab

- نقوم بـ تحديث IP (العنوان) من هنا في Power SNMP free manager

tools → Config → تحديث IP (العنوان)



R(Config) # snmp-server community CCIE to SNMP-ACL

snmp-server location SNMP-manager Comment

snmp-server contact abeer@cisco.com

snmp-server host 192.168.1.3 version 2c CCIE Key

snmp-server enable traps enable all default traps

ip access-list standard SNMP-ACL

permit 192.168.1.3

المزيد على البرنامجه new logo واذا لم يجدت بـ Power SNMP manager Discover Copy run start Community properties basic 192.168.1.255 version 2c SNMP obj navigator MIB download MIB locator page object navigator SNMP obj navigator obj ID OIDs و نقوم بـ تحويل او ID

SNMP (supported on almost all devices)
ex)

objectID

• OID ↴ object ID

R# show int fo/1
fo/1 is ^{OID} up, line protocol is ^{OID} up
^{OID} MTU=—, delay=—, ^{OID} BW=—

وسيقوم الـ router بارسال request لمعرفة حالة int

مثلاً يقوم الـ router بإرسال query كل OID كالتالي . ويجدر ذكر أن كل OID ينتمي لمجموعة (mgmt information base) MIB مثل OID ↴

* SNMP SW [mRTG(open src) - PRTG - Solarwinds - CiscoWorks]

* SNMP V2c → Community string clear text

* SNMP V3 → user based authentication - encryption - group based
+ group (sensors) | no need to change group

R(Config)# snmp-server community CISCO to

web-based application goes PRTG | the configuration

Devices → R click on local device and add device → automatic device identification

credentials for SNMP Device

(community) click → Continue

auto discovery | no need to change auto discovery