

شرح منهج شبكات سيسكو

CCNA

Cisco Certified Network Associate



2012

مذكرة

رقم : 4

المدرّب

م. خالد بيومي

إعداد

ياسر بن محمد ألفهيد

ALFAHAID@GMAIL.COM

تم الإعداد في : 1429 هـ / 2008 م

تم النشر في : 1433 هـ / 2012 م

:: مذكرة ملخصة من دورة تدريبية ::



أهدي هذا العمل :

- إلى كل شاب طموح يعشق العلم والتعلم ويهمه بناء نفسه وتقدم مجتمعه ورفعة وطنه وأمته.



ثمن هذا العمل :

- هو دعوة بظهر الغيب بالتوفيق في الدنيا والآخرة لأخيكم الفقير والراجي لعفوه ربه .



مقولة أعجبتني :

- " طموحاتي الكبرى بعيدة جدا مثل الشمس ، قد لا أستطيع الوصول إليها ولكن يمكنني النظر لأعلى لرؤية جمالها ، والإيمان بها ، ومحاولة السعي وراءها حيث تقودني " (ألكوت)

للإطلاع على باقي الأوراق والمذكرات المنشورة
في مفضلتي على حساب تويتر



@ALFahaid

<https://twitter.com/ALFahaid>

تخوي حتى الآن : 18 ورقة و 3 مذكرات

أو عبر دروب بوكس Dropbox على الرابط

<https://www.dropbox.com/sh/s9xdu87q5r73q2r/MjqYNGCI7N?%20m>

وَاللَّهُ يَحْفَظُكُمْ وَيَرِثُ عَالِكُمْ

المحتويات

The Contents



Ch1:	Introduction To Network	4
Ch2/3:	IP Subnetting	7
Ch4:	Cisco Router	9
Ch5/6:	IP Routing	12
Ch7:	Access Lists [ACL]	18
Ch8:	Managing Cisco IOS Software	21
Ch9:	Switching [Layer 2]	24
Ch10:	Virtual LANs [VLAN]	26
Ch11:	Network Address Translation [NAT]	29
Ch12:	Wireless LAN [WLAN]	31
Ch13:	Internet Protocol Version 6 [IPv6]	33
Ch14:	Wide Area Networking [WAN]	37

Chapter: 1

Introduction To Network

What's Network ? تعريف الشبكة

Network is a group of computers connected with others to **share data**.

مجموعة من الحواسيب متصلة مع بعضها لمشاركة البيانات

Types of Network: أنواع الشبكات

1. (LAN) Local Area Network أكتب أوامر	الفرق بين LAN و WAN :
2. (WAN) Wide Area Network	1- المساحة الجغرافية
3. (MAN) Metropolitan Area network	2- ال Service وهي الخدمة لنقل البيانات.. مثل: leas line/frame relay/ATM
4. (SAN) Storage Area network	تغطي مدينة ((وغير مطبقة في السعودية))
5. (VPN) Virtual Private Network	شبكة خاصة للسيرفرات (توجد داخل LAN)
6. Intranets and Extranets. فرقها عن LAN أضغط على روابط للأوامر	طريقة التواصل بين شبكتين LAN في مكانين بعيدين : VPN-1 Dial up -2 أعلى مع أنها أكثر Security
	Intranets معناها انترنت داخلية و Extranets انترنت خارجية

شرح إضافي لل SAN

الفائدة من SAN هو Disaster Recovery والذي يقوم بـ:	وظيفتها هو ربط السيرفرات لكن يجب أن يتوفر:
1- عمل نسخة احتياطية Backup	1- Cluster service
2- توزيع الأحمال Load Balance	2- High speed internet

شرح إضافي لل VPN

نوعين يتصلون بال LAN الأصلية



باستخدام VPN

في الإنترنت راح نستخدم شيء اسمه Tunnel لكي نحافظ على البيانات من الاختراق

NIC = Network Interface Card

DNS → IP رقم الموقع إلى اسم الموقع

ARP = Address Resolution protocol

ARP → IP إلى MAC تحويل

RARP → IP إلى MAC تحويل

Logical × مادي Physical

Virtual × افتراضي real

رقمه	وظيفته	اسم البروتوكول	م
343	تصفح + تشفير للبيانات	HTTPS	1
80	تصفح + بدون تشفير للبيانات	HTTP	2
20/21	رفع / تحميل الملفات	FTP	3
25	إرسال للبريد	SMTP	4
53	تحويل اسم الموقع إلى أرقام	DNS	5
23	الإدارة من بعد	TELNET	6

OSI-RM [Open System Interconnection – Reference Model] :

م	OSI-RM	أسماء الداتا عند الانتقال	Protocol		Device	الوظيفة	TCP/IP
7	Application	data	HTTP-FTP-SMTP DNS-TELNET HTTPs-POP3		-	Interface between app & protocol	(1) Application
6	Presentation	data			-	-compressionضغط -conversionتحويل -encryptionتشفير	
5	Session	data			-	-monitorمراقبة open session on the host	
4	Transport	Segments	TCP HTTP-FTP DNS- TELNET	UDP TFTP-DNS DHCP	-	Delivery method مسئول عن عملية التوصيل	(2) Transport
3	Network	Packets	IP – ARP		1-Router 2-Switch[L3]	Provide logical address [address for delivery on network]	(3) Internet
2	DataLink	Frames	LAN & WAN TECHNOLGY		1-Bridge 2-NIC 3-Switch[L2]	Provide physical address [MAC]	(4) Network Access
1	Physical	Bits			1-Hub يستخدم لتوصيل الأجهزة 2-Repeater يستخدم لتكبير الإشارة	000011011 000111111	

- ال OSI-RM نموذج عام ومن تطبيقاته وأمثله : 1-TCP/IP 2-IPX/SPX 3-Apple Talk
- **TCP**= Transmission Control Protocol [Reliable method] **UDP**= User Datagram Protocol [Unreliable method]
- كل طبقة له خاصية الاتصال مع الطبقة الأعلى منها والطبقة الأسفل منها فقط.
- البروتوكول هو مجموعة من القواعد والخطوات التي تعرف لي عملية الإرسال والاستقبال (مثل واحد يتكلم عربي والثاني يتكلم انجليزي لازم يكون هناك لغة موحدة) .
- الدخول عن طريق الأوامر للجهاز الآخر [Start->run->\\اسم الجهاز] OR [Start->run->\\IP address]
- كل شيء احتاج أعمله داخل الشبكة احتاج Protocol
- أقصى مسافة لجهاز Repeater هو (2.5K) ومعناه احتاج إلى (4Reapater) لأن كل Repeater مسافته 500M.
- ميزة Switch عن Hub هو وجود mac table الذي يوفر باندويث
- نفس الشيء : MAC table = CAM table = Bridging table (CAM= Content address memory)
- الراوتر يستخدم في توصيل الشبكات وليس في التوصيل بين الأجهزة.

شكل الشبكة	Network Topology	(مسار الداتا للوصول إلى الهدف)
مادية	Physical topology	منطقية
		Logical topology

Network Topologies [Physical]: أشكال الشبكة المادية:

النوع	الميزة	العيب
1- Bus	سهولة في التطبيق	لو حصل مشكلة في الخط الرئيسي راح تكون مشكلة في الشبكة كاملة
2- Star	سهولة في التطبيق	لو حصل مشكلة في center point راح تكون مشكلة في الشبكة كاملة
3- Extended		
4- Ring	ما يحصل تصادم للداتا No collision	
5- Mesh		

Network Media : أنواع الوسائط في النقل

1- Copper نحاسي					2- Fiber Optical الألياف الضوئية	3- Wireless لاسلكي
Coaxial cable		زوج ملفوف [TP] Twisted Pair cable				
Thick	Thin	STP	ScTP	UTP		
المسافة القصوى=500متر السرعات=1000/100/10	المسافة القصوى=185متر السرعات=100/100/10mbps	Shielded TP استخدم هذا الكابل إذا كان يمر بمنطقة توليد موجات ليحميها	Screened TP	UnShielded TP هذا المستخدم في المعامل والشركات	* للشرح التفصيلي شاهد صفحة رقم : (32)	

* للشرح التفصيلي
شاهد صفحة رقم :
(32)

100 Base T		
الباندويث BW	أرضي Baseband و عكسها الفضاء Broadband	المسافة

Ethernet Cabling :

- 1- Straight-through cable ويستخدم للأجهزة المختلفة
- 2- Crossover cable ويستخدم للأجهزة المتشابهة
- 3- Rolled cable (Router=>Host) ويستعمل لعمل Config للراوتر فقط مع الهوست (دسكتوب أو لابتوب)

قاعدة	
Host & Router	أجهزة متشابهة
Switch & Hub	أجهزة متشابهة

أنواع Console cable	
1-Rollover (منفذ شبكة => منفذ شبكة) RG45 RG45	2-adapter (منفذ شاشة => منفذ شبكة) RG45 DB9

- وللعلم فإنه يوجد منفذ اسمه (console port) ليس له علاقة باسم الكابل.

Chapter: 2/3

IP Subnetting

* What Is a Subnet?

A subnet is a physical segment of a network that is separated from the rest of the network by a router or routers.
هي باختصار عندما يتم تقسيم الشبكة إلى أجزاء فإن الجزء الواحد يسمى سب نتينق

* The benefit from subnet :

- 1- المحافظة على البانديث
- 2- التعرف على المشكلة بسهولة

* IPv4 :

- 1- 32 bits.
- 2- Decimal number representation 10.10.1.0 : مثال
- 3- Dotted decimal -.-.- 4 octets and every octet consist of 8 bits

Rules : القواعد لاختبار IP يصلح أو لا

- 1- $0 \leq \text{octet} \leq 255$
- 2- $1 \leq \text{octet} 1 \leq 126$ or
 $128 \leq \text{octet} 1 \leq 191$ or
 $192 \leq \text{octet} 1 \leq 223$
- 3- all host bits must not = 0 → broadcast = لو كانت كلها أصفار بتكون
all host bits must not = 1 → network address = لو كانت كلها واحدات بتكون

**** number 127 → Trouble shooting عملية

IP			
فيه جزئين 10.10.1.0			
Network ID بنعرف ال IP يعني ال host موجود في أي شبكة Subnet		Host ID بيعرفني سعة الشبكة capacity of network	
Subnet Mask هي اللي بتفرق لي بين network ID & Host ID			
Network address	اللي Valid range	Broad cast	

Class A	1 - 126	Used for network هذا اللي نتعامل معه في الشبكات
Class B	128 - 191	
Class C	192 - 223	
Class D	224 - 239	Multicast Video – Audio
Class E	240 - 254	Future

* ال octet الأول هو الذي يحدد نوع الكلاس

Subnet Mask (SM)

مثال على السب نت ماسك

192.168.0.1/24 → 255.255.255.0

Rules : لاختبار أي subnet mask يصلح أو لا

- 1- لما يظهر بعد الواحد صفر يجب أن يكون الباقي أصفار

يعني راح تكون كل الأرقام الممكنة في السب نت ماسك هي
0 or 255 or this number only

0000	0000	0
1000	0000	128
1100	0000	192
1110	0000	224
1111	0000	240
1111	1000	248
1111	1100	252
1111	1110	254
1111	1111	255

class	Default SM
Class A	255.0.0.0 / 8
Class B	255.255.0.0 / 16
Class C	255.255.255.0 / 24

IP		
Network ID		Host ID
هو الجزء في IP المقابل للواحدات في SM		هو الجزء في IP المقابل للأصفار في SM

القوانين

المستخدمة في IP

1-

أقدر استخدمه إذا طلب: 1- سعة الشبكة (أي عدد الأجهزة الممكنة) 2- السب نت ماسك SM	عدد الأجهزة $\text{Number of Host} = 2^n - 2$ $n = \text{number of host bits}$ or $= \text{number of zero bits}$ يعني عدد الأصفار الموجودة في SM	هذا عدد الواحدات /28 $2^n = \text{Number of Host} + 2$ $2^8 \quad 2^7 \quad 2^6 \quad 2^5 \quad 2^4 \quad 2^3 \quad 2^2 \quad 2^1 \quad 2^0$ 256 128 64 32 16 8 4 2 1 اكتبه في الاختبار
--	--	---

هنا انتبه تتعامل مع الأصفار

2-

أقدر استخدمه إذا طلب: 1- ال SM 2- عدد الشبكات	عدد الشبكات (الفرعية) $\text{Number of Subnets} = 2^y$ (default) Y = new SM (عدد الواحدات) - old SM (عدد الواحدات) new SM = Y + old SM	لو عطاني في الاختبارات Subnet Mask استخدم هذا القانون والذي قبله * لازم يعطيك معلومتين في السؤال
---	--	---

هنا انتبه تتعامل مع الواحدات

3-

أقدر استخدمه إذا طلب 1- IP valid or not 2- valid rang 3- network address 4- broadcast	أي شيء خاص بالادرس استخدم هذا القانون $\text{Block size (BS)} = 256 - [\text{أي عدد موجود في سب نت ماسك غير 0 و 255}]$ للتسهيل : لو كانت قيمة BS صغيرة وقيم octet في IP address كبير أخذ قيمة octet في الادرس وأقسمه على قيمة BS الناتج أضربه في قيمة BS وبعدا أخذ العدد الصحيح وهو اللي راح يحدد لي النت وورك ادرس point-to-point → /30 دائما	255.255.255.142 يعني في الادرس ناخذ الرابع 192.7.8.70 لو عطاني في الاختبارات Address استخدم هذا القانون
---	---	--

إذا كان SM ما فيه رقم غريب عن 255 & 0
فهنا ما نستخدم قاعدة BS بل نستخدم هذه الجدول مباشرة

	Network address	Broadcast	Valid rang
/8 →	X.0.0.0	X.255.255.255	X.0.0.1 X.255.255.254
/16 →	X.Y.0.0	X.Y.255.255	X.Y.0.1 X.Y.255.254
/24 →	X.Y.Z.0	X.Y.Z.255	X.Y.Z.1 X.Y.Z.254

إذا كان يوجد أكثر من subnet mask في الشبكة (على الراوتر) تسمى :

VLSM

Variable Length Subnet Nask

إذا كان يوجد وحده subnet mask فقط في الشبكة (على الراوتر) تسمى :

Non VLSM

* وإذا كان يوجد أكثر من subnet mask وأكثر من class تسمى DisContiguous <==

* وإذا كان يوجد أكثر من subnet mask وواحد class تسمى Contiguous <==

Summarization

Larger Network address – smaller Network address =

مثال : عطاني شبكة وفيها أكثر من IP

172.16.1.0/24 - 172.16.2.0/24 - 172.16.3.0/24

أطرح الصغير من الكبير

$\begin{array}{r} 172.16.3.0 \\ 172.16.1.0 \\ \hline 0 \quad 0 \quad 2 \quad 0 \\ 1\text{bit} + 8\text{bit} = 9\text{bits} \\ \text{sm} = 24 - 9 = 15 \end{array}$ <p>وراح يكون السب نت ماسك الجديد كالتالي :</p>	$2^8 \quad 2^7 \quad 2^6 \quad 2^5 \quad 2^4 \quad 2^3 \quad 2^2 \quad 2^1 \quad 2^0$ 256 128 64 32 16 8 4 2 1
---	---

* يمكن تحديد ال Host ID و Net ID من خلال السب نت ماسك وال Net ID يحدد لي هذا الجهاز أين يقع .

* ممكن أن يتشابه السب نت ماسك في كل سب نت وممكن يختلف

* إذا عطاني السب نت ماسك القديمة أناظر في الأدرس IP وأطلع منه أي كلاس (طبعاً من خلال octet الأول).

Chapter: 4

Cisco Router

Router			
External component			Internal component
Interface			1- mother board 2- Rom – Ram 3- Flash memory 4- NVRAM 5-Non Volition RAM 6- CPU 7-power supply
LAN	WAN	Config port	
E F G 10G 10 100 1000 10000	-serial (lease line/frame relay) - ISDN(BRI/PRI) -ATM(ATM)	-console - auxiliiy	
Subnet ⇄ subnet	LAN ⇄ LAN WAN ⇄ WAN		

Internal component المكونات الداخلية

1- ROM (الرقم السري لما أنساه)

- a) store boot strap protocol & post
- b) Rommon (Ram monitor) for trouble shooting
- c) mini IOS

2- Flash memory فائدتها : أأزن عليها

- store IOS Image

3- RAM فائدتها : 1- تخزين IOS المفكوك 2- تخزين الإعدادات الحالية

- store decompressed version of IOS Image
- store running config

4- NVRAM ذاكرة لا تتطاير

- store startup config

Tow type from config :

1- Running config الراوتر شغال

2- start up في وقت عملية ال boot up للراوتر

Router			
Interface			Routing table
LAN	WAN	Config port	Static Dynamic Routing Protocol Interior Exterior Distance Victor Link state Hybrid Ex: -RIP -IGRP Ex: -OSPF Ex: -EIGRP Ex: -BGP

* نظام التشغيل المستخدم للراوترات [IOS [Internetwork Operating System] :

وأحيانا يسمى : IOS image OR image

و يمكن نعمله Reinstall – upgrade

* امتداد ملف نظام التشغيل : *.bin

طرق تشغيل الراوتر :

م	الطريقة	إضافة
1	باستخدام Console Session (كيبل لونه أزرق) يستخدم لما يكون الراوتر جديد	يحتاج اتصال مباشر لجهاز الكمبيوتر وشخص يعمل عليه
2	باستخدام Auxiliary Session (كيبل لونه أسود) يستخدم لما يكون الراوتر جديد	استخدمه لو كان الشخص اللي راح يعمل config خارج الشبكة (ما يحتاج اتصال مباشر) في فتحة Aux تشبك كيبل اسمه console منفذ شاشة ⇄ منفذ شبكة
3	باستخدام Telnet Session (يستخدم لما يكون الراوتر له IP أي معمول له Config سابق فقط	

Method for config router		
CLI		SDM
Command Line Interface		Security Device Manager
Command		GUI

خطوات تشغيل الراوتر Boot up Router

تحميل هذا البروتوكول	1	Boot strap ROM وهذا موجود في ال	هذا البروتوكول ليقوم الراوتر للعمل
تشغيل	2	Run post [Power on self test]	يتأكد من سلامة المكونات الداخلية للراوتر
تحميل نظام التشغيل	3	Load Image [IOS] flash يحملها من	
يفك الضغط ويخزن في الرام	4	Decompress Image & store decompressed IOS into Ram	
يعرض معلومات	5	Display information from post program	
تحميل الconfig	6	Load configuration content from NVRAM	اسمها start up

لو ما لقي شيء في NVRAM (وهذي تصير لما يكون الراوتر جديد) فعندها راح يشتغل من setup mode

*لك خيارين عند استخدام setup mode :

1- Basic management

2- Extended setup

* مودم DSL هو سويتش لكنه يسوي عملية راوتينج (فالسلك عادي)

Any [pc] on the network and has IP
Host [client // server]
End user نفس المستخدم
End system نفس الجهاز
Edge or interface port or router or hub [terminal] نهاية أو حد

Commands	
Router>	User Mode
Router>enable OR en	تفعيل الراوتر
Router#	Privileged Mode
Router#disable تعطيل الراوتر	You can go back from privileged mode into user mode by using the disable command.
Router>	
Router#config t الدخول للخصائص-عام	Terminal (any changes save in DRAM)
Router(config)#	Memory (any changes save in NVRAM)
	Network (any changes save in TFTP or FTP Server)
Router(config)#int f0/0 الدخول للخصائص-خاص	Int = interface , f= fastethernet
Router(config-if)#	
Router(config-if)#exit للخروج من الخصائص-خاص	
Router(config)#end OR ^Z للخروج من الخصائص-عام	
Router#	
Router#? إذا ما عرفت تكمل الأمر ممكن تستخدم علامة الاستفهام	Editing and Help Features
Router#conf ?	إذا ضغطت (Enter) يظهر الكتابات سطر سطر
	إذا ضغطت (Space) يظهر الكتابات صفحة صفحة
Router#config t	"Hostname"
Router(config)#host yaser	
yaser(config)#	
Router(config)#banner motd \$ ((motd= Message of the day))	Banners هي طريقة للمعرفة وللتذكر من المدير عن عمل رواتر معين .. ونضع علامة غريبة في النهاية لالتهاء مثل \$ لرويتها ارجع ثم اضغط Enter
Hello. This router for center control \$	

Router#show run <i>static route إدخال</i> Router(config)#do sh run Router#show history Router#sh start	Privileged Mode لازم يكون في Privileged Mode config وضع هذا الأمر يعرض آخر 10 أوامر يعرض معلومات ال Config
Router1#copy run satart Router2#copy run satart Router1#erase start Router2#erase start	هذا الأمر يحفظ ال config للراوتر في NV-RAM هذا الأمر للإزالة Delete the startup-config
Routr(config)#enable password RRRRR باسورد غير مشفر Routr(config)#enable secret RRRRR باسورد مشفر Routr(config)#NO enable password Routr(config)#NO enable secret	1- هذا الرقم السري للدخول من حالة User Mode إلى Privileged Mode بطريقة مشفرة أو غير مشفرة لإزالة الرقم السري نضيف NO قبل الأمر نفسه
Routr(config)#line cons 0 // aux 0 // vty 0 4 (telnet معناها) Routr(config-line)#pass RRRRR Routr(config-line)#login Routr(config-line)#exec-timeout 5 7	2- لعمل حماية على console و Auxiliary و telnet وبكذا قبل الانتقال من مرحلة User Mode إلى Privilege Mode راح يطلب رقم سري آخر سطر معناه وقت معين وينتهي وقت ادخال الرقم السري 5= دقائق و 7=ثواني (لو حط 0 0 فماراح ينتهي الوقت أبدا)
Routr(config)#enable password RRRRR باسورد غير مشفر Routr(config)#enable secret RRRRR باسورد مشفر Routr(config)#NO enable password Routr(config)#NO enable secret	هذا الرقم السري للدخول من حالة User Mode إلى Privilege Mode بطريقة مشفرة أو غير مشفرة (هنا وضع ما يسمى Privilege password) لإزالة الرقم السري نضيف NO قبل الأمر نفسه
Router#sh run Router(config)#service password-encryption Router(config)#no service password-encryption	طريقة وخدمة لتشفير الأرقام السرية التي تم ادخالها Encrypting Your Passwords (To cancel previous command)
Router(config)#int f0/0 Router(config-if)#desc Sales Lan	هذي طريقة لوصف نفس البورت بحيث يسهل للمدير معرفة البورت وعمله بسرعة وسهولة Descriptions
[1] Router>en Router#conf t Router(config)#int f0/0 AND f0/1 Router(config-if)#no shut [2]Router(config-if)#ip add 10.10.10.100 255.255.255.0	To config any router interface you must do this steps: Interface configuration Add = address هنا خطوات تفعيل وتشغيل فتحة الراوتر
[3]Router(config)#int s0/0 Router(config-if)#no shut Router(config-if)#ip address 10.10.20.1 255.255.255.0 Router(config-if)#clock rate 64000	Serial Interface Commands لو كان السريل DTE ما نكتب السطر الأخير (هذا الافتراضي) لو كان السريل DCE نكتب الأوامر كاملة (السرعات) Data circuit equipment //// Data terminal equipment
Router#ping 10.10.10.1 Router#sh int f0/0 يعرض معلومات عن الكونفيغ Router#sh ip int Router#sh ip int brief Router#sh controllers serial 0/0 Router#sh ip route	Verifying Your Configuration؟ الاختبار الشبكة هل هي تعمل أولا ؟ الكيبل والأشياء الفيزيائية تعمل Up= يعرض كل ال interface وهل تعمل وهل لها ip أو لا ؟ يعرض interface مخصص هل تعمل وهل لها ip أو لا ؟ لاستعراض السريل هل هو DCE or DTE يعرض ال routing table
Router(config)#int f0/0 Router(config-if)#ip address 10.10.1.100 255.255.255.0 Router(config-if)#no shut Router(config)#ip domain-name xp Router(config)#crypto key generate rsa general-keys modulus 1024 Router(config)# ip http server Router(config)# ip http secure-server Router(config)# ip http authentication local Router(config)# username a privilege 15 password 0 a	SDM you must configure السطر هذا والذي بعده فقط إذا أردت تشغيل http OR https حرف A هو أي اسم مستخدم وكلمة مرور و 0 تعمل للتشفير

Chapter: 5/6

IP Routing

DHCP يعطي IP أوتوماتيك
الجديد DNS والقديم WINS

Routing	Routed	Route	Router
يبنى الجدول	يبنى الباكيت	المسار	نفس الجهاز

* طريقتين للتوجيه route types : 1- Static 2- Dynamic

Static -1

مميزات:

1- ما يحتاج راوتر ذو إمكانيات هائلة 2- أكثر Security 3- المحافظة على البانديوث بين الراوترين

عيوب:

1- للشبكات الصغيرة فقط 2- إذا حصل تغيير فيكون عمل مجهد على admin 3- حصول أخطاء أكبر

طريقة الربط بين راوترين وكل راوتر على شبكتين tow LAN	
أولاً : عمل Config في الراوتر الأول ليعرف Subnet 3 and 4 الموجودة في الراوتر الثاني	
R1(config) #IP^route^10.10.3.0^255.255.255.0^10.10.5.2	
R1(config) #IP^route^10.10.4.0^255.255.255.0^10.10.5.2	
ثانياً : عمل Config في الراوتر الثاني ليعرف Subnet 1 and 2 الموجودة في الراوتر الأول	
R1(config) #IP^route^10.10.1.0^255.255.255.0^10.10.5.1	
R1(config) #IP^route^10.10.2.0^255.255.255.0^10.10.5.1	
وللإلغاء أضغ NO قبل الأمر .. وللتأكد R1&2#sh^ip^route سيظهر لك C وهي الأهم	
Stub network = network has one exit interface	
يمكن استخدام Default Route ولو أنا ما أعرف ال IP للجهة الأخرى	
R1(config)#IP^route^0.0.0.0^0.0.0.0^10.10.5.1 ونفس الشيء في الراوتر الثاني	

Router#tracert 10.10.3.1 هذا على مستوى الراوتر	تتبع مسار البكت من المصدر وحتى مكان الوصول وتعرف مكان المشكلة لو حصلت From recourse to destination
Router#tracert 10.10.3.1 هذا على مستوى الهوست	
Ping هو أمر يخبر عن وجود اتصال أو لا بدون تحديد مكان المشكلة لو فيه	

-2 Dynamic

هنا معناه استخدم مجموعة من البروتوكولات

الفرق بين	
Routing protocol	Routed protocol
- ptotocol used for building routing protocol .. ex:RIP-EIGRP-OSPF	- protocol used for building packet hat need to be routed .. ex:TCP/IP-IPX/SPX-Apple talk
بيعمل ال Forwarding table	هو بيعمل البكت أصلاً

الأنظمة المستقلة (AS) "autonomous systems"

- هو تقسيم وتوزيع المسارات في الراوترات إلى أجزاء صغيرة لأحافظ على البانديوث ويشبه عملية ال subnetting كما يهدف إلى المحافظة على resource في الراوتر مثل ال ram وغيره

- ممكن تضع رقم AS من 1 إلى 65000

- #(Exterior)Inter-AS = AS خارج AS داخل AS = # (Interior) Intra-AS

Gateway router : Direct link to router in another AS

Routing table				
Static	Dynamic			
	Routing Protocol			
	Interior			Exterior
	Distance Victor	Link state	Hybrid	
	Ex: -RIP -IGRP (for Cisco)	Ex: -OSPF	Ex: -EIGRP	

Interior protocol [details] بروتوكولات داخلية						
Routing Protocol	kind	*AD	تعمل على	**Num	***Algorithm	ملحوظات
Distance Vector	RIP	120	Open	15	BellManford	Small network
	IGRP	100	Cisco Only	255	BellManford	Large network وهذا أصبح غير موجود
Hybrid	EIGRP	90	Cisco Only	255	Dual	Large network Protocol RTP
Link State مخلوط بين الأول والثاني	OSPF	110	Open	No limit	Dijkstra	Large network
	IS-IS					

*AD= administrative distance يستخدمها الراوتر في المفاضلة بين الطرق ويأخذ الأقل وإذا كان متساوي يشوف الcost وهو عبارة عن hop count	**Max hop count كم أقصى راوتر يمكن أن يصل إليه	فائدته هو اختيار Best path selection
--	---	---

فائدته لو ما جاء ack من راوتر معين راح يرسل له unicast لذلك الراوتر **Protocol RTP:**

* Distance Vector Routing[RIP/IGRP]:

1. Max hop count
2. split horizon تقنية تمنع اللوب بحيث ما يعيد إرسال المعلومة إلى مصدر المعلومة
3. Route poisoning تقنية بحيث لما تغلق أو تطيح شبكة معينة يعطي +1
4. holddown timers ينتظر لفترة زمنية ثم يبحث

Convergence time زمن التقارب

الوقت الذي يأخذه الراوتر لبناء Routing table

[1] Routing Information Protocol (RIP) [Distance Vector]

RIP v1	RIP v2
Classful Routing معناه بيعث net add بدون SM	Classless Routing
No support for VLSM أي لا يدعم السبنت ماسك المختلفة	Support for VLSM
No support for discontinuous networks أي لا يدعم السبنت غير المتصلة (المختلفة)	Support for discontinuous networks
Use broadcast	Use broadcast or multicast-D تستخدم في كلاس

contiguous	
VLSM	FIXED LENGTH SM

discontiguous	
VLSM	Non VLSM

* RIP Timers types :

1. **update timer:** (30 seconds) معناه كل فترة زمنية يبعث تحديثات لجاره
2. **invalid timer:** (180 seconds) لو ماجاني تأكيد خلال هالمدة راح يلغي المعلومة
3. **flush timer:** (240 seconds) نفس اللي قبله لكن هذا إذا انتهت 240 ثانية وما جاء تأكيد راح يمسخها من Routing table
4. **Holddown timer:** (180 seconds) خاصة ب.....

Configuring RIP Routing

```
R1#config t
R1(config)#router rip
R1(config-router)#net^10.10.1.0
R1(config-router)# net^10.10.2.0
R1(config-router)# net^10.10.5.0
R1(config-router)#ver^2
R1(config-router)#^z ==> [control + z] معناها هنا
R1# sh^IP^route
R1#debug^IP^RIP
```

ونفس الطريقة بالضبط نعملها في الراوتر الثاني مع تغيير فقط رقم السبنت (وهي المضلل عليها هنا)
- ملاحظة مهمة : تكتب الشبكات اللي على الراوتر وليست اللي في الجهة المقابلة

لنقلها إلى V2 للاستفادة من الخواص التي يقدمها وافترضني V1 يشغل

تعلمني الباكيت اللي يرسلها ويستقبلها

passive-interface

```
Router#config t
Router(config)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#passive-interface s0/0
```

[2] Interior Gateway Routing Protocol [IGRP] [Distance Vector]

بروتوكولات خاصة بـ EIGRP و IGRP وهذا أصبح غير موجود حالياً

IGRP
Classful Routing
No support VLSM
No support discontinuous networks
Uses an autonomous system number لازم يكون نفس رقم AS علشان الشبكة تشوف بعضها
Use broadcast
Cisco

* IGRP Timers types :

5. **update timer:** (90 seconds)
6. **invalid timer:** (270 seconds)
7. **flush timer:** (630 seconds)
8. **Holddown timer:** (280 seconds)

Configuring IGRP Routing

```
R1#config t
R1(config)#router igrp 10
R1(config-router)#net 10.10.1.0
R1(config-router)#net 10.10.2.0
R1(config-router)#net 10.10.5.0
R1(config)# no router igrp 10
show ip protocols يعرض أي بروتوكول شغال داخل الراوتر
debug ip igrp events الباكيت اللي أستقبلها وأرسلها
debug ip igrp transactions الأحداث التي تحدث الآن في الوقت الحالي
```

same RIP with one important difference: you use an autonomous system(AS) number (Here 10) .

- ونقوم بتطبيق نفس الخطوات على الراوتر الثاني

To Delete routing table built by IGRP

[3] Enhanced Interior Gateway Routing Protocol [EIGRP][Hybrid]

* البروتوكولات المختلفة التالية (TCP/IP - IPX/SPX - APPLE TALK) يستطيع التعامل معها EIGRP فقط

EIGRP
Classless Routing
support VLSM
support discontinuous networks
Uses an autonomous system number
Cisco

Communication via Reliable Transport Protocol (RTP)

* Build three table :

- 1- Neighbor table وهي أن الراوتر يعرف ما هي جيرانه من الراوترات
 - 2- Topology table هنا توجد معلومات من الجيران واللغات التي تشتغل هنا
 - 3- Routing table هنا آخر شيء وفيه أحسن المسارات للراوتر
- وأحسن مسار يسمى *successor route* وثاني أحسن مسار يسمى *Feasible successor*

Load Balance: خاصية توزيع الأحمال و البيانات للمسارات الفاضية

Configuring EIGRP Routing	
<ul style="list-style-type: none"> • Configuring Discontiguous Networks <p>R1(config)#router eigrp 100 255 R1(config-router)#net 10.10.1.0 R1(config-router)#net 10.10.2.0 R1(config-router)#net 10.10.5.0 R1 (config-router)#no auto-summary</p> <ul style="list-style-type: none"> • To make manual summarization <p>Router(config)#int s0/0 Router(config-if)#ip summary-address eigrp 10 192.168.10.64 255.255.255.224</p>	<p>وبعدين نسوي حفظ وحفظ باسم ونفس الشيء نطبقه على الراوتر الثاني مع تغيير رقم السب نت</p> <p>لو كانت الشبكة EIGRP و discontinuous فاته راح يستخدم Auto summarization وفائدته يرجع السب نت ماسك إلى أصلها على حسب IP مثل : $10.10.1.0 \Rightarrow \text{السب نت ماسك } /8$ $172.16.0.0 \Rightarrow \text{السب نت ماسك } /24$ وعلشان ألغية أكتب ...no</p>
show ip route	Shows the entire routing table
show ip route eigrp EIGRP يعرض الطرق العمولة بـ	Shows only EIGRP entries in the routing table
show ip eigrp neighbors neighbor يعرض	Shows all EIGRP neighbors
show ip eigrp topology Topology table يعرض	Shows entries in the EIGRP topology table

* ال Auto summary تكون سبب discontinuous وهو اختلاف subnetmask

[4] Open Shortest Path First [OSPF] [Link State]

OSPF
Classless Routing
support VLSM
support discontinuous networks
Uses an autonomous system number Area ويقسمها إلى أقسام ووحدات صغيرة تسمى Area ولها مصطلح يسمى Back bone وهي Area 0 - العمود الفقري ومن أهم فوائده يقلل Convergence time
Support IP only.
Manual Summarization.
Use Wild mask [inverse sm] [Wild card mask] وهو قلب الواحدات إلى أصفار وقلب الأصفار إلى واحدات

* ملاحظة مهمة : ال OSPF يستخدم Wild Mask ولا يستخدم Subnet mask
 * config OSPF لازم يكون في area 0 وتسمى Backbone
 * S3 [AD/cost]

طريقة حساب Wild Mask مباشرة ... مثلا :

/28 → 255.255.255.240
 255.255.255.255

 0 . 0 . 0 . 15

* Build three table :

- 1- Neighbor table
- 2- Topology table
- 3- Routing table

$$\text{Cost (metric)} = \frac{100,000}{\text{BW [kilo]}}$$

Router ID (RID): is the highest IP address used to identify the router. [Identification] أعلى IP
Link is an interface on a router.

Link-State: the status of link between two routers حالة اللنك

Link-state database (topological database).

Area: جزء من AS ويحصل تبادل بين بعضهم البعض

Routing table: يعني أحسن المسارات مسجلة في الراوتر

Adjacencies router : DR and BDR neighbor router يعني الراوتر يبعث فقط للراوترات الرئيسة ونائبه

Designated router (DR): يعتبر مثل الرئيس

backup designated router (BDR): يعتبر مثل نائب الرئيس

DR election based on: (طبعا الهدف من وجودها هو تقليل الباندويث) طرق انتخاب DR و BDR

- 1- Priority [highest] (أعلى أهمية = 255) بالافتراضي تكون 1 على الراوتر
- 2- RID [highest] أعلى IP يأخذه الراوتر

DRouter وباقي الراوترات (باقي الشعب) يسمى

في حالة Point-to-Point لا يوجد انتخاب DR و BDR

DR & BDR يكون عند انتخاب

- Multiaccess Broadcast Net [Ethernet : مثالها]
- Multiaccess NonBroadcast Net [Frame Relay : مثالها]

Configuring OSPF Routing

```
R1#config t
R1(config)#router ospf 1
R1(config-router)#net 10.10.1.0^0.0.0.255 area 0
R1(config-router)#net 10.10.2.0^0.0.0.255 area 0
R1(config-router)#net 10.10.5.0^0.0.0.255 area 0
* To change priority
Router(config)#int s0/0
Router(config-if)#ip ospf priority 2
```

رقم واحد معناه = على الراوتر Process ID [local] وفي الراوتر الثاني أخط 2
 هنا وضع wild Mask فانتبه ومعناه إن أقدر أشغل ospf على أكثر من config
 - نسوي نفس الإعدادات على الراوتر الثاني

نزيد Priority لنجعل الراوتر الأقوى هو الأول DR

show ip route عُشْمان أشوف الطرق المعمولة بهذا البروتوكول ولا أقدر أشوفها إلا إذا عملت كونهيكل لكل الراوترين	Shows the entire routing table
show ip ospf	Display OSPF information for one or all OSPF processes running on the router.
show ip ospf database	the number of links and the neighboring router's ID
show ip ospf interface	Displays all interface-related OSPF information.

Loop back Interfaces

* ال RID يأخذ أعلى IP
 * لكن لو حصل shot down لل IP راح يتغير وبعدها راح يزيد config وهذا راح يسبب لي ربكة في الشبكة ، فأبغى أثبت IP عن طريق logical IP بغض النظر عن الأشياء الفيزيائية .
 Loopback interfaces are logical interfaces

لما ألقى Logical IP أنسى شيء اسمه Physical IP
 أخذ أعلى Logical IP وإذا ما لقيته أخذ أعلى Physical IP

Configuring Loop back Interfaces	
R1(config)#int loopback 0 R1(config-if)#ip address 172.16.10.1 255.255.255.255 R1(config-if)#no shut	

Chapter: 7

Managing Traffic with Access Control Lists [ACL]

ACL	<div>R</div> <div>مثلاً: R1 [OK] HTTP R2 [NO] FTP</div>	<div>ACL</div> <div>C1 permit HTTP C2 permit SMTP C3 deny FTP</div> <div><div>الإجراء الأكشنaction</div><div>أنواع الأكشنaction</div><div><div>permitسماح</div><div>denyمنع</div></div></div>
	<div>لو جاء شيء غير معروف مثلاً: TELNET: سيكون في المنع الضمني</div>	<div>implicit denyمنع ضمني</div>

- أولاً أبنيتها ثم أربطها في حالة الدخول أو في حالة الخروج ويمكن في الدخول والخروج .
 - قاعدة : لو جاءت أكثر من ACL سوف تطبق آخر وحده فقط.

Types of access lists [ACL]			
Standard	Extended	Named هنا الفرق أحط اسم وليس رقم مثلاً BlockSales	
-choose from rang لازم أعطيتها رقم 1-99 or 1900-1999 - Conditions based on: 1) Action (deny or permit) 2) Source address of packet: 0Host(single IP) 0Subnet(many IP) 0Any	-choose from rang لازم أعطيتها رقم 100-199 or 2000-2699 - Conditions based on: 1) Action (deny or permit) 2) Transport protocol(TCP or UDP) (if any packet made by app protocol (يعني بروتوكول شغال في الأليكشن لير 3)Source address (Host-Subnet-Any) 4)destination address (Host-Subnet-Any) 5)Application protocol that built packet	Standard	Extended

[1] Standard access lists [ACL]

(الشروط لاستخدامهم هو تحديد شيئين فقط هما) Conditions:

- source address
- action (permit or deny)

Source		
Host	Subnet	Any

Configuring Standard [ACL]

<p>[1] Create conditions , Determine specific IP Router(config)#access-list 10 deny <u>host</u> 172.16.30.2 لمنع جهاز واحد فقط</p> <p>OR</p> <p>Router(config)#access-list 10 deny 0.0.0.0 172.16.30.2</p> <p>Determine any packet Lab_A(config)#access-list 10 permit <u>any</u> اسمح لأي بكت غير اللي منعت في الشروط فوق</p> <p>OR</p> <p>Lab_A(config)#access-list 10 permit 0.0.0.0 255.255.255.255</p> <p>Lab_A(config)#access-list 10 deny 172.16.30.2 0.0.0.255 لمنع سب نت كاملة</p> <p>[2] Assign ACL on interface Dest مكان الوصول في مكان الوصول Router(config)#int f0/0</p> <p>Router(config-if)#ip access-group 10 out</p> <p>* Controlling VTY (Telnet) Access</p> <p>Lab_A(config)#access-list 50 permit host 172.16.10.3 طريقة للسماح لشخص واحد في السبنت إنه يستخدم telnet</p> <p>Lab_A(config)#line vty 0 4</p> <p>Lab_A(config-line)#access-class 50 in</p> <p>R(config)#no access-list 10 or 50 'which number you chose it'</p>	<p>Any ==> 0.0.0.0 255.255.255.255 Host → 0.0.0.0 فيه شرط واحد فقط هنا هو منع أي باكت من هذا الـ 172.16.30.2 الهوست</p> <p>هنا wide mask make the dest OUT الأصل هنا هو out في برنامج السيمليشن R (config-if)#ip access-group 10 IN مرة in ومرة out</p> <p>طريقة إلغاء الـ ACL</p>
--	---

* طريقة حل منع سب نت معينة من خلال الآي بي مع السب نت ماسك :

1- إيجاد البلوك سايز BS

2- تحديد Broadcast و Network address

3- نظرهم من بعض ويخرج لي (wide mask)

4 - سيكون الحل كالآتي : **R (config)#access-list 10 deny 172.16.30.0 0.0.0.0**

بحيث الـ IP الأول سيكون Network address والثاني سيكون الـ wide mask

[2] Extended access lists [ACL]

* **Extended ACL:**

1- source 2- destination 3-protocol[packet type] 4-action

قاعدة مهمة هنا

-Assign ACL on source interface and make the direction IN

مثال 1:

action	source	dest	Protocol
			Telnet

R(config)#access-list 110 deny TCP any 172.16.1.0 0.0.0.255 eq 23

نستخدم هذا إذا كان بروتوكول يشتغل في طبقة APP layer مثل HTTP/TELNET/FTP/SMTP

لكن لو كان الـ IP ما يشتغل في طبقة APP layer فما يحتاج أكتب نوع البروتوكول TCP/UDP

Any → des معناه : كل جهاز ممنوع من الوصول إلى

Source			Dest		
Host	Subnet	Any	Host	Subnet	Any
			Single IP	طالعة من Subnet معينة	طالعة من أي جهاز
			طالعة من جهاز واحد		

مثال 2:

R(config)#access-list 110 deny TCP host 10.10.1.1 host 10.10.2.50 eq FTP

في الأخير أضيف هذا السطر

R(config)#access-list 110 permit IP any any

Configuring Extended [ACL]

<p>[1] Create conditions</p> <p>Lab_A(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23</p> <p>Lab_A(config)#access-list 110 permit ip any any</p> <p>[2]Assign ACL on interface وهي المرحلة الثانية وهي الربط</p> <p>Router(config)#int f0/0 نحطه على السورس <==</p> <p>Router(config-if)#ip access-group 110 in</p>	
--	--

[3] Named access lists [ACL]

Configuring Named [ACL]

* To create named access list: -

[1] Create ACL

Lab_A(config)#ip access-list standard BlockSales

[2] Create conditions

Lab_A(config-std-nacl)#deny 172.16.40.0^0.0.0.255 اعمل الشرط مباشرة

Lab_A(config-std-nacl)#permit any

[3] Assign ACL to interface

Lab_A(config)#int e1

Lab_A(config-if)#ip access-group BlockSales out

كيف أضيف الشروط في أوقات معينة فقط Time-Based ACLs

[1] create a period

Router(config)#time-range no-http هذا اسم فقط والمفروض شيء يدل على المعنىRouter(config-time-range)#periodic weekend 06:00 to 12:00 الأول معناها في الصباح والثانية في المساء

[2] attach the created period to ACL

Router(config)#ip access-list extended Time اسم فقط

Router(config-ext-nacl)#deny tcp any any eq www time-range no-http

[3] Assign ACL on interface

Router(config-ext-nacl)#interface f0/0

Router(config-if)#ip access-group Time in

Remarks

** Uses in Extended ACL

R(config)#access-list 110 remark Permit Bob from Sales Only To Finance اسم فقط أي شيء

R(config)#access-list 110 permit ip host 172.16.10.1 172.16.20.0 0.0.0.255

R(config)#access-list 110 permit ip any any

** Uses in Named ACL

R(config)#ip access-list extended No_Telnet

R(config-ext-nacl)#remark Deny all of Sales from Telnetting to Marketing أي شيء

R(config-ext-nacl)#deny tcp 172.16.30.0 0.0.0.255 172.16.40.0 0.0.0.255 eq 23

Switch Port ACLs

[1] Create conditions

S1(config)#mac access-list extended My_MAC_List اسم فقط

S1(config-ext-macl)#deny any host 000d.29bd.4b85 رقم الماك

S1(config-ext-macl)#permit any any

[2] Assign ACL on port

S1(config-ext-macl)#int f0/6

S1(config-if)#mac access-group My_MAC_List in

R#show access-list ip/ipx/apple يعرض كل ACL المعمولة على الراوتر سواء أ ب

R#show access-list 110 يعرض ACL فقط المعمولة برقم 110

R#show ip access-list يعرض ACL المعمولة على IP فقط

R#show ip interface يعرض كل شيء على interface وإذا كان فيها ACL أو لا

R#show running-config سيحضر كل شيء

R#Show mac access-group MAC يعرض ACL المعمولة على MAC

في Exten named نفس الشرط بس نبديل التالي

1-Standard to Extended

أحول الشرط الثاني وإنشائه إلى-2

deny tcp 10.10.1.0^0.0.0.255 host 10.10.2.2 eq ftp

permit ip any any

3- out to in

يشتغل فقط في named

Weekend اسم معروف في الراوتر

www or 80 or HTTP

الأيام:

Saturdays

sundays

الملاحظات

يسوي ملاحظات مثل البرمجة لتعرف

[ACL] وش عملها

تقنية Remark موجودة فقط في Ext & named

ACL

على مستوى السويتش

هنا ملغية في السويتش subnet

فقط host OR any

هنا بدال ip نعط mac

ما دامت any فمعناه إنني راح أضع ACL في كل منفذ وهذا متعبه فبدلا منها استخدم ال range

S1(config-ext-macl)#int range f0/6-10

TFTP هذا قبل v12	UDP	ما تشتغل على WINDOWS ولا يعرفها ولا يقدر يتعرف عليها
FTP	TCP	يعمل على WINDOWS و يعرفها ويقدر يتعرف عليها
HTTP		
HTTPs		

Backing Up the Cisco IOS

**** To back up the Cisco IOS to a TFTP server, you use this command**

R#copy flash FTP يعني من المصدر إلى الوصول

OR

R#copy flash TFTP في الاختبار أضع هذا

بعد الضغط على الأمر في الأعلى راح يطلب اسم الفلاش ثم اسم الـهوس (السيرفر) وبعد كذا هل تبغى ينسخه بنفس الاسم أو باسم

آخر ثم انتر بعدها راح يقوم بعملية النسخ وراح تجد الملف في جهازك في مجلد جديد هو الذي قام بإتشانه اسمه Inetpub

*** To know the name of the IOS image, use this command :**

R#sh flash يعطيني اسم الفلاش والمساحة الحرة والمستخدم والمجموع

or

R#sh ver يعطي حجم الـرام كاملاً للفلاش

or

R#dir flash:

----.bin وأعرف اسم image سيكون امتدادها

R#copy FTP flash طريقة عمل restor استرجاع

Router#ping FTP_server

* IOS file system

Router#show file info flash:c1841.bin

Router#delete flash:c1841.bin

Router#pwd يجيب الدايركتوري اللي أنا اشتغل عليه

1- أول خطوة هي تحويل الوندوز FTP من خلال لوحة التحكم ثم إضافة/إزالة برنامج ثم المكونات ثم IIS=>internet info service

هذا السطر وما بعده يستخدم الأوامر مثل الموجودة في الدوس قديماً

أكبر مساحة لل config هو مساحة NVRAM

1- أتأكد من وجود ربط

2- أتأكد من عمل FTP

امتداد نظام التشغيل هو ----.bin

**** To copy the router's configuration from a router to a FTP server**

Router#copy run FTP هذين الأمرين يتشابهون ولا يوجد فرق بينهم

or

Router#copy start FTP

**** Copying the Current Configuration to NVRAM**

Router#copy run start

**** If you did copy the router's configuration to a TFTP server as a second backup, you can restore the configuration**

Router#copy TFTP run or ftp

أسوي نسخة backup لل config

أنواع config

1- start

2- run

طريق إرجاع ال config

Cisco Discovery Protocol (CDP) [L2]

- هو بروتوكول شغال على راوترات وسويتشات سيسكو فقط ، يعني لما يكون فيه نوعين مختلفين ما راح يعمل .
- وظيفته : إن كل راوتر يرسل باكت تعريفية إلى جيرانه ، وتفيدني في حل المشاكل وفي L3 Troubleshooting

كل فترة زمنية يرسل لجاره وجيرانه ممكن يكونو راوترات أو سويتشات	CDP timer	how often CDP packets are transmitted to all active interfaces.
لها فترة زمنية وتنتهي (وهي المعلومة القادمة من الجار) المعلومات اللي ياخذها من جاره تقعد لمدة محددة من خلال هذه الموقت	CDP holdtime	the amount of time that the device will hold packets received from neighbor devices.

Configuration**Router#sh cdp**

**** Use the global commands cdp holdtime and cdp timer to configure the CDP holdtime and timer on a router:**

Router(config)#cdp timer 90 الافتراضي إنه يقوم بالتحديث كل 60 ثانية ولتغيير الوقت كيفما أريد
Router(config)#cdp holdtime 240 الافتراضي إنه يقوم بالتحديث كل 180 ثانية ولتغيير الوقت كيفما أريد

**** Gathering Neighbor Information by using this command**

Router#sh cdp nei detail يعرض التفاصيل

**** Gathering Interface Traffic Information including the number of CDP packets sent and received and the errors with CDP.**

Router#sh cdp traffic يعرض كم بكت أرسلته وكم بكت استقبلته

**** Gathering Port and Interface Information including CDP status on router interfaces or switch ports.**

Router#sh cdp interface يجيب قائمة بالانترفيس اللي تشتغل CDP

**** To turn off CDP on one interface on a router,**

Router(config)#int s0 إذا ما أبغاه يرسل البكت أدخل على الراوتر وأمنعه

Router(config-if)#no cdp enable

Chapter: 9

Switching Layer2

ال Mac address مكون من 48bits == hexadecimal

* Three Switch Functions at Layer 2:

1. Address learning هي عملية بناء MAC table
2. Forward [if Destination known معروف] / filter [if Destination unknown غير معروف] Broadcast على الجميع ماعدا الأساس (المصدر) source
3. Loop avoidance (Broadcast storm)

- ممكن يربط بين سويتشين بأكثر من لينك (تسمى : multi-link)
- السويتش يأخذ IP واحد فقط

* Spanning Tree Protocol (STP) : بروتوكول منع اللوب

الفائدة من هذا البروتوكول هو منع عملية اللوب loop avoidance في الطبقة الثانية layer2

- 1- المشكلة هي وجود multi-link فعن طريق هذا البروتوكول أ منع جميع المسارات وأ فعل مسار واحد فقط single link وهذا logical
- 2- يقوم البروتوكول على تحويل المسار من closed path إلى open path

* STP steps والعمل والانتخاب:

1- elect (انتخاب) Root Bridge (switch) based on :

- a) priority [less] أختار أقل أهمية (رقم الأهمية الافتراضي في سويتشات سيسكو هي 32,768)
- b) Bridge ID (BID) MAC address [less] رقم أقل

لكن في السويتشات والتي اسمها Non-RB يكون اختيار الـ DP من حيث:

- a) priority أقل شيء (رقم الأهمية الافتراضي في سويتشات سيسكو هي 32,768)
- b) BID (MAC) (طبعاً هنا المقصود الـ MAC)

2- All ports on (Root Bridge) become [(designated port) [Forward Port]]

كل البورتات على الروت بريدج تسمى فورورد بورت

3- Remaining Bridge[sw] become [Non-Root Bridge]

البورتات في السويتشات الباقية تسمى Non-Root Bridge

4-For each Non-Root Bridge only one Root Port

في السويتشات Non-RB يوجد روت بورت واحد فقط وهي التي تكون مربوطة مع روت بريدج (يعني الأب الكبير)

إذا عندي أكثر من لينك multi-link يقوم STP باختيار روت بورت واحد من اللينكات وطريقة الاختيار تكون مرتبة كالتالي:

- a) cost أختار أقل شيء وإذا تساوى ننتقل للمعيار الثاني

Speed	Cost
2	10G
4	G
19	F
100	E

علماً بأن هذه الأرقام ثابتة

- b) Port number أختار أقل شيء

اللي هو رقم البورت المكتوب على السويتش f0/0 or f0/2 or f0/3

5- For each segment only one Designated Port [Forward Port]

المقصود بـ segment هنا هو الينك اللي يربط بين السويتشين

في السويتش اللي يكون RB يكون اسم البورت الموصل فيه هو DP واسم البورت في السويتش الآخر RP وعليه فأى بورت ليس DP ولا RP راح يسوي عليه block

BPDU: Bridge Protocol Data Unit تسمى بين السويتشات تكون

[STP]Spanning-Tree Port States من أعماله أيضا

1- Blocking 2- Forwarding

Configuring Cisco Catalyst Switches

*** Setting the Passwords Switch(config)#enable password <u>todd</u> -----> non Encrypted Switch(config)#enable secret <u>todd</u> -----> Encrypted *** Setting the Hostname Switch(config)#host <u>S2950</u> *** Port Security Switch(config)#int f0/1 Switch(config-if)#switchport port-security mac-address sticky Switch(config-if)#switchport port-security maximum 1 Switch(config-if)#switchport port-security violation shutdown S(config)#int range f0/1-5	MAC Address <== الجهاز - هذا ممكن أخط الماك بنفسه أو اكتب كلمة sticky فقط و sticky معناها السويتش يتعرف على الماك أليا - عدد الأجهزة المسموح للسويتش معرفتهم بـ MAC Address - لو زاد عدد تغييرات الماك عن اللي حطيت به راح ينفذ هذا الأمر (أنا أسويه) وهو إطفاء الجهاز إذا بغيت تسوي Security على مجموعة من البورتات بدال ما تسويها بورت بورت
*** Setting IP Information S2950#config t S2950(config)#int vlan1 ثابت S2950(config-if)#ip address 172.16.10.17 255.255.255.0 S2950(config-if)#no shut S2950(config-if)#exit S2950(config)#ip default-gateway 172.16.10.1	السويتش يعتبر كأنه host كيفية إعطاء IP للسويتش دائما على السويتش اختار VLAN1 لتنقل البيانات من سويتش 1 إلى سويتش 2
S#sh mac address-table S#sh spanning-tree RB و Non-RB يعرض Sw(config)#spanning-tree vlan 1 priority 16384 OR S1(config)#spanning-tree vlan 1 root primary	يعرض ال MAC Address Table تغيير ال Priority وأغيرها للأقل لما أبغى سويتش معين يكون الرووت Root Bridge ال تكون ال راح إعطائها صراحة ومباشرة

أجعل البورت Fast علشان أخطى هذا الانتظار :

يستقبل BPDUs	Block (20 sec)	الافتراضي 50 ثانية
يستقبل DPDU ويمكن يخرجها	Listening (15 sec)	
يستقبل BPDUs ويمكن يخرجها ويشارك في بناء MAC ADD TABLE	Learning (15 sec)	
	Forward	

هذه التقنيات BPDUGuard و BPDUFILTER تعمل فقط على PortFast

S2950(config)#int range f0/3-4 S2950(config-if-range)#spanning-tree portfast S2950(config-if-range)#spanning-tree bpduguard enable S2950(config-if-range)#spanning-tree bpdufilter enable	يمنع استقبال BPDUs
--	--------------------

Spanning Tree UplinkFast

NonRoot فقط على

ميزة : أعملها لما يكون عندي بديل

أول ما تحصل مشكلة يكون مجهز بورت آخر

بين ال root و nonroot ينتظر 50 ثانية فها ما ينتظر لأنه مجهز بورت آخر

S2950(config)#spanning-tree uplinkfast	
--	--

Spanning Tree BackboneFast

يأخذ مسار خلفي

اطبقها على root و nonroot وعلى كل السويتشات

S2950(config)#spanning-tree backbonefast Erasing the Switch Configuration S2950#erase startup-config	
--	--

Chapter:10

Virtual LANs [VLAN]

فوائد ال VLAN :

- 1- حلت مشكلة إنه subnet لكل interface يعني ممكن الكثير من ال subnet على عدد قليل من interface
- في الراوتر ال one physical interface يحتوي على 4.2 مليون logical interface
F0/1.1 هذا sub interface
- ما أقدر أسوي أكثر من 1024 لأن أكثر من كذا يسوي اختناق على الشبكة
- 2- حل مشكلة physical limitation (يعني لو كان السويتش مليون فأقدر أشبك شخص تابع لنفس القسم في سويتش آخر وأربطه معهم)
- 3- حل مشكلة broadcast لأنه يستهلك باندويث
- 4- عملية الأمان (أكثر من subnet)
- إذا عملت أكثر من VLAN احتاج لراوتر علشان أربط بينهم
- لكن إذا قسمت VLAN الواحدة إلى مجموعة subnet فإني أستطيع أتراسل بينهم بدون راوتر ولو كانوا في سويتشات مختلفة
- أقدر أجمع الأقسام مع بعض في VLAN وحده حتى لو كانوا في أماكن مختلفة (تحت/فوق) أو على سويتشات مختلفة
- فتحات السويتش (Ports) تكون موجودة في VLAN1 ومعناه إذا أردنا إنشاء أي VLAN فإننا نبدأ من VLAN2 كما أن VLAN1 متركبة لل- Administrator

* التصادم وحدوثه collision domain

- 1- في الهاب Hub
التصادم يحصل على مستوى الهب ككل (برود كاست للجميع)
- 2- في السويتش Switch
التصادم يحدث على مستوى البورت فقط (برود كاست للجميع ما عدا المصدر)
- 3- في الراوتر
التصادم يحدث على مستوى subnet الواحدة [each Router Interface Represents Broadcast domain]

VLAN Types	
Static VLANs	Dynamic VLANs
هنا الشغل يكون على البورت نفسه	هنا الشغل يكون على الجهاز نفسه
أنت تقوم بالعمل By admin - هنا أعمل assign لنفس البورت فلو غيرت الأجهزة أو جبت أجهزة جديدة (ما تفرق لأن الإعدادات على البورت نفسه)	برامج تقوم بالعمل By admin - هنا التحديث يكون على مستوى الأجهزة فلو غيرت أو نقلت الجهاز (فراح يستمر الجهاز في نفس VLAN)

- ما ينفع أشغل static و dynamic

- f0/1 → VLAN2[sales] , f0/2 → VLAN3[IT] , f0/3 → VLAN4[marketing] , f0/4 → VLAN5[accounting]

*There are two different types of links in a switched environment: أنواع اللينكات:

1	2						
Access links	Trunk links						
بين السويتش والهوست	بين سويتش وسويتش بين سويتش وراوتر						
البورت في السويتش الأول والثاني يجب أن يكون access port على السويتش فقط وليس الراوتر وهذا معناه أسوي Config له	البورت في السويتش الأول والثاني يجب أن يكون Trunk port على السويتش فقط وليس الراوتر وهذا معناه أسوي Config له						
	لازم يكون البورت Fast Ethernet						
	يعمل الآتي :						
	1- VLAN-ID احتاج VLAN-ID إذا كان عندي أكثر من VLAN على السويتش						
	2- تغليف Encapsulation لما أسوي نقل بين جهاز رقم 1 وجهاز رقم 5 احتاج أضيف وأنا أقوم بتحديد أي بروتوكول يستخدم:						
	<table> <tr> <th colspan="2">Frame tagging [Encapsulation]</th></tr> <tr> <th>Inter-Switch Link (ISL)</th><th>IEEE 802.1Q [dot1Q]</th></tr> <tr> <td>- Cisco</td><td>- Open standard</td></tr> </table>	Frame tagging [Encapsulation]		Inter-Switch Link (ISL)	IEEE 802.1Q [dot1Q]	- Cisco	- Open standard
Frame tagging [Encapsulation]							
Inter-Switch Link (ISL)	IEEE 802.1Q [dot1Q]						
- Cisco	- Open standard						

حددنا السبب نت ماسك مسبقا في السؤال

Packet		
Data	Voice Real time	Video Real time
	هنا ما يتحمل انتظار delay فاعطيها priority أكبر و عليه استخدم QoS[Quality of service] الصوت يحتاج جودة خدمة أكثر من غيره	

* إذا كنت أنواع البيانات هي التي فوق فمعناه شبكتي intelligent

Configuring Voice VLANs	
Switch(config)#mls qos Switch(config)#interface f0/1 Switch(config-if)#mls qos trust cos Switch(config-if)#switchport voice vlan dot1p Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 3 Switch(config-if)#switchport voice vlan 10	

Chapter: 11

Network Address Translation

[NAT]

IP	
Virtual [private]	Real [public]
10.0.0.1 : 10.255.255.254	
172.16.0.1 : 172.31.255.254	
192.168.0.1 : 192.168.255.254	
أي IP غير موجود في هذا الرنج فهو Real IP	

ال NAT هي علاقة بين virtual IP و real IP بحيث يقوم بالتحويل بينهم وفائدته : مقدرة الأجهزة المختلفة الدخول على النت (حيث أن الحصول على real IP لكل جهاز مكلف جدا)

PAT → Port Address Translation

NAT			
Static	Dynamic	Overloading == [PAT]	
One virtual IP => one real IP	Many virtual IP => Many real IP شرط: Number of real IP=number of virtual IP Many real IP CALLD pool of real IP	Static With Overloading Many virtual IP => One real IP	Dynamic With Overloading Many virtual IP => Many real IP

ال NAT هو أحد الحلول ((مثلا يمكن استخدام البروكسي))

NAT Names		
Inside local	Inside global	Outside global
Name of inside source address before translation	Name of inside host after translation	Name of outside destination host after translation
المقصود فيه Virtual IP	المقصود فيه Real IP	المحطة التي أبغى أوصل لها خارج شبكتي

Static NAT	
<p>[1]Creates a static NAT translation between 192.168.10.1 and 192.1.2.109</p> <p>Router(config)#ip nat inside source static 192.168.10.1 192.1.2.109</p> <p>[2]Configures NAT inside interface</p> <p>Router(config)# interface f0/0</p> <p>Router(config-if)# ip address 192.168.10.1 255.255.255.0</p> <p>Router(config-if)# ip nat inside</p> <p>[3] Configures NAT outside interface</p> <p>Router(config)# interface Serial0/0</p> <p>Router(config-if)# ip address 192.1.2.109 255.255.255.240</p> <p>Router(config-if)# ip nat outside</p>	<p>هذا الجهاز المسموح له الإنترنت</p> <p>192.168.10.1 Virtual IP</p> <p>192.1.2.109 Real IP</p>

Dynamic NAT	
<p>[1]Defines a NAT pool (outside addresses) named MyPool with a range of addresses 60.1.1.2 – 60.1.1.6</p> <p>Router(config)#ip nat pool MyPool 60.1.1.1 60.1.1.6 netmask 255.255.255.248</p> <p>[2]Determine inside addresses that will use NAT, that addresses are defined in ACL</p> <p>Router(config)#ip nat inside source list 10 pool MyPool</p> <p>Router(config)# access-list 10 permit 192.168.10.0 0.0.0.255</p> <p>[3] Configures NAT inside interface</p> <p>[4] Configures NAT outside interface</p>	<p>مجموعة من many Real address Pool=> IP من ISP تشتري</p> <p>هنا يعني 6 أجهزة (IPs) مشتركة من ISP</p> <p>هنا يبنى الجدول وال 10 معناها رقم ACL</p> <p>يقدر يدخل 254 جهاز لكن في الوقت الواحد 6 أجهزة فقط</p> <p>نفس الأوامر في Static NAT</p>

وعلشان أستخدمة استخدم Port علشان أقدر أخرج أكثر عدد من الأجهزة (واستخدم رقم أعلى من 1024 لأن ما قبله محجوز)

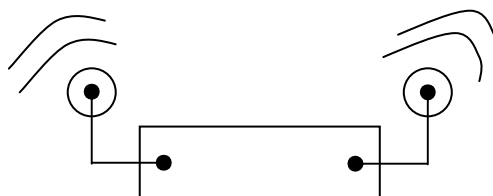
Overload NAT (PAT)	
<p>[1] Defines a NAT pool (outside addresses) named MyPool with a range of Single address 60.1.1.1</p> <p>Router(config)#ip nat pool MyPool 60.1.1.1 60.1.1.1 netmask 255.255.255.248</p> <p>[2]Determine inside addresses that will use NAT, that addresses are defined in ACL</p> <p>Router(config)#ip nat inside source list 10 pool MyPool <u>overload</u> =====></p> <p>Router(config)# access-list 10 permit 192.168.10.0 0.0.0.255</p> <p>[3] Configures NAT inside interface</p> <p>[4] Configures NAT outside interface</p>	<p>جهاز واحد فقط</p> <p>وش نوع ال NAT المستخدمة هنا Static PAT or Static overload = هنا بيكون</p>

Simple Verification of NAT	
<p>* To see basic IP address translation information, use the following command:</p> <p>Router#show ip nat translation</p> <p>This output will show the sending address, the translation, and the destination address on each debug line:</p> <p>Router#debug ip nat</p> <p>* To cancel the debug استخدم الأمر التالي لإلغاء</p> <p>R#undebug all</p> <p>Or</p> <p>R#un all</p>	<p>يعرض ال table</p> <p>يوريني العملية التي يرسلها ويستقبلها ويحولها و عملية debug تستهلك resource فتره معينة ثم أغلقها</p>

Chapter: 12

Wireless LAN

[WLAN]



* إذا أبغى اتصال لا سلكي احتاج :

- 1- أكسس بوينت Access Point (مثل السويتش في الشبكة السلكية – يعني مجمع أجهزة مع بعضها)
- 2- كرت شبكة لا سلكي (مثل كرت الشبكة في الشبكة السلكية)

التواصل يتم عبر الموجات الكهرومغناطيسية Electromagnetic

2.4 GHZ	Wireless	802.11 b and 802.11g	ما يحتاج لها تصريح Unlicense
5 GHZ	Waves	802.11 a	ما يحتاج لها تصريح Unlicense

Agency	Purpose
مسئولة عن عمل الاستاندرد للشبكات اللاسلكية Institute of Electrical and Electronics Engineers (IEEE)	Creates and maintains operational standards
مسئولة عن إعطاء تصاريح للموجات والترددات – وهذه الهيئة موجودة في أمريكا Federal Communications Commission (FCC)	Regulates the use of wireless devices in the U.S.
مسئولة عن إعطاء تصاريح للموجات والترددات – وهذه الهيئة موجودة في أوروبا European Telecommunications Standards Institute (ETSI)	Chartered to produce common standards in Europe
Wi-Fi Alliance	Promotes and tests for WLAN interoperability
WLAN Association (WLAN)	Educates and raises consumer awareness regarding WLANs

للعلم فإنه يوجد ترددات لا تحتاج إلى ترخيص مثل : 900MHz / 2.4GHz / 5 GHz والباقي يحتاج ترخيص من الهيئة الخاصة في دولتك.

	802.11b	802.11g	802.11a
Data rate	Up to 11 Mbps	Up to 54 Mbps	Up to 54 Mbps
Modulation method	DSSS	DSSS & OFDM	OFDM
Frequency band	2.4GHz	2.4GHz	5 GHz
عدد القنوات channels numbers	14	14	عدد القنوات في النظام الأمريكي = 23 عدد القنوات في النظام الأوروبي = 19
لو كان نفس التردد بجانب بعض أي القنوات أختار Non-overlapping channels	3non → 1-6-11	3non → 1-6-11	12

إضافات :

- 1- كلما زادت الـ data rate كلما قلت الـ cover area
- 2- كلما زاد الـ Frequency كلما قلت الـ cover area وزاد الـ data rate
- 3- النوع b and g يتعاملون مع بعض لأن لهم نفس التردد بسبب البروتوكول (Request To Send, Clear To Send) RTS/CTS or CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) ما يحدث أي تصادم

DSSS → Direct Sequence Spread Spectrum ||| OFDM → Orthogonal Frequency Division Multiplexing

- ال AD-HOK هي طريقة ربط بين جهازين بدون أكسس بوينت

حلول شركة سيسكو للأسلكي Cisco's Unified Wireless Solution

- **MESH :**

- Root Access Points (RAPs) معناه : واصل على الشبكة السلكية
- Mesh Access Points (MAPs) معناه : واصل على الشبكة السلكية عن طريق الروت

- **AWPP:** بروتوكول يحدد أفضل مسار للوصول من ال MESH إلى Root

- Adapter wireless path protocol

-This protocol allows RAPs to communicate with each other to determine the best path back to the wired network via the RAP.

- **Wireless Security :**

1. **Open Access**

2. **SSIDs, WEP, and MAC Address Authentication**

SSID → Service Set Identifiers اسم الشبكة عندما تعرض ما هي الشبكات اللاسلكية المتصلة

WEP → Wired Equivalency Protocol يسوي تكوين لمجموعة من المفاتيح وهي الباس لكن يرسلها نص غير مشفر

MAC addresses → بحيث الأجهزة المسجلة فقط هي التي تدخل

3. **WPA or WPA 2 [Pre-Shared Key (PSK)] يعطي تشفير أكثر-يرسل الباسورد مشفر**

- WPA → Wi-Fi Protected Access and WPA2 (المطور) Pre-Shared Key (PSK) is a better form of wireless security than any other basic wireless security methods mentioned so far.

الفرق بين الأول والثاني (المطور) هو زيادة الخانات الممكنة في وضع الباسورد

4. **Cisco Unified Wireless Network Security حلول لتكوين شبكة لاسلكية على أكمل وجه**

- Secure Connectivity for WLANs عن طريق الداتا
- Trust and Identity for WLANs عن طريق الاثنتوكيشن والاثورايز
- Threat Defense for WLANs عن طريق معرفة التهديدات

- اسم الراوترات التي تدعم الوايرلس == ISR integrated service router

راوتر الخدمات المتكاملة

Chapter: 13

Internet Protocol Version 6 (IPv6)

IPv6	IPv4
128 bits	32 bits

تتعامل مع Hexadecimal	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit
	00AB	Cf00	2434	1270	3210	4210	5611	877	991A

افصل بينهم بنقطتين (كولن) ::--::--::--::--::

- [IP v.4] number of add = 2^{32}
- [IP v.6] number of add = 2^{128}
- No size for header

** The Benefits and Uses of IP v.6 :

1. IPv6 is 128 bits which gives (3.4×10^{38}) of addresses.
2. The header in an IPv6 packet have half the fields استخدام البانديث.
3. There is no broadcast in IPv6 because it uses multicast traffic instead.

	X:X:X:X:X:X:X
الشكل الأصلي	1080:0000:0000:0000:0008:0800:200C:417A
تبسيط	1080:0:0:0:8:800:200C:417A
تبسيط أكثر ، بحيث الأصفار التي بعد بعضها اختصارها وأحط :: ولا يمكن استخدام هذا الاختصار إلا مرة واحدة فقط	1080::8:800:200C:417A

0:0:0:0:0:0:1
::1
ويسمى loop back ويشبهه 127.0.0.1 في v4 وهو يسمى local host

IPv6	
prefix-address	prefix-length
	مثل سب نت ماسك

F0/1=> 12:34:56:7::1/64	-ال 64 معناها prefix length وهي مثل سب نت ماسك والأربع الأرقام الأولى ما تتغير أبد داخل السب نت الواحدة ولو تغيرت فمعناه يكون في سب نت مختلفة
F0/1=> 12:34:56:8::1/64	-العدد الأخير وهو 1 يكون من 1 إلى FFFF بحيث يعطيني سب نت مختلفة وطبعاً عرفناه من سب نت ماسك
12:34:56:7:: net add هذا يعتبر مثل	

هذا الشغل لل Router interface
EUI هي عملية generate لباقي البتات بحيث تكمله إلى 128 بت عن طريق MAC address تبع الهوست.
حيث أنه Prefix length يجب أنه ما يقل عن 64 بت

ثابتة → MAC : 48 bits

طريقة الإضافة عن طريقة هذا الرقم وهو FFFF وهو ثابت ، مثال :

0000.abcd.0001
↓
FFFF
0000.abff.ffcd.0001

Host Config		
Manual	Automatic	
	stateless	statefull
	No DHCP	DHCP
	Found in the network	Found in the network
	Automatic يأخذ XP ويندوز DHCP هنا يرسل عن طريق	

من ميزات IPv6 على IPv4 إنه يستخدم multicast فقط ولا يوجد broadcast

** Address Types: -

1. Unicast address تروح لعنوان معين – مثل IPv4 single
2. Multicast address توصل للناس كلها- مثل class D in IPv4
3. Anycast address توصل لراوتر معين على حسب أحسن مسار والغرض إني أرسل باكت للانتر فيس فقط
4. Global unicast addresses مثل v.4 IP Public
5. Link-local addresses مثل v.4 IP Privet

أيضاً يوجد داخل IPv6 real and virtual مثل IPv4 ولكن ال virtual يسمى

0:0:0:0:0:192.168.100.1 This is how an IPv4 address would be written in a mixed IPv6/IPv4 network environment.	
2000::/3 The global unicast address range	يمثل real IP 0010.0000.0000.0000
FC00::/7 The unique local unicast range غير مستخدم الآن FE80::/10 The link-local unicast range هذا بداله	يمثل private IP 1111.1110.1000.0000
FF00::/8 The multicast range	يمثل multi-cast

Configuring Cisco Routers with IPv6	
<p>* Enable IPv6 علشان أشغل ال IPv6 لانه بالافتراضي مش شغال</p> <p>Router(config)#ipv6 unicast-routing</p> <p>• Configure IPv6 on the interface</p> <p>Router(config)#int f0/0</p> <p>Router(config-if)#ipv6 address 2001:db8:3c4d:1:0260:d6FF:FE73:1987/64</p> <p>OR</p> <p>• You can allow the device to use its MAC address and pad it to make the interface ID.</p> <p>Router(config-if)#ipv6 address 2001:db8:3c4d:1::64 eui-64 هذي Extended user interface بحيث يسوي إنشاء لل 64 بت الباقية</p>	<p>محدد dse / single IP</p> <p>Prefix length</p> <p>يسوي إنشاء وتكون عن طريق الماك وهذي أضعها بحيث ما يكون فيه تكرار من عندي</p>

Dynamic Host Configuration Protocol (DHCPv6)

احتاج هذه الأشياء للإعدادات ب IP v6

DHCPv6 Client	A node that initiates requests on a link to obtain configuration parameters.
DHCPv6 Server	A node that responds to requests from clients to provide addresses, prefix lengths, or other configuration parameters.
DHCPv6 Relay مثل ساعي البريد	A node that acts as an intermediary to deliver DHCPv6 messages between clients and servers. ويستخدم بحيث ما يكون ضغط على DHCP فهو يعتبر وسيط ويتم تجميع الطلبات وإرسالها لل DHCP
DHCPv6 Agent	يمكن أحطه either a server or a relay.

Configuring Cisco Routers with IPv6

Dynamic Host Configuration Protocol (DHCPv6)

```
Router(config)#ipv6 dhcp pool test اسم
Router(config-dhcp)#prefix-delegation pool test lifetime 3600 3600 الأرقام هذي بالثواني
Router(config)#int f 0/0
Router(config-if)#ipv6 dhcp server test
```

IPv6 Routing Protocols

- **RIPng** [next generation الإصدار الثاني]


```
Router(config)#int f 0/0 أشغله على مستوى ال interface فقط
Router(config-if)#IPV6 rip 1 enable ر قم 1 هنا معناه process ID
```
- **EIGRPv6**

```
Router(config)#ipv6 router eigrp 10 رقم 10 هنا معناه Autonisim system
Router(config-rtr)#no shutdown
Router(config)#int f 0/0
Router(config-if)#ipv6 eigrp 10
```
- **OSPFv3**

```
Router (config)#ipv6 router ospf 10 ر قم 1 هنا معناه process ID
Router (config-rtr)#router-id 1.1.1.1 هو اللي يأخذ أعلى id في انتخاب DR فأحدده هنا مباشرة
Router(config)#int f 0/0 أشغله على مستوى ال interface فقط
Router(config-if)#ipv6 ospf 10 area 0
```

Migrating to IPv6

كيف أسوي upgrade متوافق من IPv4 إلى IPv6

1- Dual Stacking

It allows our devices to communicate using either IPv4 or IPv6.

```
Router(config)#ipv6 unicast-routing
Router(config)#interface fastethernet 0/0
Router(config-if)#ipv6 address 2001:db8:3c4d:1::/64 eui-64
Router(config-if)#ip address 192.168.255.1 255.255.255.0
```

2- 6to4 Tunneling

```
Router1(config)#int tunnel 0
Router1(config-if)#ipv6 address 2001:db8:1:1::1/64
Router1(config-if)#tunnel source 192.168.30.1
Router1(config-if)#tunnel destination 192.168.40.1
Router1(config-if)#tunnel mode ipv6ip
Router2(config)#int tunnel 0
Router2(config-if)#ipv6 address 2001:db8:2:2::1/64
Router2(config-if)#tunnel source 192.168.40.1
Router2(config-if)#tunnel destination 192.168.30.1
Router2(config-if)#tunnel mode ipv6ip
```

Configuring IPv6 on Our Internetwork

```
Corp#config t
Corp(config)#ipv6 unicast-routing
Corp(config)#int f0/1
Corp(config-if)#ipv6 address 2001:db8:3c4d:11::/64 eui-64
Corp(config-if)#int s0/0/0
Corp(config-if)#ipv6 address 2001:db8:3c4d:12::/64 eui-64
Corp(config-if)#int s0/0/1
Corp(config-if)#ipv6 address 2001:db8:3c4d:13::/64 eui-64
Corp(config-if)#int s0/1/0
Corp(config-if)#ipv6 address 2001:db8:3c4d:14::/64 eui-64
Corp(config-if)#int s0/2/0
Corp(config-if)#ipv6 address 2001:db8:3c4d:15::/64 eui-64
Corp(config-if)#^Z
Corp#copy run start
R1#config t
R1(config)#ipv6 unicast-routing
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:db8:3c4d:12::/64 eui-64
R1(config-if)#int s0/0/1
R1(config-if)#ipv6 address 2001:db8:3c4d:13::/64 eui-64
R2#config t
R2(config)#ipv6 unicast-routing
R2(config)#int s0/2/0
R2(config-if)#ipv6 address 2001:db8:3c4d:14::/64 eui-64
R3#config t
R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/1
```

RS = الرقم الأول
RA = الرقم الثاني

وأسوي هذا علشان ما يتشابه في ال generation بين two switches بحيث ما يتشابهة ويشغل state less

الانترفيس يأخذ واحد من IPv4 و IPv6

استخدم اختيار أحد الطريقتين إذا كان الجهاز (الراوتر-السويتش-الهوست) يقدر يتعامل بالطريقتين

أدخل شيء معمول ب v6 إلى شيء معمول ب v4

استخدمه إذا كان يمر بشبكة لا تعرف IPv6

إذا أبلغاه two ways أسوي الإعدادات على الراوتر
إذا أبلغاه one way أسوي الإعدادات على راوتر واحد

R3(config-if)#ipv6 address 2001:db8:3c4d:15::/64 eui-64

1- Configuring RIPng

```
Corp#config t
Corp(config)#int f0/1
Corp(config-if)#ipv6 rip 1 enable
Corp(config-if)#int s0/0/0
Corp(config-if)#ipv6 rip 1 enable
Corp(config-if)#int s0/0/1
Corp(config-if)#ipv6 rip 1 enable
Corp(config-if)#int s0/1/0
Corp(config-if)#ipv6 rip 1 enable
Corp(config-if)#int s0/2/0
Corp(config-if)#ipv6 rip 1 enable
```

• Configuring RIPng

```
R1#config t
R1(config)#int s0/0/0
R1(config-if)#ipv6 rip 1 enable
R1(config-if)#int s0/0/1
R1(config-if)#ipv6 rip 1 enable
R2#config t
R2(config)#int s0/2/0
R2(config-if)#ipv6 rip 1 enable
R3#config t
R3(config)#int s0/0/1
R3(config-if)#ipv6 rip 1 enable
```

• Verifying RIPng

```
R3#sh ipv6 route
R3#sh ipv6 protocols
R3#sh ipv6 rip
R3#sh ipv6 interface serial 0/0/1
R3#debug ipv6 rip
```

2- Configuring OSPFv3

```
Corp#config t
Corp(config)#int f0/1
Corp(config-if)#ipv6 ospf 1 area 0
Corp(config-if)#int s0/0/1
Corp(config-if)#ipv6 ospf 1 area 0
Corp(config-if)#int s0/1/0
Corp(config-if)#ipv6 ospf 1 area 0
Corp(config-if)#int s0/2/0
Corp(config-if)#ipv6 ospf 1 area 0
```

• Configuring OSPFv3

```
R1#config t
R1(config)#int s0/0/1
R1(config-if)#ipv6 ospf 1 area 0
R2#config t
R2(config)#int s0/2/0
R2(config-if)#ipv6 ospf 1 area 0
R3#config t
R3(config)#int s0/0/1
R3(config-if)#ipv6 ospf 1 area 0
```

• Verifying OSPFv3

```
R3#sh ipv6 route
R3#sh ipv6 protocols
R3#sh ipv6 protocols
R3#sh ipv6 protocols
Corp#debug ipv6 ospf packet
Corp#un all
```

No shut لازم

أحتاج واحد من هذين البروتوكولين لكي تتشوف الأجهزة بعضها البعض

Chapter: 14

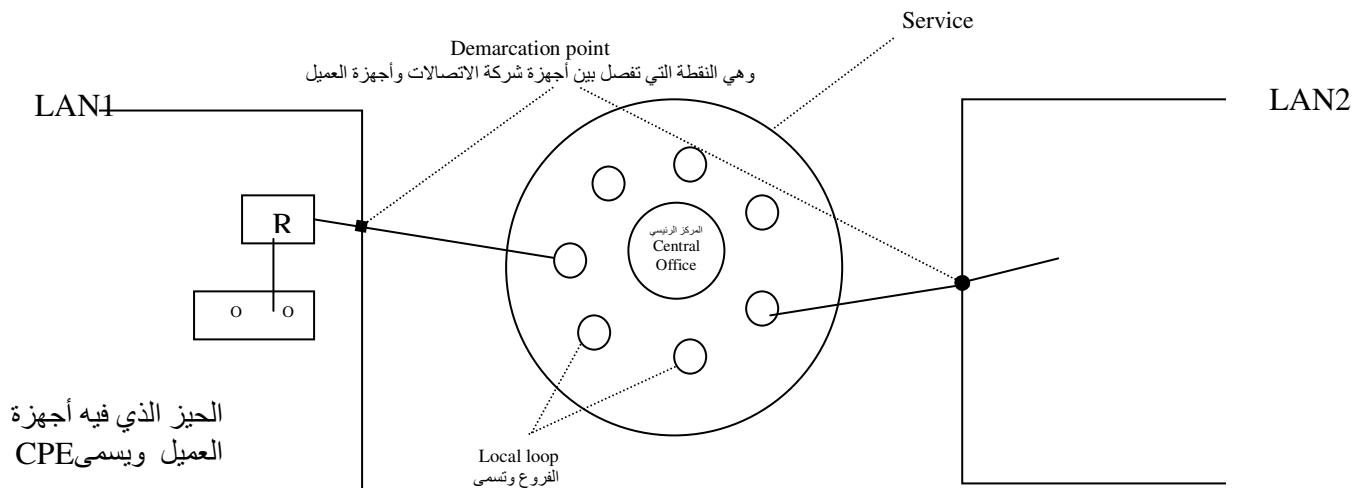
Wide Area Networking

[WAN]

أي سيرفيس (خدمة) : قائمة على شركة الاتصالات في الدولة

Defining WAN Terms:

- Customer premises equipment (CPE)
- Demarcation point
- Local loop
- Central office (CO)



** WAN Connection Types الأنواع التي يمكن استخدامها داخل WAN

- 1- Dedicated for example: lease line خط مخصص
- 2- Circuit switched for example : ISDN or dial up خط ادفع عليه متى ما استخدمته والفرق بينهم السرعات فـ ISDN 56K و 128K or 1.5Mbps dial up
- 3- Packet switch for example : Frame relay خط واحد لكن عليه أكثر من عميل

لوفيه سيرفيس service جميع الراوترات راح تشتغل DTE وليس DCE ...
وإذا كانت مربوطة بسيريل فراح يستخدم CSU/DSU [Circuit Service Unit / Data Service Unit]

DSL → Based band
WI-MAX → Broad band

إذا مرت الباكيت من خلال ال service يجب أن يكون هناك تغليف Encaps و لكل سيرفيس تغليف وبروتوكول خاص به:

protocol		
HDLC High-Level Data-Link Control	PPP Point-to-Point Protocol	Frame Relay
ويستخدم فقط في : 1-lease line	ويستخدم فقط في : 1-lease line 2-ISDN 3-Dial up	ويستخدم فقط في : 1-Frame Relay
إذا استخدمته يجب أن يكون كل الراوترين من نفس الشركة	ويوجد به أكثر من بروتوكول 1- LCP (Link Control Protocol) → يتأكد من وصول البيانات إلى محطة الوصول ويعمل في Layer2 2- NCP (Network Control Protocol) → يقدر يتعامل مع أي نوع من أنواع البروتوكولات L3 3- Authentication protocol	* You can't use HDLC or PPP with Frame Relay. With Frame Relay there are two encapsulation types: 1- Cisco 2- IETF (Internet Engineering Task Force)

*** PPP has many advantage:**

1- multi-link **Back up** ممكن يفيدني في

2- Callback معاودة الاتصال

3- Authentication التحقق

a- CHAP (Challenge Hand Authentication Protocol) → [Encrypted] مشفر

b- PAP (Password Authentication Protocol) → [Clear Text] واضح

4- Compression الضغط

5- Route packet for different routed packet

Configuring PPP on Cisco Routers

<ul style="list-style-type: none"> • Turn on PPP on connected interface تغليظ ب PPP <pre>Router(config)#int s0 Router(config-if)#encapsulation ppp</pre> <ul style="list-style-type: none"> • Configuring PPP Authentication تحقق <pre>Router(config)#hostname <u>RouterA</u> اسم RouterA(config)#username <u>RouterB</u> password <u>cisco</u> RouterA(config)#int s0 RouterA(config-if)#ppp authentication chap pap RouterA(config)#hostname <u>RouterB</u> اسم RouterB(config)#username <u>RouterA</u> password <u>cisco</u> RouterB(config)#int s0 RouterB(config-if)#ppp authentication chap pap</pre>	<p>Base config:</p> <p>1- أشغل ال interface وأعطيه IP</p> <p>2- أحدد نوع البروتوكول RIP أو OSPF</p> <p>ال PPP يستخدم في :</p> <p>1- Lease line</p> <p>2- Dial up</p> <p>3- ISDN</p> <p>يحاول بكل البروتوكولين</p> <p>أسمي اسم المستخدم الأول بالثاني ونفس الباس</p> <p>وأسمي اسم المستخدم الثاني بالاول ونفس الباس</p>
---	--

Frame Relay

يقسم الباندويث على أكثر من واحد ((بدال ما يستخدم Lease line الغالي))

Frame Relay ما يفهم البروتوكول TCP/IP فهنا نستخدم بروتوكول آخر للتغليظ وهو **Frame Relay**

* Frame Relay has become one of the **most popular** WAN services deployed.

* Frame Relay is a **packet-switched** technology

* Frame Relay, by default, is classified as a non-broadcast multi-access (**NBMA**)

*** Frame Relay PVCs are:**

اللينك بين FR switch والراوتر تسمى PVC [Permanent Virtual Circuit] وهو مختلف عن السويتشات العادية

1- devices using (DLCI) *Data Link Connection Identifiers* يعطي رقم تعريف للباكت

Local Management Interface (LMI) **Signal** (إشارة) **أوجد Up 24H** يكون **PVC** **أخلي**

is a signaling standard used between your router and the first Frame Relay switch it's connected to.

واللي يحدد نوع LMI هو مزود الخدمة ISP

**** There are three different types of LMI message formats:**

1- Cisco (default) 2- ANSI (open standard) 3- Q.933A. (open standard)

Frame Relay Implementation

<pre>RouterA(config)#int s0/0 RouterA(config-if)#no shut RouterA(config-if)#encapsulation frame-relay IETF RouterA(config-if)#ip address 172.16.20.1 255.255.255.0 RouterA(config-if)#frame-relay lmi-type <u>ansi</u> ممكن تختار من الثلاث أنواع RouterA(config-if)#frame-relay interface-dlci 101</pre>	<p>تغليظ ال frame relay ب IETF</p>
--	------------------------------------

<i>show frame lmi</i> يعرض نوع LMI المستخدمة	Give you the LMI traffic statistics exchanged between the local router and the Frame Relay switch.
<i>show frame pvc</i>	* list all configured PVCs and DLCI numbers. * It provides the status of each PVC connection and traffic statistics.
<i>show interface</i>	* Check for LMI traffic. * Displays line, protocol, DLCI, and LMI information.
<i>show frame map</i>	Displays the Network layer-to-DLCI mappings.

Virtual Private Networks (VPN)

** There are three different categories of VPNs:

- 1- Remote access VPNs
- 2- Remote users VPN
- 3- Site-to-site VPNs

** Tunneling protocols طبعا ال tunnel يكون logical والفائدة منه هو عملية تشفير

- 1- Point-to-Point Tunneling Protocol (PPTP) (open standard)
- 2- Layer 2 Tunneling Protocol (L2TP) (open standard) هذا أكثر سكيورتي
- 3- Generic Routing Encapsulation (GRE) فقط على راوترات سيسكو

** Security Protocols (IPSec) يستخدم برتوكول L2TP ويستخدم شينان

- 1- Authentication Header (AH)
- 2- Encapsulating Security Payload (ESP)

IPsec → encrypted

IP → Clear