

الفهرس

الموضوع	رقم الصفحة
المقدمة	
مقدمة عن سيسكو	4
مكونات الراوتر	4
نظام التشغيل IOS (Internetwork Operating System)	8
برنامج Hyper Terminal	10
برنامج سيسكو التعليمي Cisco Packet tracer.	17
حماية الراوتر بكلمة مرور	25
كلمة مرور على مدخل Consol.	25
الدخول للراوتر من بعد	28
عناوين الشبكات IP Address	31
انواع الرسائل بين اجهزة الشبكات	32
التوجيه Rounting	34
التوجيه الثابت Static Rounting	36
المسار الافتراضي Defualt Route	37
برتوكول التوجيه Routing Information Protocol (RIP)	38
برتوكول التوجيه , Routing Protocol (OSPF)	40
برتوكول التوجيه Routing Protocol (EIGRP)	45
نظام التحكم بالدخول Access Control List (ACL)	49
برتوكول توزيع العناوين DHCP	57
ترجمة عناوين الشبكات Network Address Translations (NAT)	60

السوتش Switching

65.....	تاريخ السوتش
66.....	ما هو السوتش
71.....	الضبط الابتدائي Cisco Catalyst
74.....	ضبط المبدل Switch Configuration
76.....	اضافة عنوان IP Address للشبكة الافتراضية VLAN
71.....	ضبط البوابة الافتراضية في المبدل Default Gateway on the Switch
74.....	ضبط رمز دخول للسوتش Secret Password
74.....	حماية مدخل الكونسول للسوتش
74.....	حماية الدخول من بعد للجهاز
74.....	استخدام شفرة حماية الرمز السري Encrypting Password
74.....	وضع رسالة تنبيهية للمستخدمين Configuring Banner
75.....	تعيين عنوان للسوتش
75.....	حفظ الضبط السابق Saving Configuration
76.....	انواع مداخل الكابل و السوتش
77.....	تقسيم الشبكة المحلية الي اقسام داخلية VLAN
80.....	عملية التوصيل بين الشبكات المحلية Inter VLAN
82.....	Spanning Tree Protocol (STP)

المقدمة :

الحمد لله الذي زين قلوب أوليائه بأنوار الوفاق، وسقى أسرار أحبائه شراباً لذيذ المذاق، وألزم قلوب الخائفين الوجَل والإشفاق، فلا يعلم الإنسان في أي الدواوين كتب ولا في أيّ الفريقين يساق.

وأشهد أن سيدنا وحبينا وشفيعنا محمداً عبد الله ورسوله، وصفيه من خلقه وحببيه، خاتم أنبيائه، وسيد أصفياه، المخصوص بالمقام المحمود، في اليوم المشهود، الذي جُمع فيه الأنبياء تحت لوائه.

أما بعد ..

نظرا لأهمية الربط الشبكي بين أجهزة الحاسوب في سوق العمل وتوسع مجالات تقنية الشبكات و حاجة الافراد و المؤسسات لأستخدامات الانترنت و مشاركة التطبيقات!! ,

أقدم هذه الورقات التي من شأنها تبسيط منهج سيسكو لشبكات الحاسوب و يساعد المبتدئين على معرفة اهمية الشبكات و القدرة على التدريب الذاتي بشرح كل ما يحتاجه الدارس للبدء بالتطبيق العملي و رفع مستوي النمو التقني .

(ملخص شبكات سيسكو) بشقيه النظري و العملي الذي يحتوي على اوامر التطبيق اللازمة في بناء الشبكات و ربط فروع قطاع الاعمال كما يحتوي على شرح مبسط مستخدماً امثلة من واقع تقنية المعلومات . مستعينا بصور تقريبية و تقديم متسلسل لدروس منهج CCNA Routing & Switching كما يشمل سرد من اوامر الضبط و الاعدادات الذي يحتاجه الدارس لتجاوز اختبار **CCNA 200-125** .

يشمل هذا الملخص على دروس و مواضيع متناسقة بشكل يساعد القارئ على استيعاب المنهج بشكل هرمي بدا من التطبيقات المستخدمة في تصميم الشبكات و شرح استخدامات تطبيق سيسكو الشهير (Cisco Packet Tracer 6.1) ومن ثم شرح عملي لبرنامج (HyperTerminal) الذي يستخدم في اعداد الراوترات و المبدلات , يحتوي كل موضوع على الشكل التصميمي و الصورة التقريبية و اوامر نظام التشغيل (IOS) الضرورية للتطبيق , كما يحتوي على اوامر حل المشكلات و المعاينة و الفحص .

تم ارفاق مع (مختصر شبكات سيسكو) قرص صلب يحتوي على كل البرامج و التطبيقات اللازمة في التدريب على محاكاة واقع الشبكات

مقدمة عن سيسكو :

سيسكو شركة امريكية عملاقة متخصصة بعلم الشبكات بشكل عام و الشركة توفر اجهزة الموجهات و المقسمات الخاصة بالشبكات و ابدعت في هذا المجال .

و تطورت الشركة لتنشئ برامج تدريبية لديها لكل طلاب الشبكات حول العالم و انشئت ما يسمى ب سيسكو نيتورك أكاديمي (Cisco Network Academy) وهي الأكاديمية الاولى في العالم التي تقدم شهادات متخصصة بالشبكات , و اصبحت هذه الشهادات معتمدة حول العلم لذلك سميت بالشهادات العالمية . اسست سيسكو سنة 1984 من طرف مجموعة من الباحثين و العلماء على رأسهم ليونارد بوساك و ساندي لرنر من جامعة ستانفورد بسان فرانسيسكو . و كان الهدف من تأسيسها هو تسهيل الربط الشبكي بين الحواسيب و جعلها أكثر فاعلية . ومن اشهر منتجات الشركة الموجهات (Router)

تعريف الراوتر (Router):

المعنى اللغوي هو " الموجه " وهو جهاز مثل جهاز الكمبيوتر يعتبر من اهم الاجهزة المستخدمة في ربط الشبكات المختلفة , يقوم الراوتر بتوجيه الباكت (البيانات) بين الشبكات المختلفة و يتألف من مجموعة من العتاد و البرمجيات .

يعمل الموجه في طبقة الشبكة Network layer وهي الطبقة الثالثة من الطبقات السبعة , سوف ياتي تفاصيل الطبقات لاحقا . و يعمل الموجه على مستويين :

مستوى التحكم : حيث يقوم بايجاد أفضل طريق (او افضل وجهة) لارسال البيانات من المرسل الي المستقبل .

مستوى التمرير و النقل : حيث يقوم بعملية النقل الفعلي للبيانات المستقبلية من واجهة الاستقبال لواجهة الارسال التي اختارها في المرحلة السابقة .

و يعتمد الموجه على جدول التوجيه Routing Table لاجاد اقصر طريق للبيانات

الشكل الموالي يوضح شكل راوتر سيسكوموديل 1800 من الجهة الامامية :



مختصر شبكات سيسكو CCNA Routing and Switching

1 ضوء نظام الطاقة LED يعمل عندما نقوم بتوصيل كابل جهاز الراوتر بالكهرباء و يكون لونه اخضر.

ضوء نشاط النظام : عندما يكون الضوء الاخضر في حالة نشاط تكون هناك عملية استقبال او ارسال للبيانات في الشبكة او عند الدخول الي الجهاز للتعديل في خصائصه .



المكونات الاساسية للراوتر

1 المكونات الخارجية :

منفذ serial port و في الصوري منفذين يكون التمييز serial 0 , serial 1



ملاحظة

تصنف مداخل و منافذ serial الي DCE Data Communication Equipment و هو منفذ ينظم مرور الكهرباء داخل الكابل .

منفذ DTE Data Terminal Equipment و هو منفذ يقوم باستقبال الاوامر من DCE

و وظيفة منفذ التوصيل serial هي توصيل الراوتر مع راوتر اخر بواسطة serial cable



4 منفذ بطاقات الشبكة Ethernet , Gigabyte , FastEthernet , وهذه المنافذ تتميز ايضا باضافة رقم مثل ethernet0 , ethernet1 , ethernet2 .. او gigabyte1 , gigabyte2 .. او fastethernet0/0,ethernet0/1 , ethernet0/2...

و يستخدم تلك المنافذ لربط الراوتر مع السويتش (Switch) او مع جهاز كمبيوتر او مع راوتر اخر

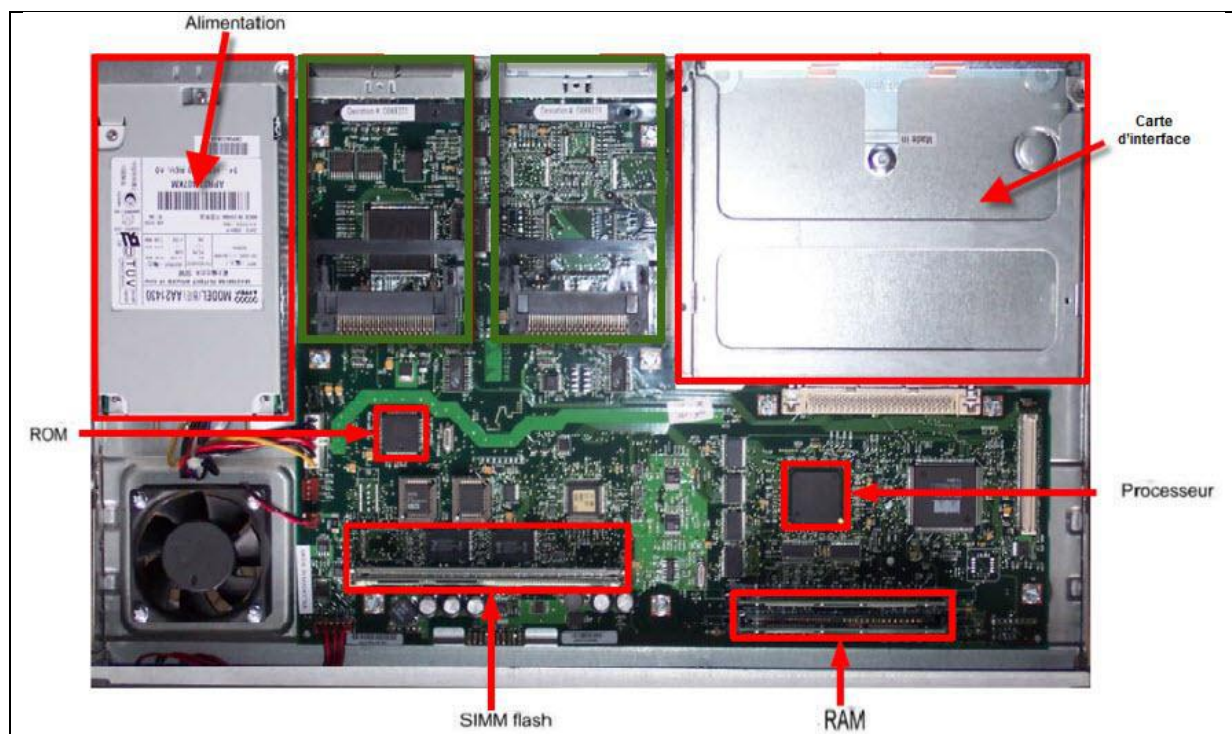
2 منفذ التحكم (console port) و غالبا ما يكون لونه ازرق , يستخدم لربط الراوتر مع الكمبيوتر المسؤول عن اعداد ضبط الراوتر بواسطة احدى البرامج المساعدة للدخول الي نظام تشغيل الراوتر

3 منفذ AUX اختصارا auxiliaire عادة ما يكون لونه اسود و يستخدم لربط الراوتر بالمودم

5 كرت ذاكرة خارجية قابلة للتغير removable flash momre

6 منفذ USB Univeral Serial Bus

المكونات الداخلية للروتر :



وحدة تغذية الطاقة :- تقوم بتزويد المكونات بالتيار الكهربائي و يوفر الطاقة اللازمة لتشغيل المكونات الداخلية .

وحدة التخزين :- و هي وحدة تخزين نظام تشغيل الروتر .

المعالج processor :- يكون للروتر معالج يعمل على مدار الساعة دون توقف و لها الوظائف التالية :-

* 1 * تنفيذ نظام التشغيل IOS

* 2 * تهيئة النظام و السيطرة على واجهة الشبكة

* RAM :- (ذاكرة الوصول العشوائي):

* ROM :- يتم استخدام الذاكرة ROM لتخزين رمز التشغيل الدائم (configuration register) و رمز بدء التشغيل التشخيصي و تحميل IOS من ذاكرة الفلاش الي ذاكرة الوصول العشوائي

* Flash memory :- ذاكرة الفلاش تستخدم لتخزين صورة كاملة لنظام تشغيل سيسكو IOS

* (NVRAM) :- ذاكرة الوصول العشوائي غير المتطاير:

** نظام التشغيل IOS (Internetwork Operating System) :

اشتهرت به شركة سيسكو للشبكات , و يسمى (تشغيل البرمجيات) المستخدمة في اجهزة التوجه سيسكو , و هو عبارة عن قالب برمجيات مثبت على معظم موجهات و مبدلات سيسكو و هو عنصر مهم و فعال في الانترنت لانه يعطى الفرصة لتنظيم حركة الحزم المختلفة عبر الشبكات و يشمل هذا النظام على مجموعة من التقنيات تختلف حسب حجم و قوة المسير او المبدل .

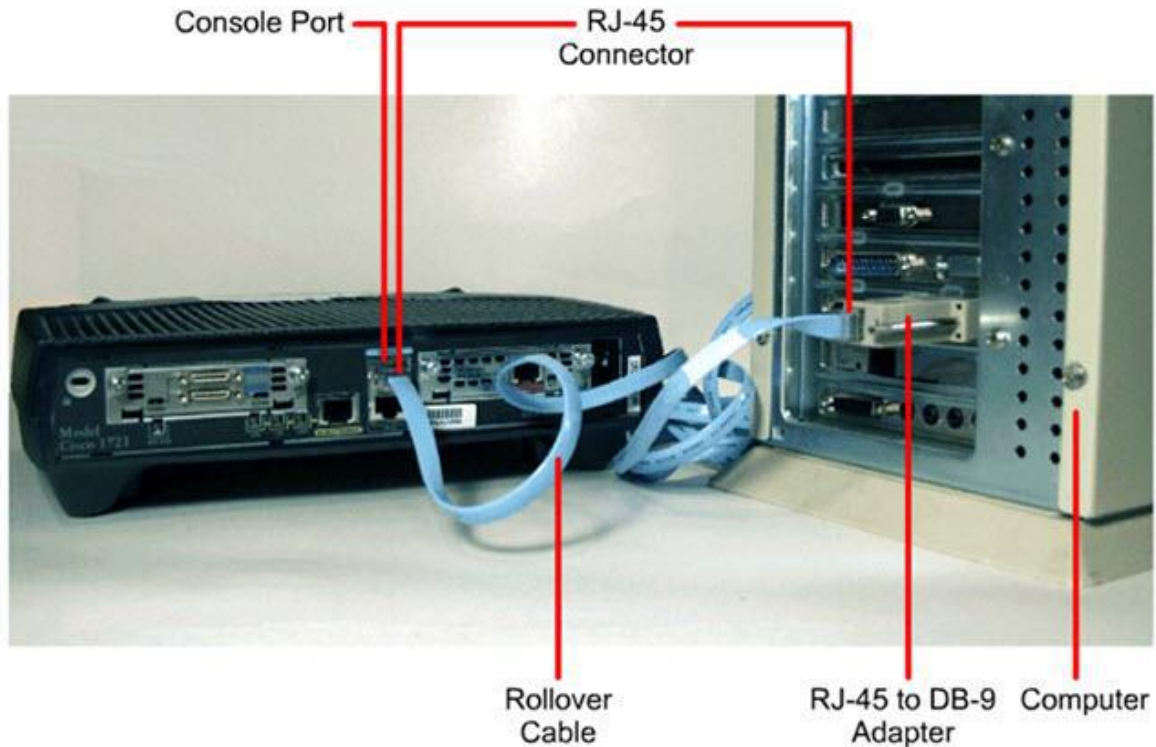
طريقة الدخول الي الراوتر :

للدخول الي نظام تشغيل راوتر سيسكو و البدء بالاعداد يجب اتباع الخطوات التالية و هي :

1 ربط الموجه مع جهاز كمبيوتر بواسطة consol cable و يكون الكابل مختلف من الجهتين توصل جهة RJ-45 connector في منفذ الراوتر على console port , اما الجهة الثانية نوصله بجهاز الكمبيوتر في serial port .



شكل التوصيل كاملا .. بواسطة كونسول كايبيل !!!!



يمكن الوصول الي بيئة CLI واجهه سطر الاوامر بعدة طرق و هي :

** عن طريق جلسة عبر منفذ التحكم Console و جهاز كمبيوتر مع برنامج HyperTerminal

** عن طريق جهاز Modem عبر المنفذ المساعد AUX عن بعد

** عن طريق اتصال شبكة باستخدام خدمة Telnet او SSH بواسطة اعداد IP address .

1 عن طريق منفذ console الموجود خلف router و هي اشهر طريقة مستخدمة ويجب استخدام برنامج HyperTerminal او اي برنامج شبيهه .

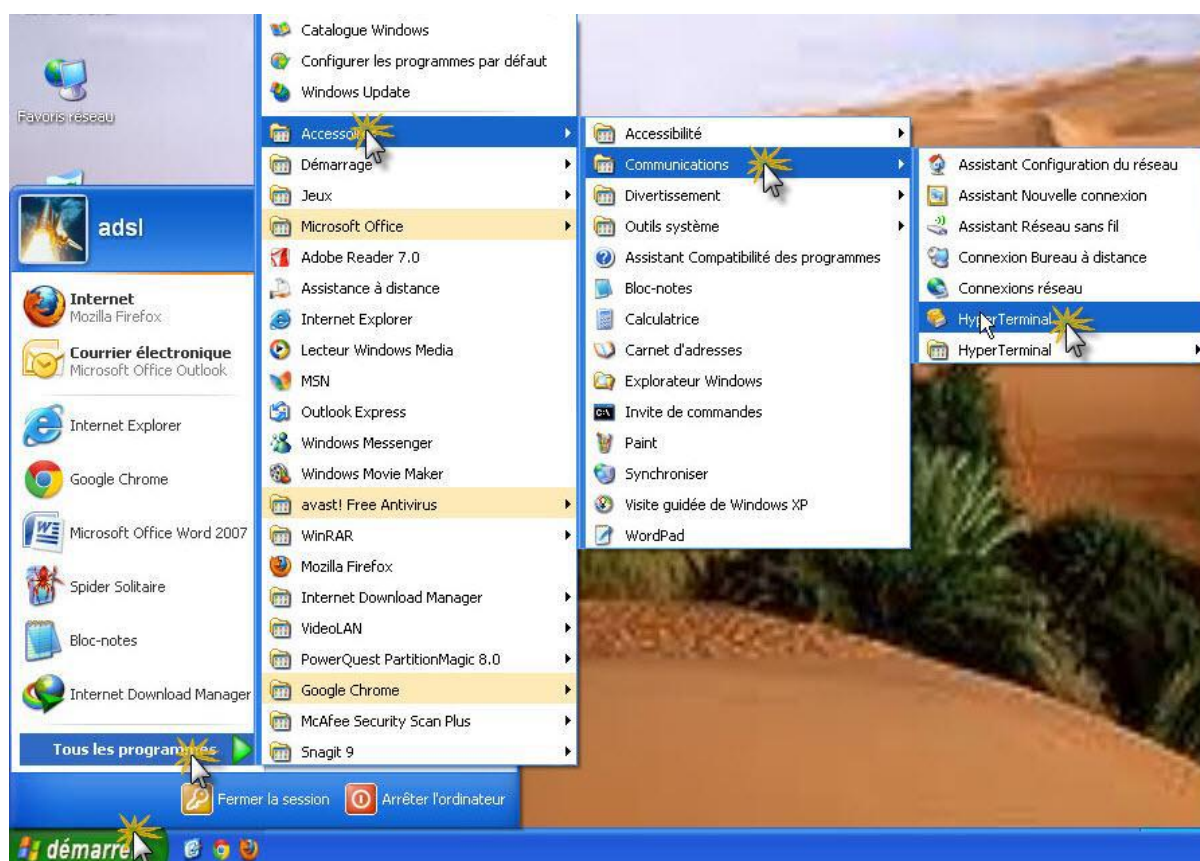
Hyper Terminal

سنأخذ برنامج HyperTerminal كمثال لتوضيح كيفية التوصيل و بقية البرامج تستخدم نفس الطريقة .

عند الدخول على برنامج HyperTerminal و اختيار اسم للاتصال , اختار المنفذ المسلسل الموجود على جهازك COM1 و الموصل على منفذ Consol Router

للدخول الي البرنامج نتبع الخطوات الاتية :

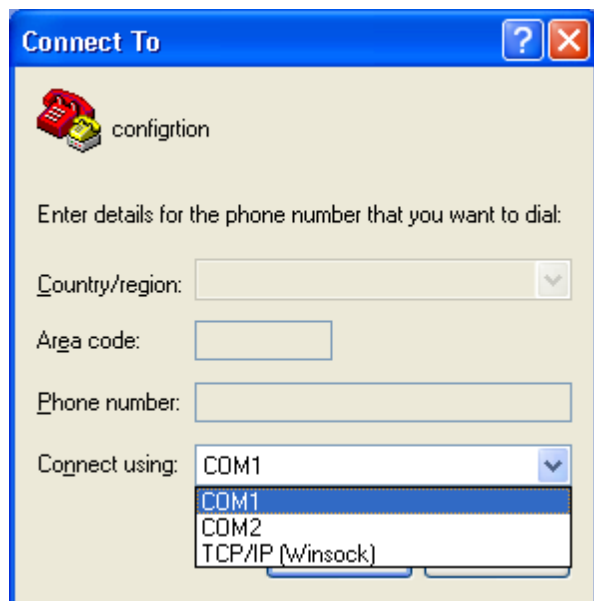
ابدأ start + جميع البرامج + اللواحق + اتصالات و نختار برنامج HyperTerminal كما بالصورة



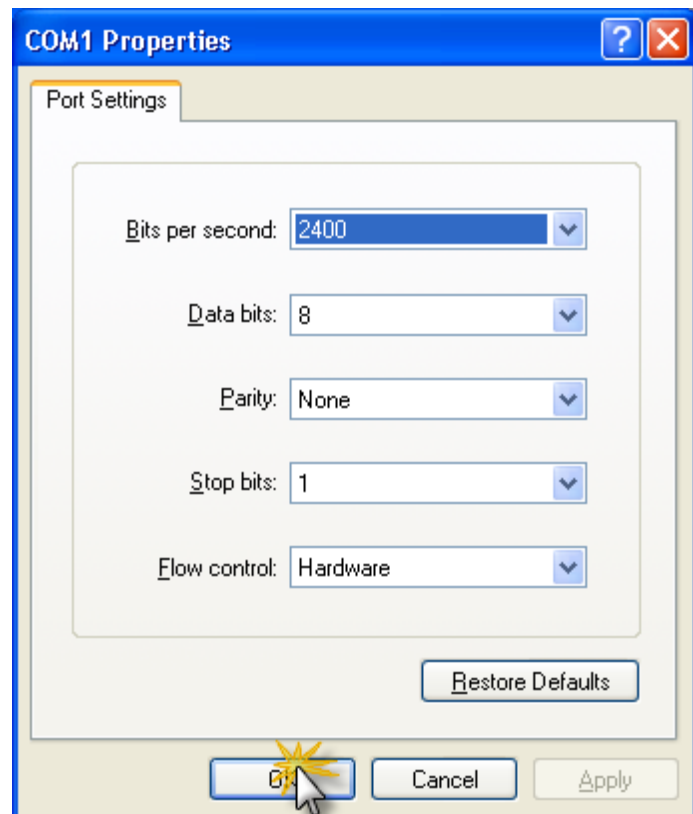
تظهر نافذة لاختيار نوع الاتصال و تسميته كما بالصورة



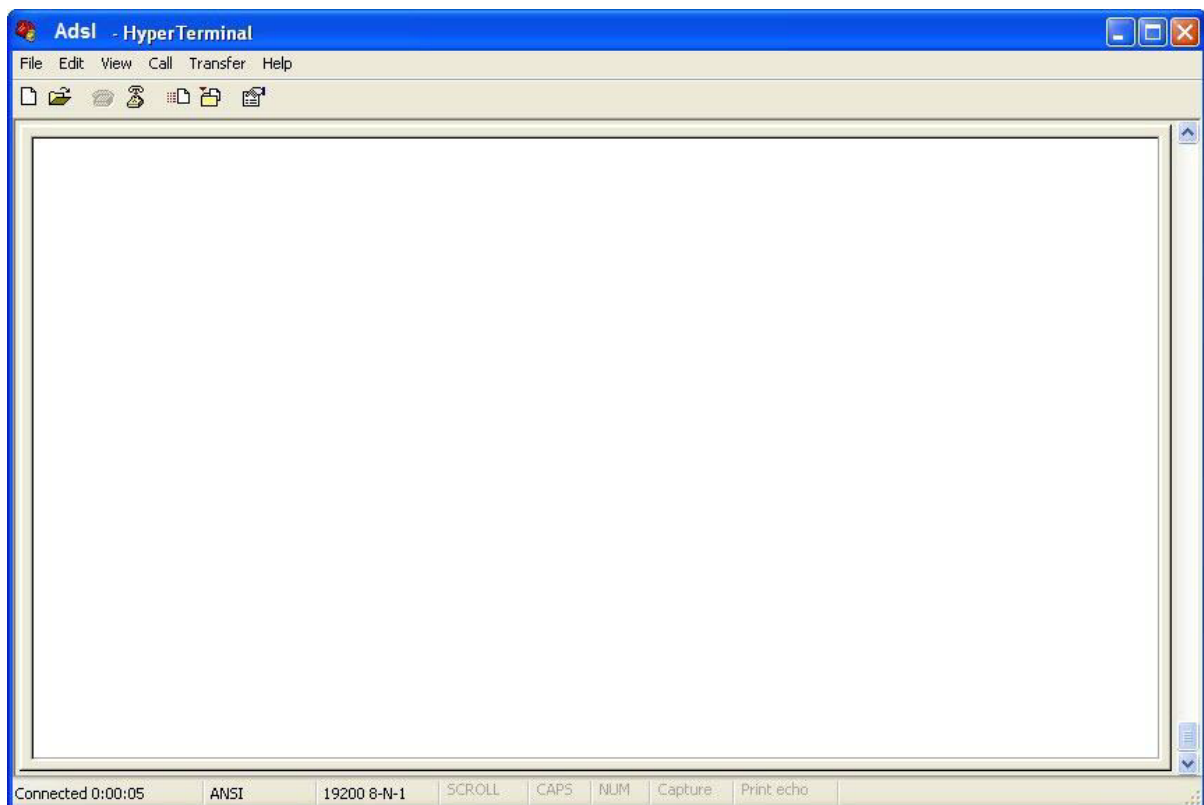
تظهر نافذة اخرى لتحديد ال port المنفذ المتصل من خلاله الكمبيوتر ثم اضغط زر OK



تظهر نافذة اخرى ستلاحظ انه يطلب منك اعدادات الاتصال , اترك الاعدادات كما هي على القيمة الافتراضية كما بالصورة التالية

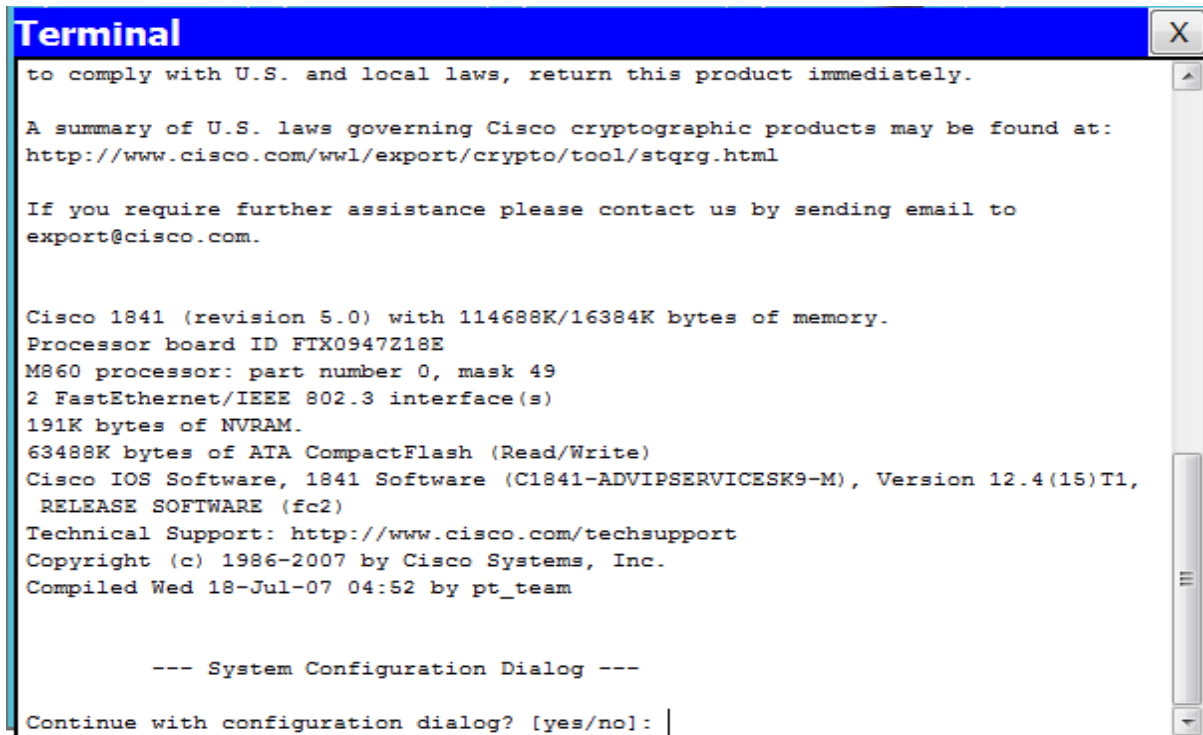


بعد ذلك تظهر واجهة التي يتم فيها كتابة الاعدادات الخاصة بالراوتر CLI (واجهة سطر الاوامر)
الصورة التالية توضح



طرق اعداد الراوتر : لاعداد راوتر سيسكو هناك طريقتين الطريقة الاولى بان تختار اعداد الموجه مع المرشد , و الثانية ان تقوم بالاعدادات بنفسك و عند الدخول الي برنامج HyperTerminal و يظهر مربع الحوار , سنشاهد معلومات خاصة بالراوتر مثل اصدار الراوتر و نظامه و قوة استيعابه ... الخ

الصورة توضح هذه المعلومات



```
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: |
```

و سنشاهد في السطر الاخير من مربع الحوار يطرح سؤال يقول:

[Continue With configuration dialog? [Yes/no]:

اذا اخترنا الامر yes يعنى انك ستتعامل مع مرشد الراوتر و هذه المرحلة تسمى نمط الاعداد Setup Mode

نمط الاعداد Setup Mode : و هي عبارة عن مربع حوار يساعد المستخدم الجديد على انشاء تكوين اساسي لأول مرة. سيقوم المستخدم بالتابع المرشد مثلا يطلب منك اختيار اسم الراوتر hostname

و يمكن الوصول لنمط الاعداد من خلال النمط المميز بكتابة الامر setup

الصورة توضح :

```
Terminal
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Router#setup

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:

Enter host name [Router]:
```

اما اذا اخترنا الامر no يعني اننا سنقوم بالإعدادات يدويا بدون مرشد بعد ذلك نضغط زر انتر في لوحة المفاتيح وندخل الى مرحلة اعداد الراوتر مباشرة

```
Terminal
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
```

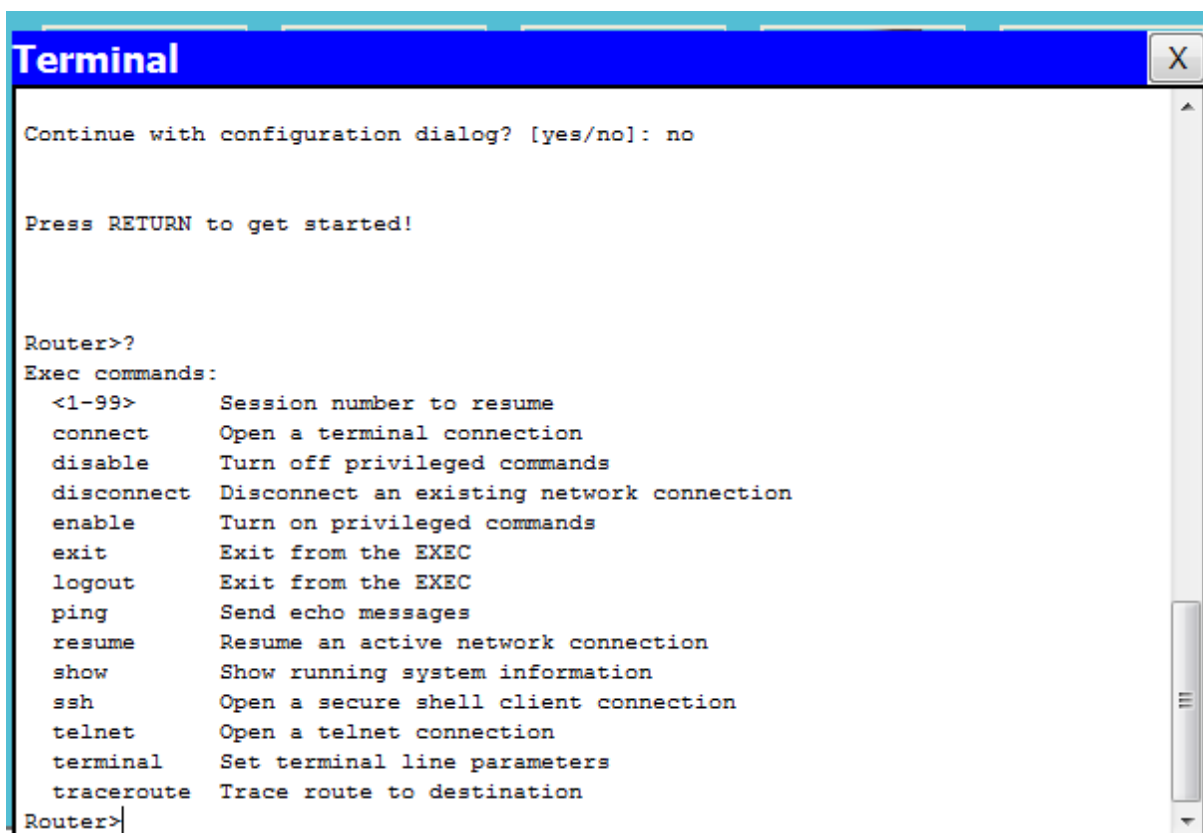

اعداد الراوتر :

وهي مراحل , كل مرحلة تتميز بعدة اوامر التي يمكن تطبيقها على الراوتر, و يمكن ان نعرف الاوامر التي تكتب في كل مرحلة بالضغط على علامة الاستفهام (?)

وضع المستخدم (**user mode**):

و هي مرحلة معاينة فقط , اي يستطيع المستخدم معاينة بعض المعلومات عن الموجه لكن لا يمكنه اجراء اي تغييرات

خلال تواجد المستخدم في مرحلة user mode يكون المؤشر كمايلي Router>



```
Terminal
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>?
Exec commands:
<1-99>      Session number to resume
connect     Open a terminal connection
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
logout      Exit from the EXEC
ping        Send echo messages
resume      Resume an active network connection
show        Show running system information
ssh         Open a secure shell client connection
telnet      Open a telnet connection
terminal    Set terminal line parameters
traceroute  Trace route to destination

Router>
```

الوضع المتميز Privilege Mode :

و يمكن الدخول الي هذه المرحلة الثانية بالامر enable وفي هذه المرحلة يمكنك عرض و اظهار نتائج تنفيذ الاوامر التي قمت بها و كذلك امكانية عمل حفظ للعمل الذي قمت به بواسطة الامر copy run start خلال التواجد في المرحلة الثانية يكون المؤشر كمايلي:

الصورة توضح المرحلة الثانية :

```
Terminal
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#
```

نمط التكوين العام الكلي **Global Configuration Mode** :

ينفذ هذا النمط اوامر فعالة مؤلفة من سطر واحد تنفذ مهام تكوين بسيطة مثل تغيير كلمة السر او اسم الراوتر او يضع المستخدم ضمن نمط تكوين عام اكثر تخصصا .

و للدخول الي هذه مرحلة نستعمل امر `configure terminal`

كما في الصورة

```
Terminal
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>ena
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

برنامج سيسكو التعليمي Cisco Packet Tracer

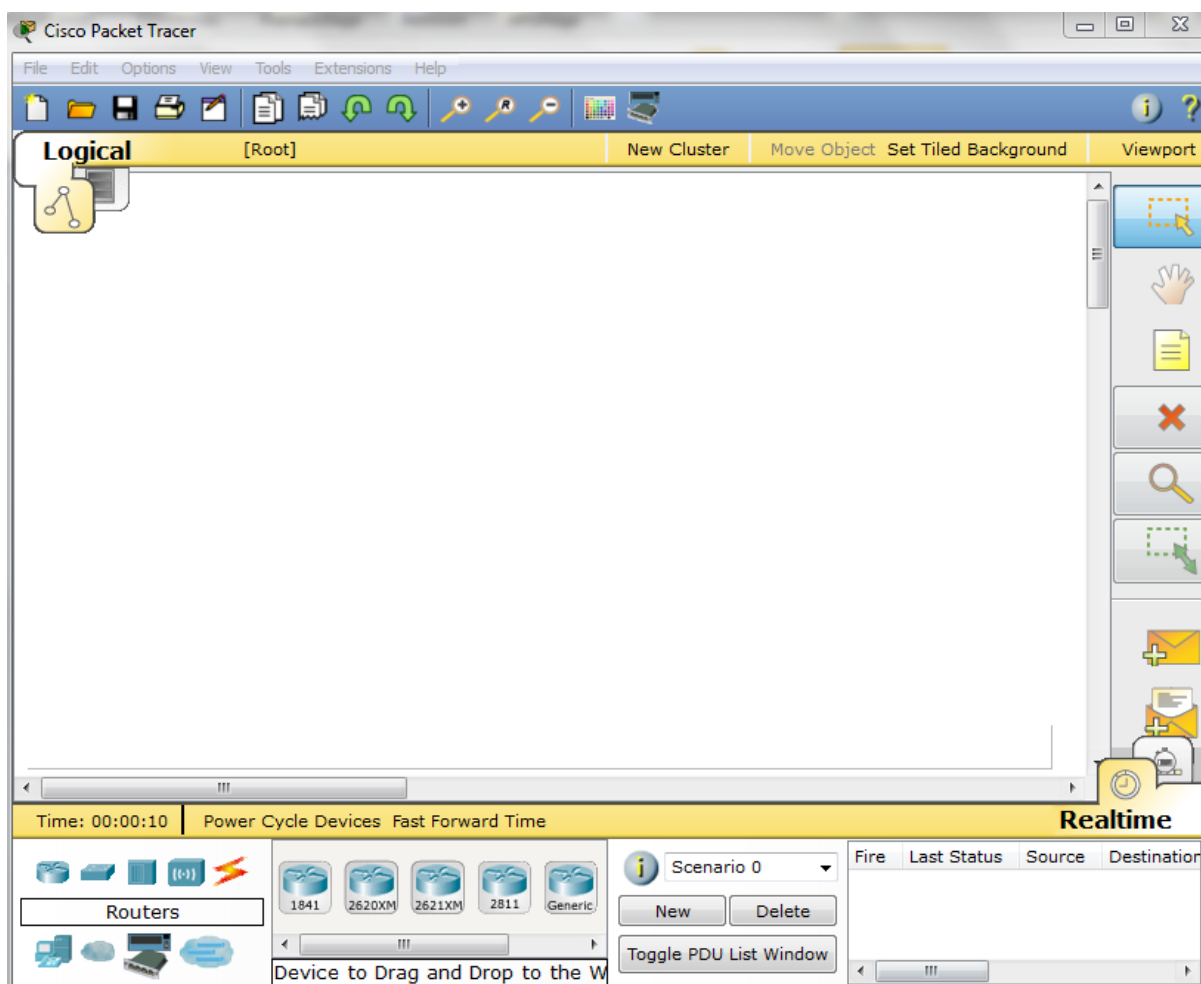
التعرف على برنامج Cisco Packet Tracer

هو برنامج تم تصميمه من قبل أكاديمية Cisco لمحاكاة الواقع في تصميم الشبكات و توفير جميع قطع Hardware الخاصة في تصميم الشبكة

لماذا صمم برنامج Cisco Packet Tracer ؟

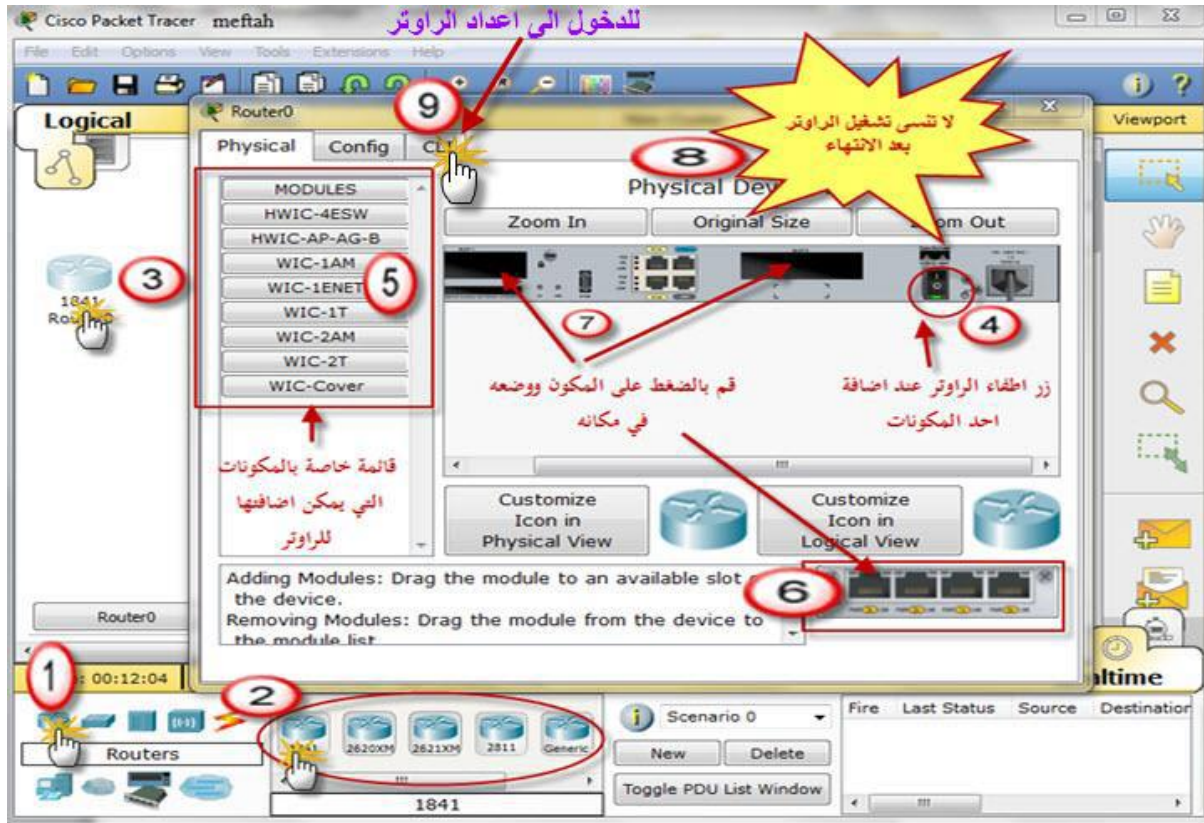
لكي يتم تصميم الشبكات بالمحاكاة , و السبب ان الافراد لا تستطيع توفير عدد الاجهزة الكافية لتصميم شبكة حقيقية فعلية على ارض الواقع , فتم برمجة البرامج ليحاكي الواقع في تصميم الشبكة .

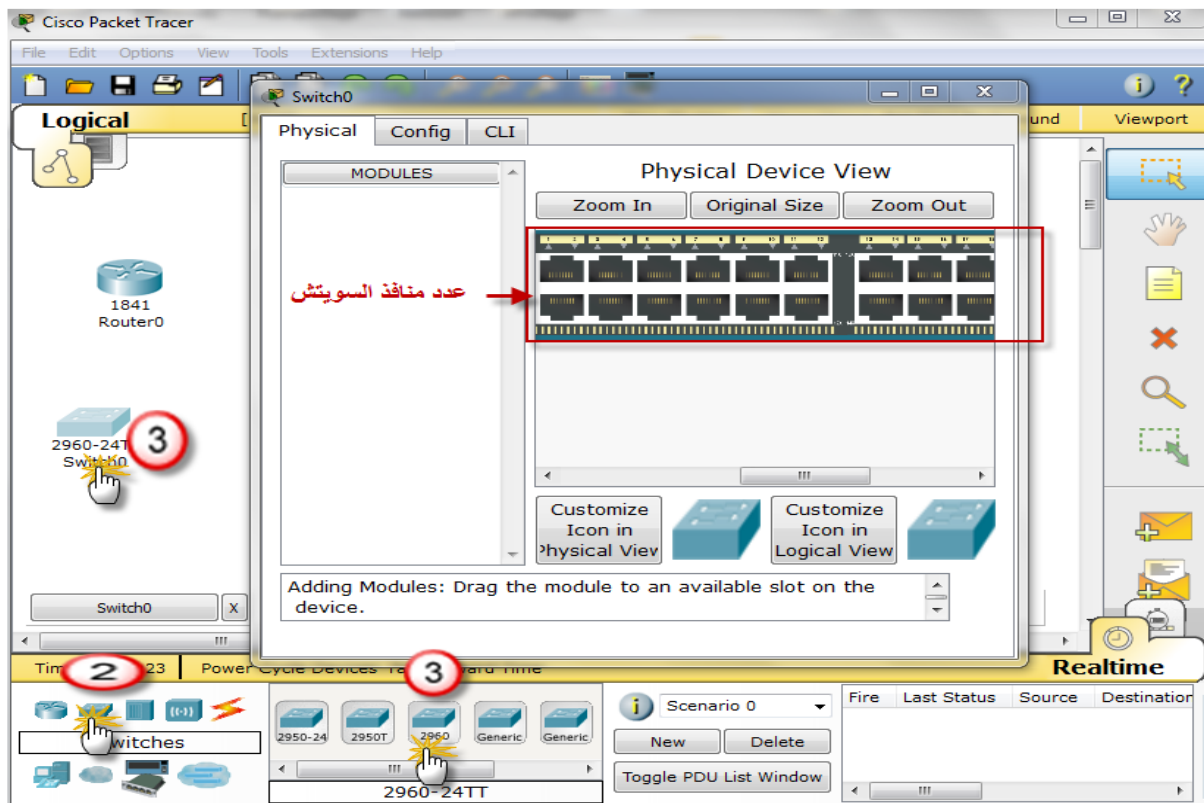
بعد تثبيت البرنامج و تشغيله تظهر الواجهة الرئيسية كما بالصورة التالية :



مكونات البرنامج :

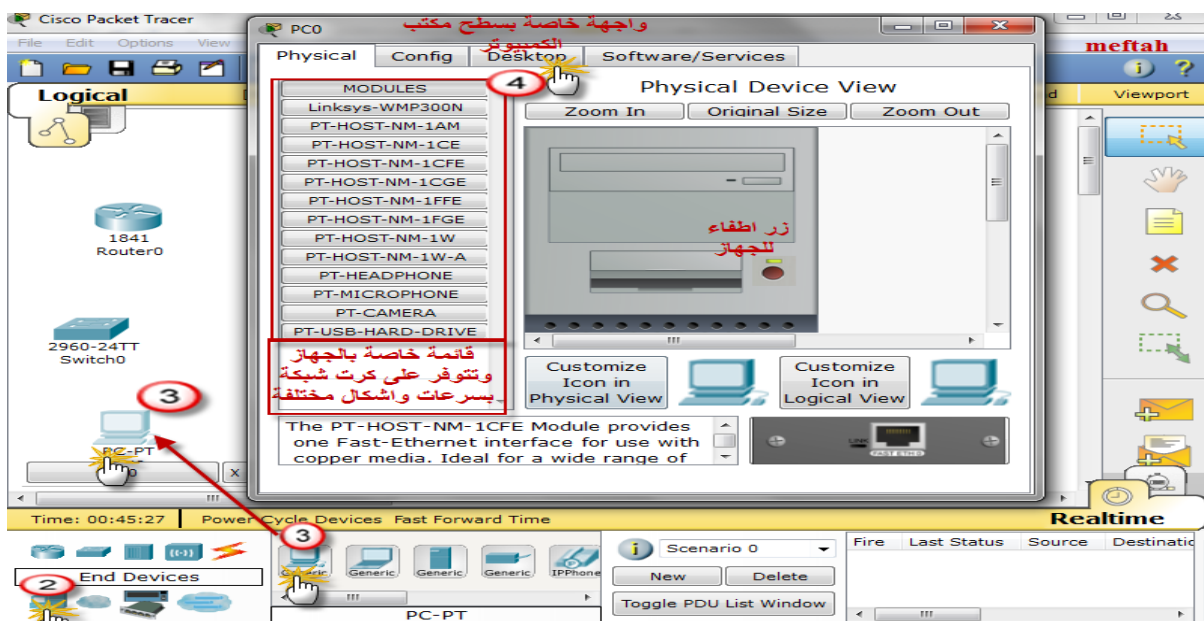
يحتوي مجموعة من الموجهات بمختلف الاصدارات و يمكن اضافة مكونات خاصة بالراوتر الصورة توضح:





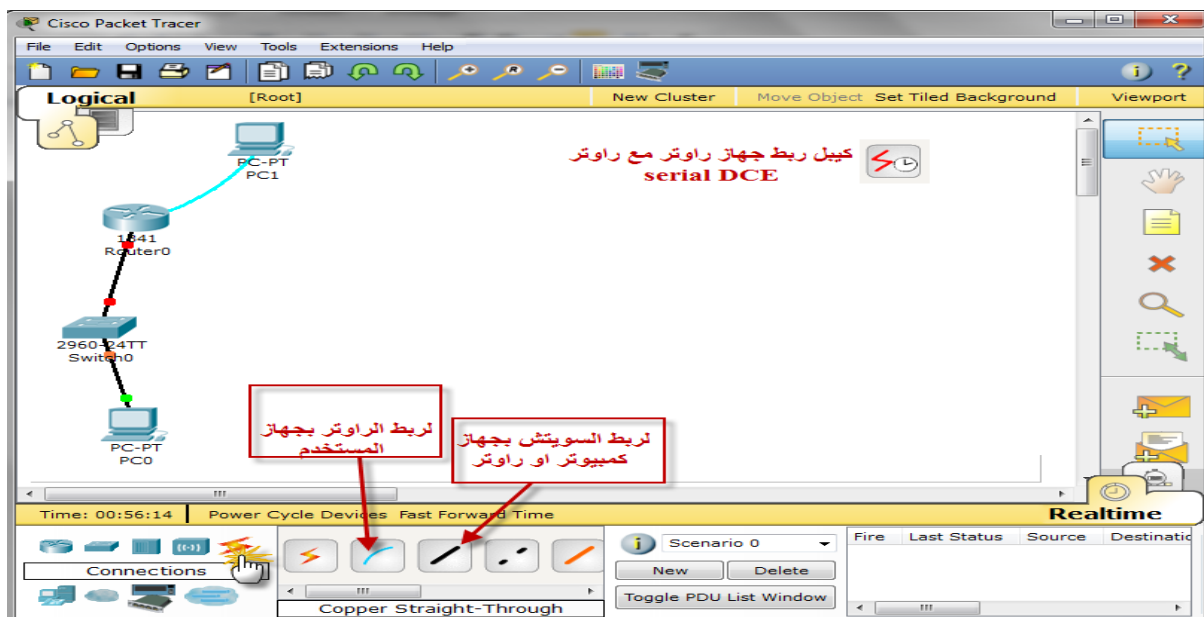
ويحتوي ايضا على اجهزة كمبيوتر بمختلف انواعها حيث يمكن ان تتحكم فيها وكأنك جالس امام الكمبيوتر

والصورة توضح



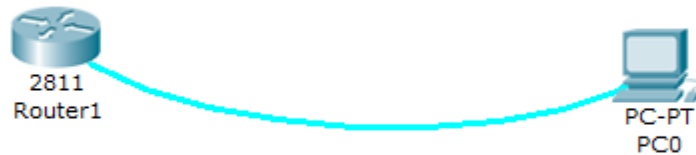


ويحتوي ايضا على مختلف انواع الكوابل المستخدمة في توصيل الشبكات كما في الواقع والصورة توضح



مختصر شبكات سيسكو CCNA Routing and Switching

بعد ربط جهاز الراوتر بكمبيوتر بواسطة كيبول Console و تشغيلها و الدخول الي برنامج HyperTerminal للبدء باعداد راوتر جديد , و في حال استخدام برنامج Cisco Packet Tracer يكون التوصيل كما يظهر في الصورة



اول شي سنعرف اصدار النظام الخاص بالراوتر , و لمعرفة اصدار الراوتر نستعمل الامر `show version` و نكتب الامر في مرحلة , وضع المتميز Privilege Mode

الصورة توضح :

```
Router>ena
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T
1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

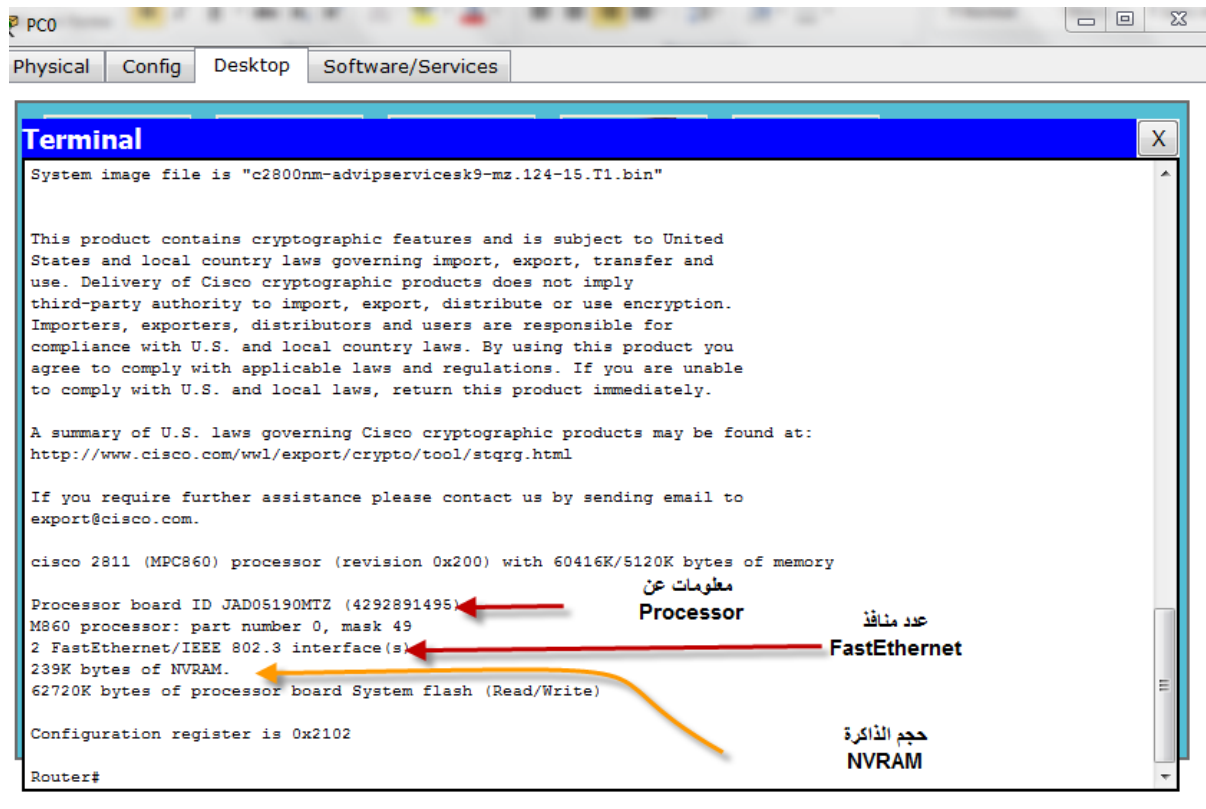
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
--More--
```

Diagram illustrating the connection between a router (2811 Router1) and a PC (PC-PT PC0) via a blue cable.

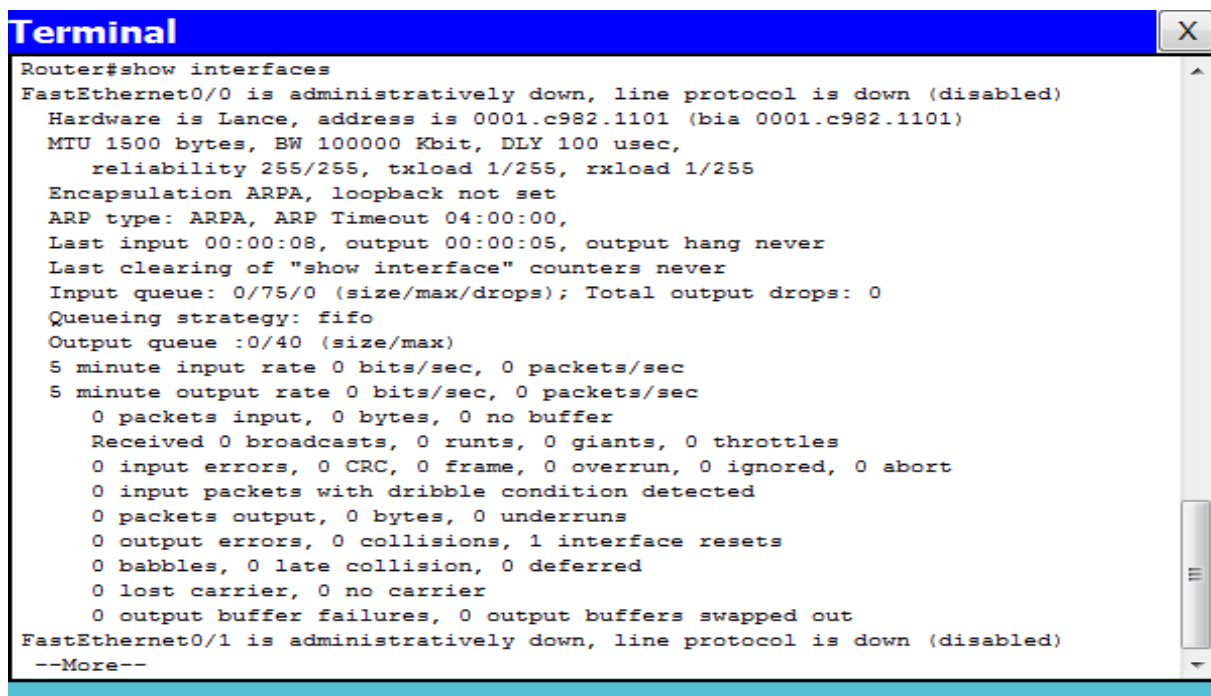
Terminal output showing the command `Router#show version` and the resulting system information. Red arrows point to the version string `Version 12.4(15)T` and the system image file `"c2800nm-advipservicesk9-mz.124-15.T1.bin"`.

مختصر شبكات سيسكو CCNA Routing and Switching

هناك معلومات أخرى خاصة بالراوتر نضغط زر انتر لمشاهدة المزيد



الان سنلقى نظرة على منافذ الراوتر بالأمر `show interfaces` ستظهر معلومات خاصة بكل منفذ على التوالي .



من الصورة السابقة نلاحظ ان جميع المنافذ الخاصة

بالراوتر ليس لها عناوين ip address و ذلك راجع لان الموجه جديد , و الان سنقوم بادخال العناوين لكل منفذ باستخدام الامر config t بهذا الامر ننتقل الي مرحلة التكوين العام global configuration mode

تسمية الراوتر : و هي عبارة عن اسم تعريف للراوتر و نستخدم الامر hostname كما في الصورة و بعد الامر مباشرة نكتب اسم الراوتر

عنوان المنافذ : ip address و نستخدم الامر interface fastethernet 0/0 و نضغط على زر انتر ثم ياخذنا الي مرحلة فرعية و بعد ذلك نكتب الامر التالي متبوع بعنوان الشبكة

```
ip address 192.168.1.100 255.255.255.0
```

ثم نقوم بتشغيل المنفذ بالامر no shutdown

و نعيد نفس الخطوات مع fastethernet 0/1

ثم نقوم بالخروج من المرحلة الفرعية بالامر exit او مباشرة بالضغط على زر ctrl+z و بعدها نقوم بحفظ العمل الذي قمنا به بالامر copy run start سيطلب منك ملف الأعداد اتركه كما هو و اضغط على زر انتر

الصورة توضح جميع الخطوات السابقة:

Terminal

```
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>ena
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname actel
actel(config)#int fa 0/0
actel(config-if)#ip address 192.168.0.1 255.255.255.0
actel(config-if)#no shutdown

actel(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

actel(config-if)#exit
actel(config)#int fa 0/1
actel(config-if)#ip address 192.168.1.1 255.255.255.0
actel(config-if)#no shutdown

actel(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

actel(config-if)#exit
actel(config)#exit
actel#
%SYS-5-CONFIG_I: Configured from console by console

actel#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
actel#
```

```
actel#config t
Enter configuration commands, one per line. End with CNTL/Z.
actel(config)#int s 0/2/0
actel(config-if)#ip address 192.168.2.1 255.255.255.0
actel(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
actel(config-if)#exit
actel(config)#int s 0/2/1
actel(config-if)#ip address 192.168.3.1 255.255.255.0
actel(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down
actel(config-if)#exit
actel(config)#exit
actel#
%SYS-5-CONFIG_I: Configured from console by console

actel#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
actel#
```

حماية الراوتر بكلمة مرور :

كلمة مرور لفتح نظام التشغيل : enable password

```
R1#  
R1#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#  
R1(config)#enable password xxxx  
R1(config)#
```

لحماية الراوتر من دخول غير المصرح لهم علينا تفعيل رمز دخول الي الراوتر , و يمكن ذلك بوضع الامر في مرحلة التكوين العام (global configuration mode)

Enable password xxxx

للتأكد من تأثير كلمة المرور على الراوتر , يمكن ان نعيد تشغيل الراوتر او الخروج بامر exit ثم الدخول مرة ثانية .

```
<Router  
Router>enable  
:Password  
:Password  
:Password
```

ملاحظة : عند كتابة رمز الدخول يكون مخفيا و ذلك تحسبا من كشف رمز الدخول من قبل اشخاص اخرين , اذا عرف عدد الكلمات من المحتمل كشف الرمز.

كلمة المرور على المنفذ console :

```
R1#  
R1#config t  
.Enter configuration commands, one per line. End with CNTL/Z  
R1(config)#line console 0  
R1(config-line)#password xxxx  
R1(config-line)#login  
R1(config-line)#exit
```

مختصر شبكات سيسكو CCNA Routing and Switching

نستعمل الامر line console 0 سيدخلنا الي مرحلة فرعية ثم نكتب

password xxxx اي رمز من اختيارك وبعد ذلك ندخل الامر login و في الاخير الامر exit للخروج

كلمة المرور على مدخل telnet :

```
#(R1(config) t
R1(config)#line vty 0 4
R1(config-line)#password xxxx
R1(config-line)#login
R1(config-line)#exit
```

نستعمل الامر line vty 0 4 من ثم ندخل كلمة السر password xxxx

و تعني هذه العبارة ان من 0 الي 4 اشخاص يستطيعون عمل telnet في نفس الوقت و الدخول للموجه من بعد بواسطة اي جهاز كمبيوتر متصل على محيط الشبكة , وبعد ذلك ندخل الامر login و من ثم الامر exit للخروج

و نقوم بحفظ الاعدادات بالامر التالي : copy run star

و لمعرفة عنوان المداخل و قناع الشبكة و اسم الراوتر و كل التفاصيل :

نستخدم الامر show run

```
R1#show running-config
...Building configuration

Current configuration : 635 bytes
!
version 12.4
!
hostname R1
!
enable password 123
!

interface FastEthernet0/0
ip address 192.168.1.100 255.255.255.0
```



```
!  
interface FastEthernet0/1  
ip address 192.168.2.100 255.255.255.0  
  
!  
line con 0  
password xxxx  
login  
!  
line aux 0  
!  
line vty 0 4  
password xxxx  
login  
!  
End
```

نلاحظ في الشكل اعلاه جميع رموز الراوتر تظهر في شكلها الحقيقي في عرض الامر `show run` مما يزيد احتمال كشف رموز الدخول و لمزيد من السرية في عرض كلمات المرور نستخدم الامر `service password-encryption` , لتشفير الرموز عندما نستعرض امر `show run`

```
actel(config)#service password-encryption  
actel(config)#^Z  
actel#  
%SYS-5-CONFIG_I: Configured from console by console  
  
actel#copy run start  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
actel#
```

عرض امر `show runn` بعد تشفير الرموز:

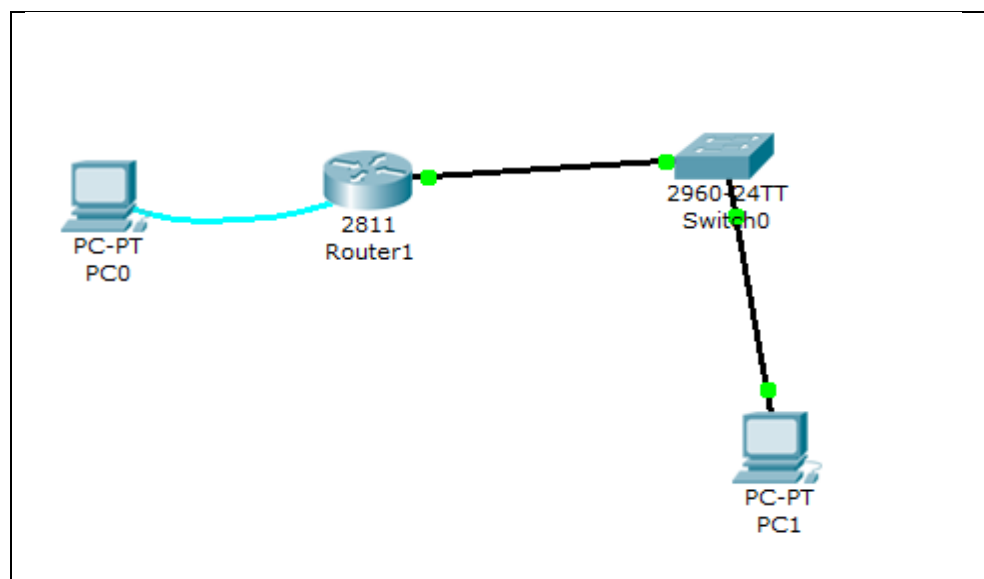
```
!  
line con 0  
password 7 0870151650  
login  
line vty 0 4  
password 7 087015165F  
login  
!  
!  
!  
end
```

```
actel>ena
actel#config t
Enter configuration commands, one per line. End with CNTL/Z.
actel(config)#enable secret 2012 ← 1
actel(config)#^Z
actel#
%SYS-5-CONFIG_I: Configured from console by console

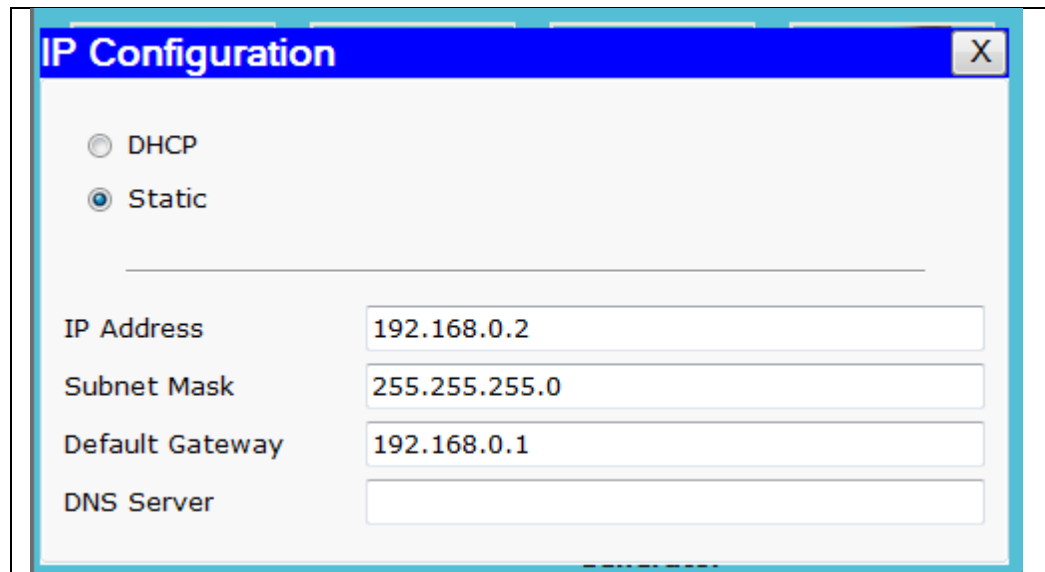
actel#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
actel#show start ← 2
Using 698 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname actel
!
!
!
enable secret 5 $1$mERr$JzbYlId3ASDMhZ/P4nPWq1
!
!
!
```

الدخول الي الراوتر عن طريق telnet:

للدخول الي الراوتر من خلال telnet سوف نربط جهاز الراوتر مع switch و السويتش مع جهاز حاسوب. كما في الصورة الاتية

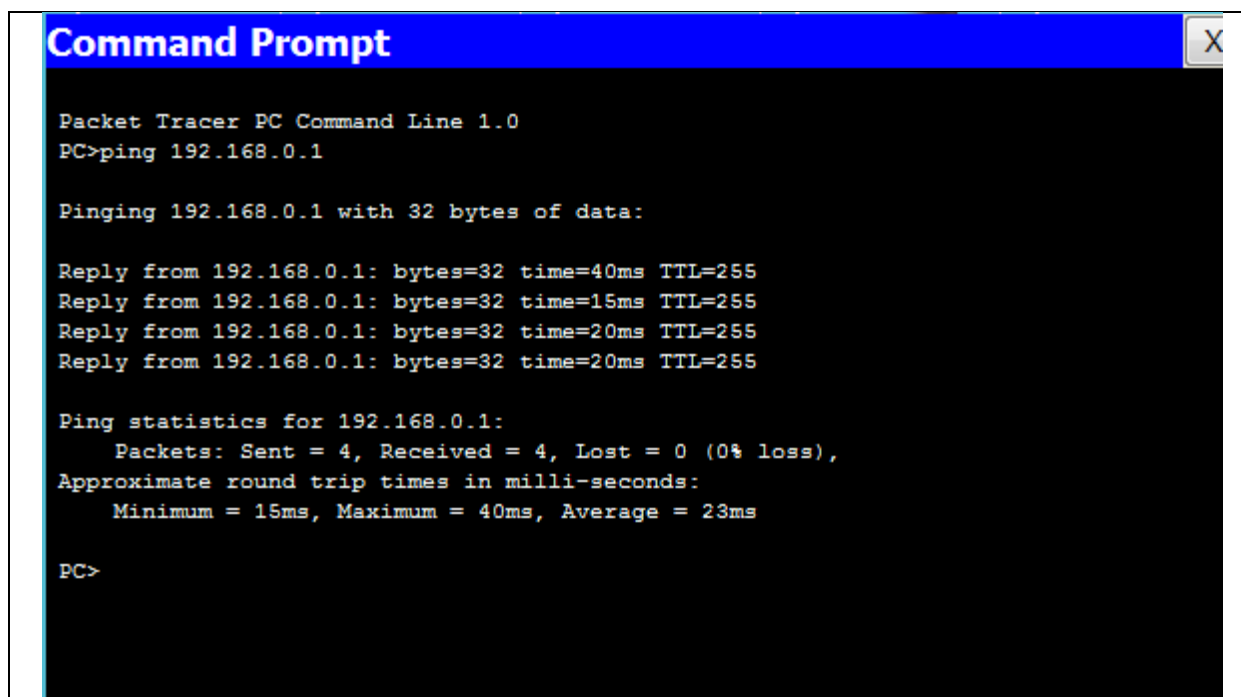


و نعطي الحاسوب عنوان و قناع الشبكة ip address and subnet mask and default gateway



The image shows a screenshot of the 'IP Configuration' window in a network simulation software. The window has a blue title bar with the text 'IP Configuration' and a close button (X). Inside the window, there are two radio buttons: 'DHCP' and 'Static'. The 'Static' radio button is selected. Below the radio buttons, there are four input fields with labels: 'IP Address' (containing '192.168.0.2'), 'Subnet Mask' (containing '255.255.255.0'), 'Default Gateway' (containing '192.168.0.1'), and 'DNS Server' (which is empty).

الان سنتحقق من الاتصال بواسطة الامر ping من جهاز الحاسوب و سنلاحظ بانها تمت بنجاح
كما في الصور :



The image shows a screenshot of a 'Command Prompt' window in a network simulation software. The window has a blue title bar with the text 'Command Prompt' and a close button (X). The background is black with white text. The text inside the window is as follows:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=40ms TTL=255
Reply from 192.168.0.1: bytes=32 time=15ms TTL=255
Reply from 192.168.0.1: bytes=32 time=20ms TTL=255
Reply from 192.168.0.1: bytes=32 time=20ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 40ms, Average = 23ms

PC>
```

مختصر شبكات سيسكو CCNA Routing and Switching

و الان من الموجه نقوم بنفس العملية ستلاحظ علامات تعجب و هي 5 تدل على ان العملية تمت بنجاح
اما ان ظهر مكان علامات التعجب نقاط هذا يدل على ان العملية لم تتم بنجاح .

```
User Access Verification

Password:

actel>ena
Password:
actel#ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

actel#
```

الدخول للراوتر بواسطة " Telnet "

الان سنقوم بعملية الدخول الي الموجه عن طريق telnet من جهاز الحاسوب و ندخل الامر التالي في مربع Run و من ثم CMD 192.168.1.100 telnet متبوع بعنوان منفذ الراوتر الذي ينتمي اليه و سيطلب منك كلمة السر الخاصة بالراوتر و خاصة الدخول عن طريق telnet

الصورة توضح:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=40ms TTL=255
Reply from 192.168.0.1: bytes=32 time=15ms TTL=255
Reply from 192.168.0.1: bytes=32 time=20ms TTL=255
Reply from 192.168.0.1: bytes=32 time=20ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 40ms, Average = 23ms

PC>telnet 192.168.0.1
Trying 192.168.0.1 ...Open

User Access Verification

Password:
actel>
```

عناوين الشبكات : IP Addressing

يجتاز كل جهاز كمبيوتر الى عنوان رقمي للتواصل و هذه العناوين تعرف ب IP Address

خصائص ال IP Address

من خصائص عناوين الكمبيوتر ان يكون جميع الحواسيب في نفس الشبكة المحلية تحمل نفس عنوان الشبكة و على ان لا يتكرر عنوان ال ip address

* عنوان ال ip من الاصدار الرابع اي ip v4 و هي عبارة عن ارقام مكونة من اربع خانوات كل خانة يتسع للارقام من 0 الي 255 يتم فصل كل خانة من الاخر بنقطة

* ينقسم عناوين الشبكة الي ثلاثة اقسام حسب توزيع الخانات ip address class

Class A 1 : يعرف هذا النوع على ان يكون الخانة الاولى عنوان الشبكة (اي يكون الرقم ثابت في جميع عناصر الشبكة) و يحمل الارقام من 1 الي 126

مثلا :: 10.0.0.0 و يجب تمييز على انه كلاس A بواسطة حالة اضافية تسمى Subnet mask (او قناع الشبكة)

مثلا Class A مع ال subnet mask تكتب !! 10.0.0.0 255.0.0.0

Class B 2 : يعرف هذا النوع على ان يكون الخانة الاولى و الثانية عناوين الشبكة (اي يكون ارقام الخانتين ثابتين في كل عناصر الشبكة)

و يعرف Class B بالارقام من 128 الي 191

مثلا : 172.16.0.0 كما علمنا سابقا هناك حالة تمييز كل كلاس و تسمى Subnet mask او قناع الشبكة

مثلا class B مع Subnet mask تكتب 172.16.0.0 255.255.0.0

Class C 3 : يعرف هذا النوع على ان يكون الخانة الاولى و الثانية و الثالثة عناوين للشبكة (اي ارقام ال 3 خانوات تكون ثابتة في جميع عناصر الشبكة)

و يعرف بالارقام من 192 الي 230

مثلا : 192.168.1.0 و يكتب مع subnet mask 192.168.1.0 255.255.255.0

انواع الرسائل بين اجهزة الشبكات :

- ❖ إرسال رسالة إلى عقدة واحدة: Unicast
- ❖ إرسال رسالة الي كل العقد : Broadcast
- ❖ إرسال رسالة لمجموعة محددة: Multicast

❖ Unicast :

طرق ارسال البيانات من وحدة ارسال الي وحدة استقبال دون مشاركة وحدات اخرى , اي اتصال من نقطة الي نقطة ,, تسمى (Unicast Message)
و مثال لذلك طريقة التواصل بين اجهزة الجوال , التواصل بين كمبيوترين ذات توصيل سلك مباشر

الشكل يوضح توصيل جهازين بسلك مباشر :-

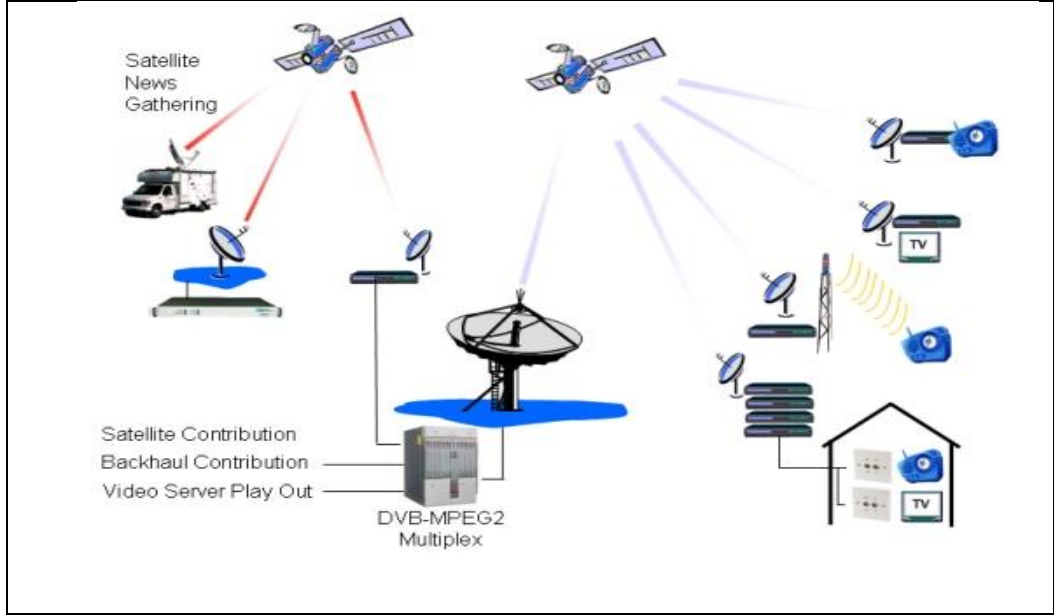


❖ Broadcast Message :

وهي عبارة عن مجموع من وحدات الاتصال الشبكي عندما تكون في نطاق تواصل واحد و تكون في عنوان شبكة واحدة و تستطيع تبادل الرسائل في ما بينها ,, اي من طرف واحد الي الكل
(Broadcast Message) تسمى

مثال :

في نظام الراديو و الفضائيات يكون البث Broadcast من محطة البث الرئيسي على نطاق محدود يحدد من قبل برج الارسال بحيث اي جهاز راديو ضمن نطاق البث يستطيع استقبال الموجان و هذا التواصل يسمى { Radio Frequency }

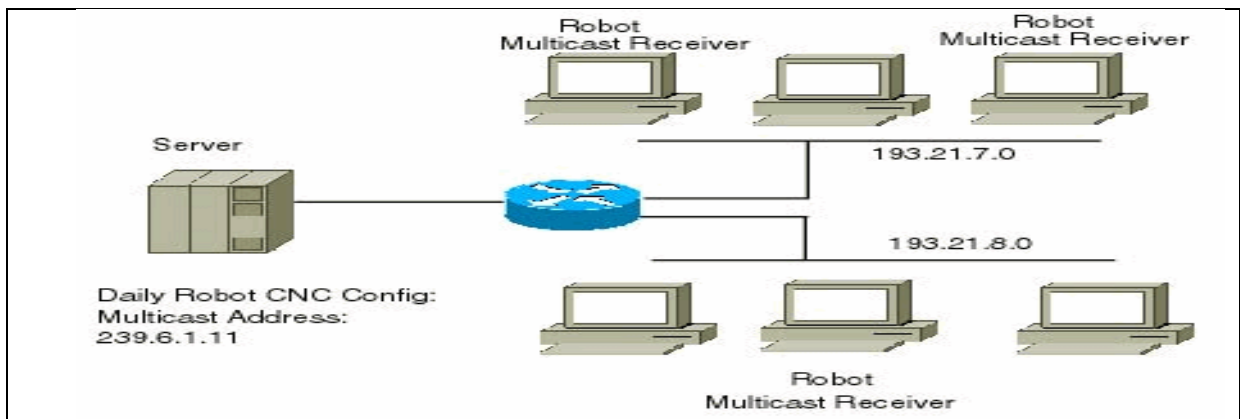


❖ Multicast

في شبكات الكمبيوتر multicast تعني الاتصال بين مجموعتين من جهات الاتصال في صورة ارسال بيانات من مجموعة الي مجموعة ثانية و يمكن ان تكون اكثر من مجموعتين , او من نقطة متصلة في شبكة الكمبيوتر الي مجموعة ذات صلة بارسال البيانات و من اشهر اشكال Broadcast طرق التواصل في البث التلفزيوني بين القنوات الفضائية , او ارسال حزمة البيانات من كمبيوتر الي مجموعة من عناصر الشبكة

كما يعرف ال multicast في ثلاثة اشكال رئيسية وهي

- من نقطة اتصال فردية الي نقطة اتصال فردية اخرى (من واحد الي واحد)
 - من مجموعة نقاط اتصال الي نقطة اتصال واحدة (من مجموعة الي واحد)
 - من مجموعة نقاط اتصال الي مجموعة نقاط اتصال اخرى (من مجموعة الي مجموعة)
- الشكل يوضح الاتصال من الخادم الي مجموعة الحواسيب



التوجيه Routing

التوجيه هو العملية التي يستخدمها جهاز التوجيه Router لاعادة توجيه الحزم Packet في اتجاه الشبكة . يقوم جهاز التوجيه باتخاذ القرارات استنادا الي عنوان ip internet protocol الخاص بالحزمة . و تستخدم كافة الاجهزة عبر طريقها عنوان ip لارسال الحزمة في الاتجاه الصحيح حتى تصل الي وجهتها . لاتخاذ القرارات الصحيحة , يجب ان تعرف اجهزة التوجيه كيف تصل الي الشبكات البعيدة .

عندما تستخدم اجهزة التوجيه الديناميكي , يتم التعرف على هذه المعلومات من قبل اجهزة التوجيه الاخرى . اما اذا عند استخدام التوجيه الثابت , يقوم مسؤول الشبكة بتكوين معلومات حول الشبكات البعيدة يدويا.

وما دام يتم تكوين المسارات الثابتة يدويا , فيجب على مسؤول الشبكة اضافة و حذف مسارات ثابتة لعكس اي تغييرات في هيكل الشبكة . في الشبكة الضخمة قد تتطلب الصيانة اليدوية لجدول التوجيه كثيرا من الوقت الاداري . اما على الشبكات الصغيرة ذات التغييرات القليلة , فان المسارات الثابتة فيها لا تتطلب صيانة لجدول التوجيه بصفة دائمة

انواع التوجيه :

التوجيه الديناميكي :

في هذا التوجيه, يتولى الراوتر بنفسه مهمة ايجاد المسارات المؤدية الي الشبكات المختلفة مستعينا ببروتوكولات التوجيه و مهمة مدير الشبكة هنا هي فقط تفعيل بروتوكول التوجيه المناسب و تعريف الشبكات ومن ثم ترك الباقي لعمل الموجه في هذا النوع من التوجيه , تبني جداول التوجيه بشكل متغير تبعا لأفضلية المسار , يناسب هذا التوجيه في الشبكات الممتدة و الاكثر تعقيدا , و يتم ذلك بواسطة تقنيات معينة تدعى بروتوكولات ,

ما هو البرتوكول ؟

البرتوكول هو مجموعة من الانظمة تحدد كيف سيتم الإتصال بين الموجهات ونشر المعلومات التي تمكنهم من تحديد الطريق بين عقدتين(جهازين) على الشبكة حيث يتم إختيار الطريق وفق خوارزميات محددة. يشير تعبير بروتوكول التوجيه إلى الطبقة الثالثة في نموذج الطبقات السبعة .

يوجد نوعين أساسيين من بروتوكولات التوجيه و هي :

❖ Distance factor :

وهي عبارة عن بروتوكولات تعتمد على بعد المسافة بين اجهزة الراوترات وعدد اجهزة الشبكات التي يتم تخطيها للوصول الي المكان المعني .

❖ Linked-state :

وهي بروتوكولات تعتمد على عدة واصفات لتحديد الطريق الافضل

الخصائص و المميزات المشتركة في النوعين :-

- ❖ اختيار الطريق الافضل بين خطوتين اعتمادا على كلفة الخطوة " Cost " .
- ❖ منع حدوث الحلقات المغلقة في الشبكة و كسرها ان حدث " loop prevention " .
- ❖ اختيار افضل طريق " Best path selection " .

ينقسم البروتوكولات على حسب الية العمل الي نوعين :

بروتوكولات التوجيه الداخلية :-

(*Interior routing protocols*)

مثال *Inernet , BGP Routing Protocol*

(*Exterior Gateway Protocol*)

Interior Gateway Protocol (IGP)

سميت بروتوكولات التوجيه الداخلية لانها مصممة للاستخدام في جانب نظام مفرد مستقل(شبكة يتحكم بها المسئول في مؤسسة ما) مثل

✚ *EIGRP* (Enhanced Interior Gateway Routing Protocol)

✚ *OSPF* (Open Shortest Path First)

✚ *RIP* (Routing Information Protocol)

التوجيه الثابت Static Route :

يستخدم توجيه مبرمجا يقوم مسؤول الشبكة بإدخاله في جهاز التوجيه و سوف تسلك البيانات دائما هذه المسارات حتى يتم تعديلها من جديد.

يعتبر التوجيه الثابت static route اصعب من dynamic routing لانه يتطلب جهد و معرفة كاملة بمسارات الشبكة

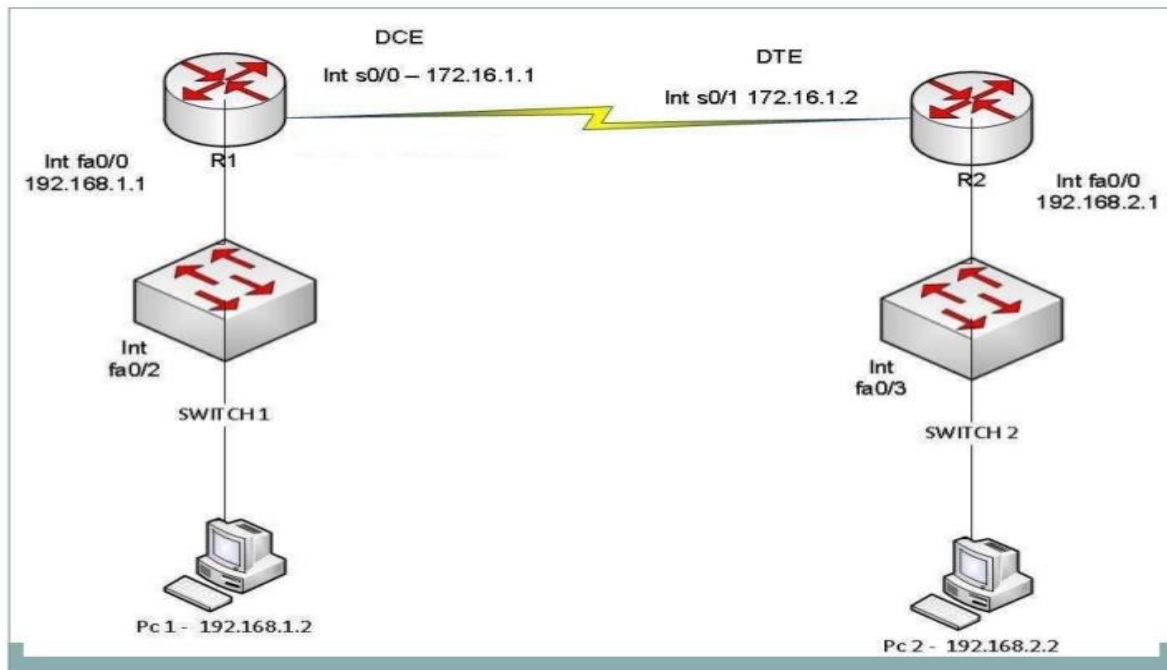
ضبط التوجيه الثابت بين فرعين او راوترين حيث كل راوتر يتمثل فرع نقطة عمل كما في المثال ادناه R1 و R2

يكون الاوامر كالآتي : من راوتر R2 يجب التوجيه الي الشبكة المحلية لدى R1 و العكس ..

```
R2 – ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

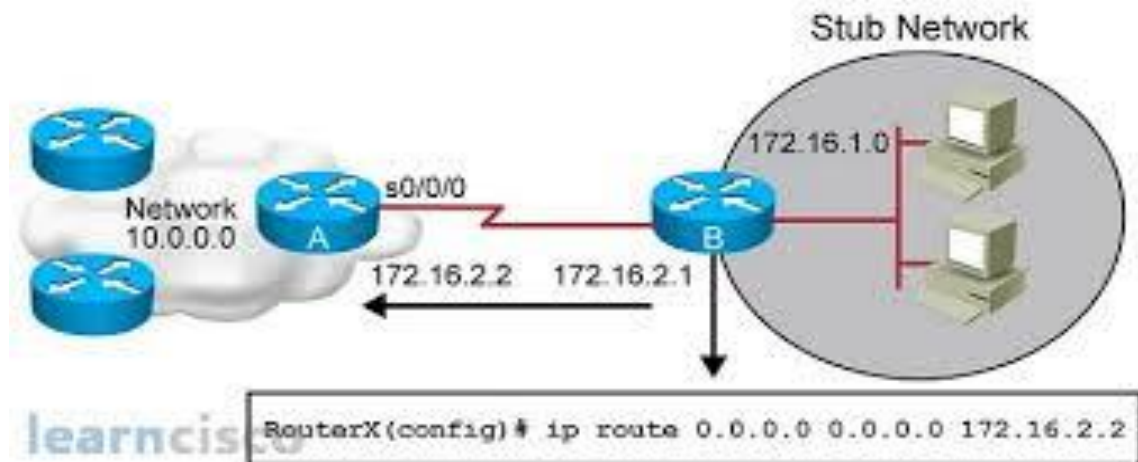
التوجيه العكسي من راوتر R1 الي R2

```
R1 – ip route 192.168.2.0 255.255.255.0 172.16.1.2
```



المسار الافتراضي : (Default Route)

في شبكات الكمبيوتر، المسار الافتراضي هو إعداد على جهاز كمبيوتر تحدد حكم توجيه الحزمة لاستخدامها عند تعذر تحديد أي مسار محدد لعنوان (IP) بروتوكول الإنترنت. يتم إرسال كافة الحزم لجهة تحده في جدول التوجيه عبر المسار الافتراضي ، و أيضا يعتبر من وسائل الحصول على الانترنت لجميع مستخدمي الشبكة .



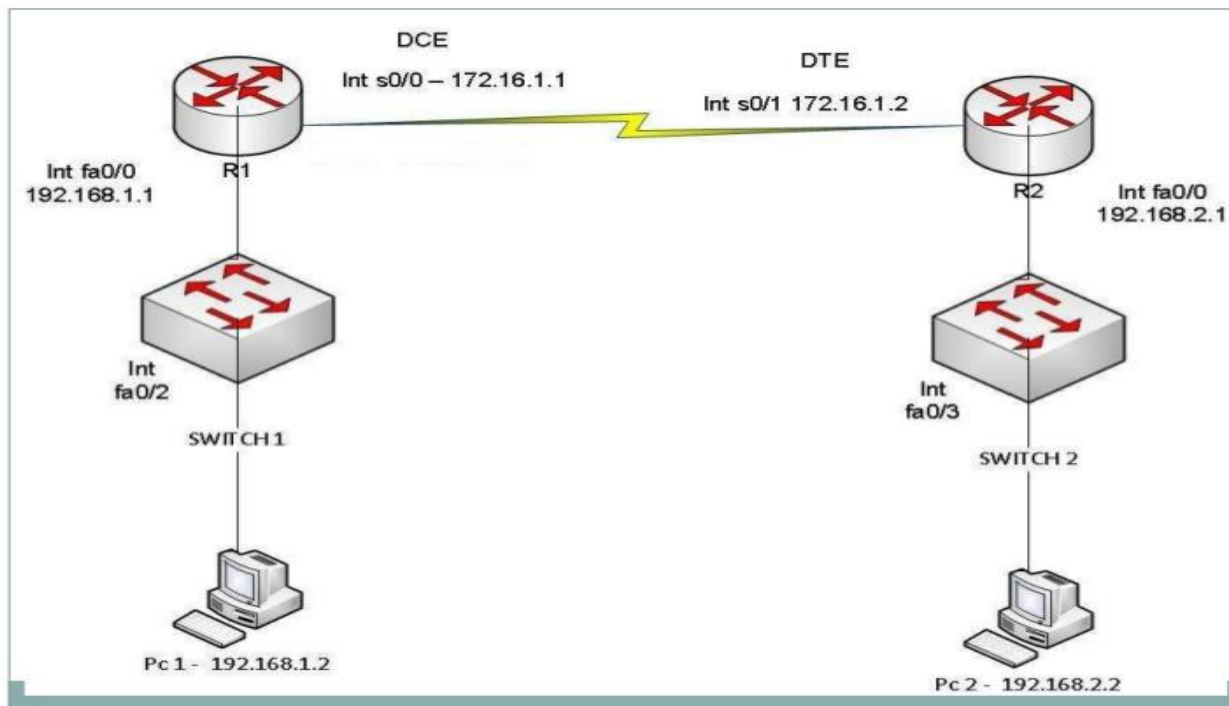
Default Route:

```
lR1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

جداول التوجيه :

ويقوم ببنائه في التوجيه الديناميكي بروتوكولات التوجيه اما في التوجيه الثابت يقوم مدير الشبكة ببناء جدول التوجيه.

بروتوكول التوجيه ريب :- (Routing Information Protocol) RIP



RIP اختصار لـ (Routing Information Protocol) هو بروتوكول توجيه ديناميكي يستخدم في الشبكات المحلية و الواسعة. ويصنف كبروتول عبارة داخلية (IGP) و يستخدم من خوارزميات التوجيه خوارزمية شعاع المسافة.

أول تعريف له كان ب [RFC 1058](#) عام 1988م. تم توسيعه عدة مرات, و أدى ذلك لإنتاج الإصدار الثاني منه RIP2 في [RFC 2453](#) و كلا الإصدارين ما يزالان قيد الاستخدام في أيامنا هذه, على الرغم من ظهور تقنيات أكثر تقدماً مثل تقنية (فتح أقصر مسار أولاً) " OSPF " و بروتوكول " IS-IS " كما تم إصدار نسخة من بروتوكول RIP متأقلمة مع البروتوكول IPV6 و هي المعيار المعرف ببروتوكول (RIPng الجيل التالي) الذي تم رفعه ب [RFC 2080](#) عام 1997.

تفعيل بروتوكول ريب الإصدار الثاني في الراوتر:- RIPv2 Configuration:

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 172.16.0.0      ! subnet mask option
R1(config-router)# no auto-summary
```

لمعرف عمل البروتوكول و فحص الاوامر: RIPv2 Verification:

- Shows information about the running routing protocol process:

- لمعرفة اي بروتوكولات التوجيه يعمل حاليا في الراوتر نستخدم الامر الاتي :-

```
R1# show ip protocols
```

- Shows the entire routing table:
• لعرض جميع عناوين التوجيه في جدول الراوتر (اي ما يمكن وصوله من قبل الراوتر) :-

```
R1# show ip route
```

- Shows routes learned ia RIP only:
• لعرض العناوين المتعرف عليها من قبل ريب (RIP) فقط .

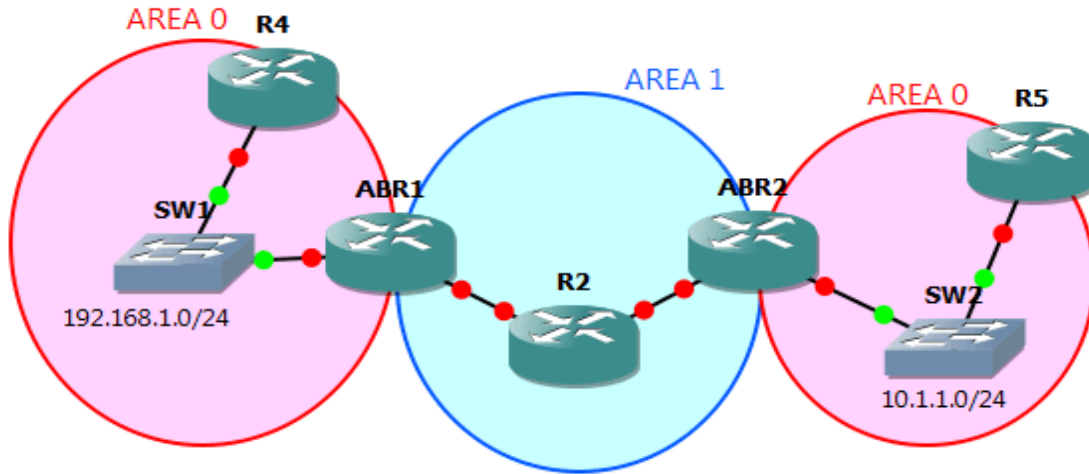
```
R1# show ip route rip .
```

Shows detailed information about the route to the specified destination network:

- لعرض تفاصيل وافية عن عنوان شبكة معينة من مجموعة الشبكات المتعرف عليها في " جدول النواين " (Routing Table)

```
R1# show ip route 192.168.3.0
```


بروتوكول التوجيه (افتح اقصر مسار اولاً) (OSPF (Open Shortest Path First



الـ (OSPF) هو بروتوكول مفتوح (open standard) يمكن أن يعمل على أجهزة الشبكات مصنعة من عدة شركات بما فيها شركة سيسكو.

يمتاز الـ (OSPF) بخصائص ومبادئ (link state) والتي أهمها ارسال التحديثات لأجهزة الراوترات بسرعة عالية , اي لحظة وقوع الحدث (event-triggered)، مما يؤدي لاستقرارية (جدول العناوين) الـ (routing tables) للراوترات. ويعمل الـ (OSPF) على منظومة تحتوي على عدد كبير من الشبكات، ولا يوجد تحديد لعدد الشبكات او عدد معين لأجهزة الراوتر العاملة في المنظومة كما هو الأمر بالنسبة لبروتوكول الـ (RIP).

يستخدم الـ (OSPF) خوارزمية الـ (Shortest Path First) وذلك من أجل حساب افضل مسار لكل شبكة.

يعمل هذا البروتوكول على اساس منظومات متداخلة تسمى (Area) كل منظومة ويعطى لكل منظومة رقم تعريف تعرف بـ (Area ID) و دائماً ما يبدأ برقم تعريف المنظومة بالرقم صفر و لابد من باقي المنظومات الاتصال بالمنظومة صفر , ويقوم الـ (OSPF) بارسال تفاصيل عن الشبكات الموجودة داخل المنظومة ولا يقتصر الأمر على عنوان الشبكة الـ (network address) فقط، بل تحتوي المعلومات المرسلة عن الشبكات، نوع الشبكة وعنوان الشبكة ورقم تعريف الراوتر الـ (Router ID) المعلن عن هذه الشبكة بالإضافة لتفاصيل أخرى.

يقوم كل راوتر بالاعلان عن الوصلات (links) التي لديه والمفعلة ضمن عمل البروتوكول وكذلك الوصلات التي تعلمها من خلال بروتوكول الـ (OSPF) والموجودة لدى الراوترات الأخرى. تستخدم الـ ("Link State Advertisements" LSAs) لنشر التفاصيل عن الوصلات الموجودة داخل المنظومة.

والجدير بالذكر بأن تفاصيل الشبكات التي تعنى بها الراوترات هي بالأساس موجودة على وصلات، أي أن طبيعة الوصلات وصفتها ينعكس على طبيعة الشبكة وصفتها، ولهذا السبب اعتمد تسمية الوصلات بدل من الشبكات.

يستخدم الـ (OSPF) قيمة الـ (bandwidth) أي السرعة لحساب كلفة (metric) الوصول لأي شبكة، وتعتمد المعادلة المخصصة لحساب الكلفة على قيمة مرجعية تسمى الـ (reference bandwidth) وقيمتها الافتراضية (108) وتقسم القيمة المرجعية على قيمة الـ (bandwidth) لإيجاد الكلفة.

$$\text{metric} = 108 / \text{bandwidth}$$

من أهم مزايا الـ (OSPF) أنه (classless) أي أنه يدعم نقل المعلومات عن الشبكات الجزئية (subnetworks)، حيث تحمل التحديثات المرسله عن الشبكات قيمة الـ (subnet mask) لكل شبكة مهما كان طوله (VLSM).

وكذلك يمتاز الـ (OSPF) بنقل البيانات المتعلقة بالشبكات بموثوقية (reliability) نتيجة استخدام رسائل مخصصة (ACK message) لتأكيد استلام الرسائل المختلفة المرسله من الـ (OSPF). وهذا شبيه بمبدأ بروتوكول (TCP) الذي يمتاز بموثوقية نقل البيانات بين أجهزة المستخدمين لكنه يؤديها بطريقة مختلفة إذ يستخدم (TCP) خانة (Field) مخصصة لذلك ضمن الـ (header) المضاف على البيانات.

يعتمد بروتوكول الـ (OSPF) في عمله على خمسة أنواع من الرسائل (messages) وهي:

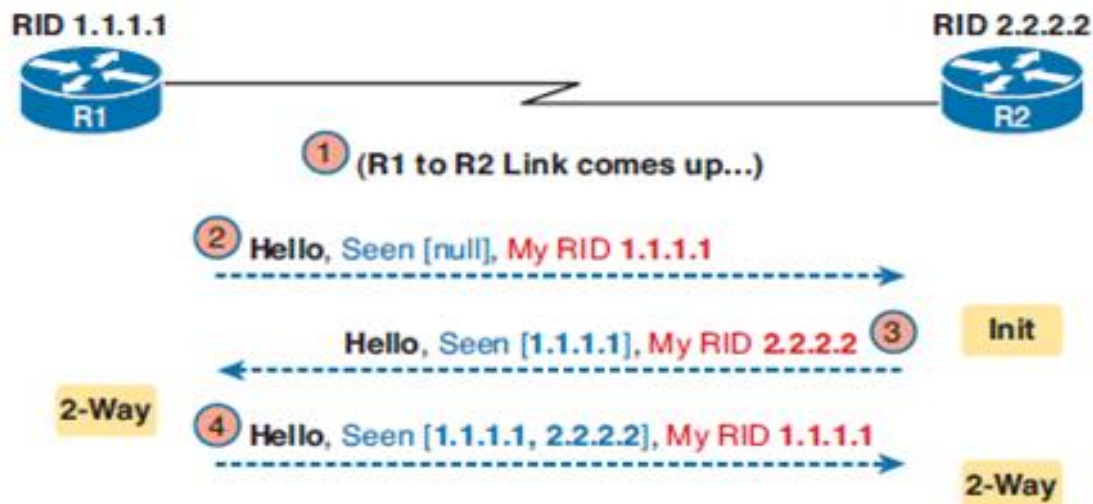
- 1- (Hello) تستخدم للتعرف عن الراوترات المجاورة والتي يعمل عليها الـ (OSPF) لتكوين علاقة تبادلية معها
 - 2- (Data Base Description (DBD) تستخدم لإرسال ملخص لقاعدة البيانات التي تحتوي على تفاصيل الوصلات الموجودة داخل المنظومة
 - 3- (Link State Request (LSR) تستخدم لطلب تفاصيل عن عدد من الوصلات المعروفة لدى أحد الراوترات المجاورة
 - 4- (Link State Update (LSU) تستخدم لإرسال التفاصيل عن عدد من الوصلات أو لإرسال تحديثات (updates) التي تجري على الوصلات. تحتوي الـ (LSU) على عدد كبير من الـ (LSAs)
 - 5- Acknowledgement تستخدم لتأكيد استلام أي إرسالية للـ (OSPF) عدا الـ (Hello)
- ويتم استخدام العنوان (224.0.0.5) لتوجيه هذه الرسائل أي يكون هذا العنوان بمثابة عنوان المرسل إليه الـ (destination address) لهذه الرسائل.

الاكتشاف والتبادل

يعمل الـ (OSPF) على اكتشاف راوترات مجاورة (automatic neighbor discovery) يعمل عليها نفس البروتوكول وذلك ليتم تبادل المعلومات الخاصة بالشبكات (الوصلات) (routing information exchange)، ولا تتم عملية التبادل أو إرسال تحديثات إلا من خلال منفذ يوصل لراوتر مجاور (neighbor router) يضاف بعد عملية الاكتشاف.

عند تشغيل بروتوكول الـ (OSPF) على الراوتر وتفعيل البروتوكول على أي منفذ (interface) للراوتر، يقوم الـ (OSPF) بإرسال (Hello packet) عبر المنفذ حامل معه رقم الراوتر (Router ID) ومعلومات أخرى، وفي حال وجود راوتر على الطرف الآخر للمنفذ الذي يعمل عليه بروتوكول الـ (OSPF) فإنه يقوم بإرسال الـ (Hello packet) للراوتر الأول رداً على طلبه في حال تحققت الشروط لذلك.

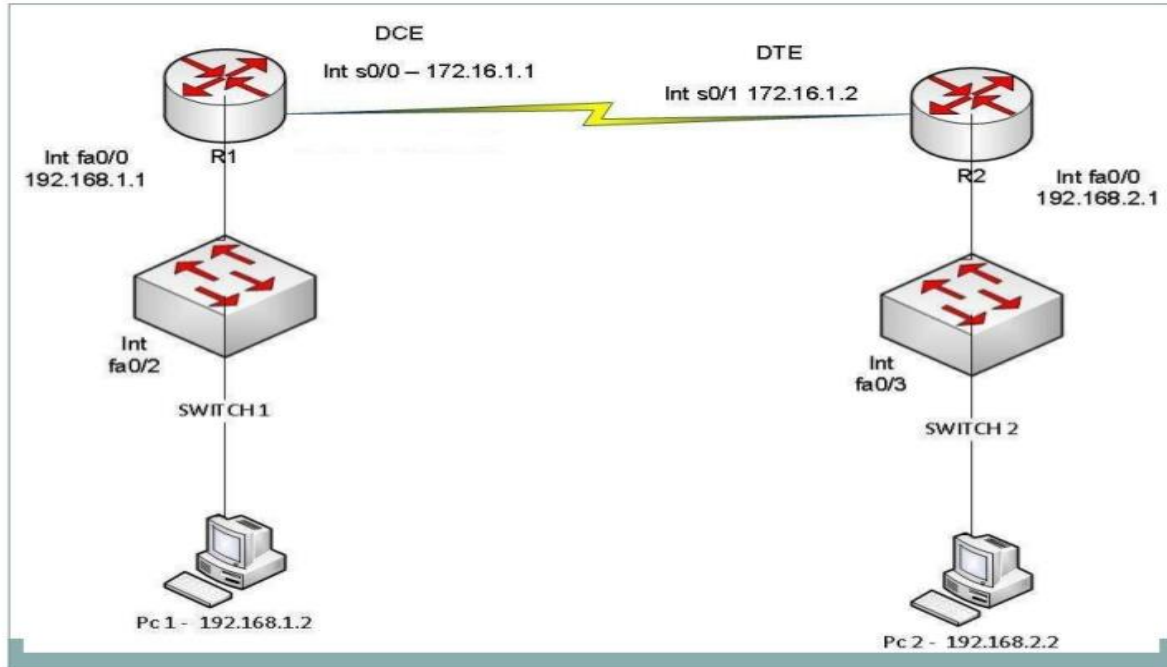
مثال:-



في الصورة التقريبية اعلاه ، نفترض أن الـ (OSPF) يعمل على الراوتر (R2) بكل منافذه، بعد تشغيل الـ (OSPF) على الراوتر (R1) وتفعيل البروتوكول على المنفذ المقابل للراوتر (R2) ، تتم الخطوات التالية:

- 1- يقوم الـ (OSPF) في الـ (R1) بإرسال (Hello) عبر المنفذ آملاً في إيجاد راوتر مجاور، تتغير الحالة عند الـ (R1) هنا من الـ (down) إلى الـ (initial).
- 2- يقوم الـ (R2) بالتحقق من بعض المعلومات المحمولة في الـ (Hello packet) لمطابقتها
- 3- في حال انطباق الشروط يقوم الـ (R2) بالرد وإرسال (Hello packet) تحمل رقم الراوتر (Router-ID) للراوتر (R1)، عندها تصبح الحالة بين الراوترين (2 way).

4- يستمر ارسال الـ (Hello packets) كل عشرة ثواني بين الطرفين بشكل متكرر للمحافظة على العلاقة التي نشأت بينهما وان لم يتم الرد من الراوتر المجاور خلال اربعين ثانية (اي اربعة رسائل Hello) يعتبر الوصل غير متصل و بالتالي قطع علاقة التبادل .



لمعرف عمل البرتوكول و فحص الاوامر: OSPF Configuration:

- Enter OSPF router configuration mode:
• لتفعيل البرتوكول في الراوتر وتعين رقم النظام (الرقم 10 يعتبر رقم النظام)

```
R1(config)# router ospf 10 ! 10 = process ID
```

- Configure one or more network commands to identify which interfaces will run OSPF:
• اضافة الشبكات للبرتوكول و تفعيلها مع الوصلات المجاورة , و تعيين رقم المنظومة

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0  
R1(config-router)# network 172.16.0.0 0.0.255.255 area 0
```

OSPF verification:

لمعرف عمل البرتوكول و فحص الاوامر:

- Shows information about the running routing protocol process:
لمعرفة اي بروتوكولات التوجيه يعمل حاليا في الراوتر :-

```
R1# show ip protocols
```

```
R1#show ip protocols
```

```
Routing Protocol is "ospf 10"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 192.168.1.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
192.168.1.0 0.0.0.255 area 0
```

```
172.16.0.0 0.0.255.255 area 0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update
---------	----------	-------------

192.168.1.1	110	00:04:12
-------------	-----	----------

192.168.3.1	110	00:04:12
-------------	-----	----------

```
Distance: (default is 110)
```

- Shows the entire routing table:
لعرض جميع عناوين التوجيه في جدول الراوتر (اي ما يمكن وصوله من قبل الراوتر) :-

```
R1# show ip route
```

- Shows routes learned via OSPF only:
لعرض العناوين المتعرف عليها من قبل (OSPF) فقط :-

```
R1# show ip route ospf
```

- Shows all neighboring routers along with their respective adjacency state:
لعرض الوصلات (الشبكات) المجاورة وحالة تلك الوصلات و تفاصيل عنها :-

EIGRP Routing Protocol:

Enhanced Interior Gateway Routing Protocol: (EIGRP

يطلق على ال EIGRP مصطلح (advanced distance-vector routing protocol) حيث تم تطويره من قبل سيسكو لحل مشاكل التي كانت تواجهها الشبكات في استخدام RIP الا انه لا يعمل على غير اجهزة سيسكو , حيث صمم ليدعم الشبكات العملاقة ليصل عدد الراوترات التي يمكن ان يعمل على EIGRP الي 255 وصلة توجه و هي ما يعرف (hop counting) اي ان البيانات المرسله تستطيع ان تتجاوز 254 نقطة مرور على الشبكة (يقصد بنقطة مرور كل ما يمكن اضافته للشبكة مثل راوتر , سوتش , جدار حماية , ... الخ) مقارنة مع RIP الذي كان يدعم فقط 16 راوتر (نقطة مرور) يعمل بروتوكول EIGRP على اساس رقم تعريفه يسمى (Autonomous System)

ماذا يعني ال **Autonomous system** ؟

Autonomous system (AS)

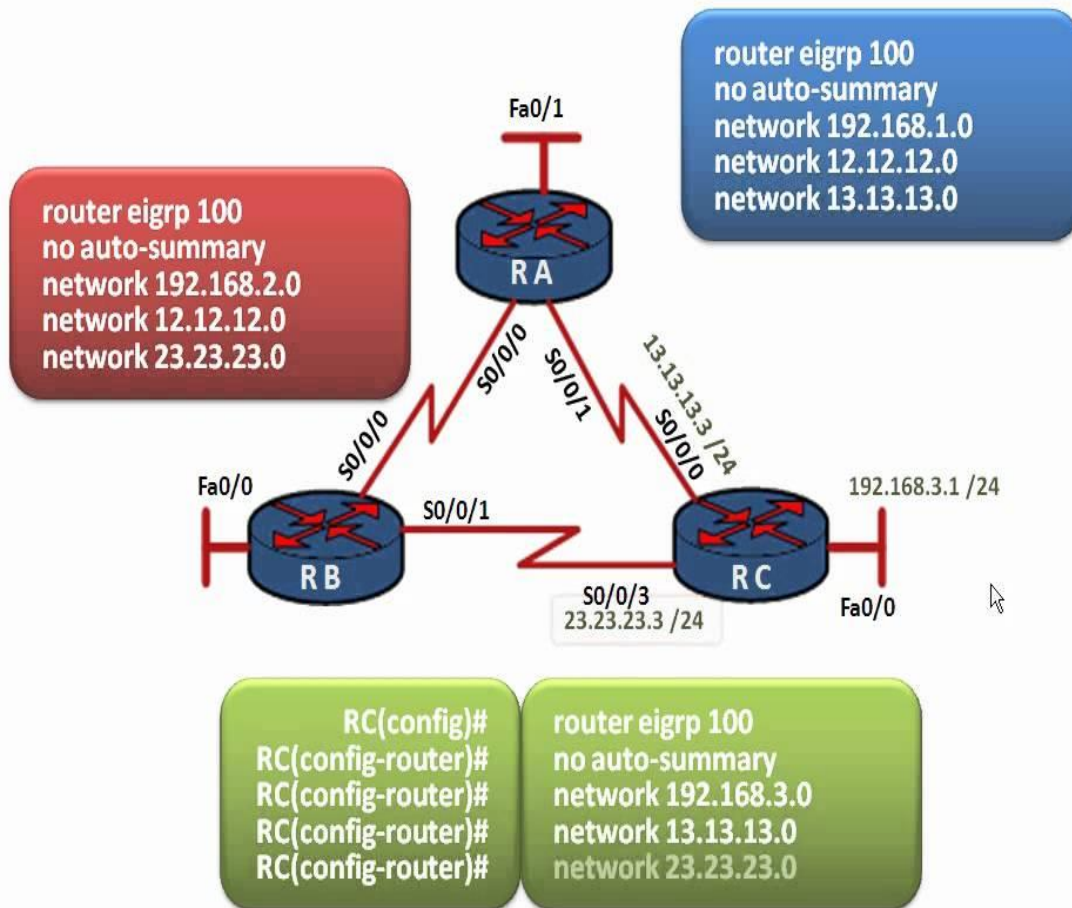
هي عبارة عن رقم تعريفه (من 1 الي 65535) يستخدم ليحدد مجموعه من الشبكات تخضع تحت قيادة كيان او منظومه تدار من قبل مؤسسه او جهه موحده ومرتبطة ببعضها البعض

مميزات بروتوكول EIGRP:

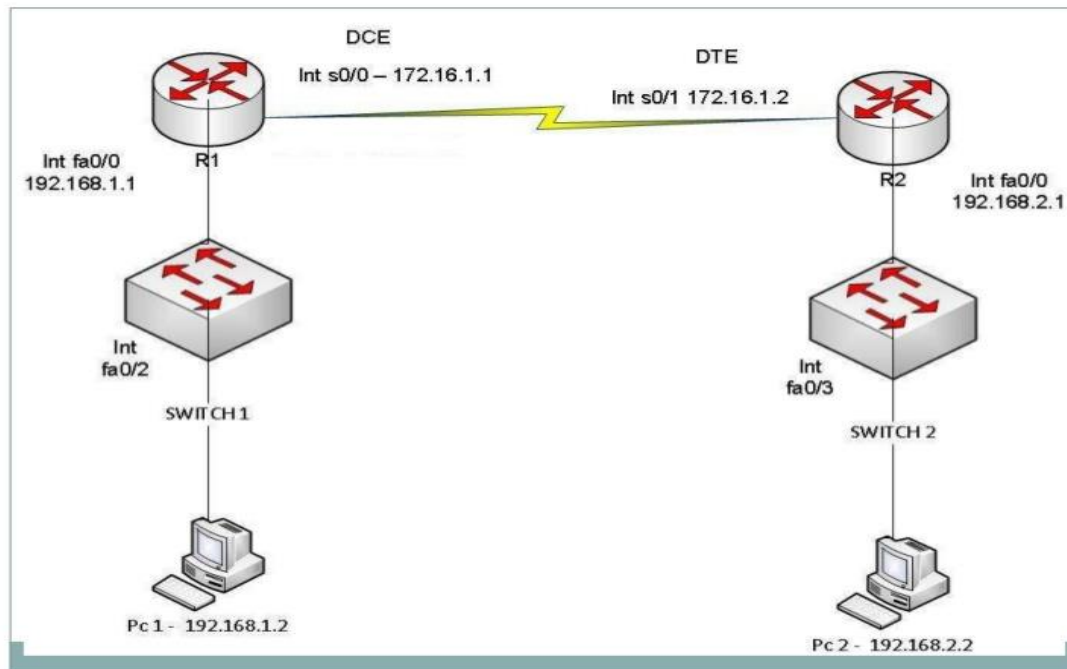
- يستخدم نفس المقاييس والحسابات distance vector routing protocol
- ليحسب أفضل واقلر طريق
- يتم تبادل أيض Neighbor Relationship بين المحولات المشاركة
- يرسل رسالة بشكل متكرر ليعلم الآخرين بأنه يعمل بشكل جيد Keep alive packets
- في الاتصال مع الاجهزة المجاورة يستخدم عنوان Broadcast address 224.0.0.1 كرسالة عامة للمجموعة الراوترات المجاورة .

رسم توضيحي لتفيل و ضبط بروتوكول eigrp :

EIGRP Configuration



ضبط و تفعيل بروتوكول EIGRP:



Mode and define AS number:

يجب تحديد رقم تعريف لمجموعة الراوترات المراد تفعيل بروتوكول eigrp فيها و يمكننا اختيار اي رقم من 1 الي 65535 على ان يكون نفس الرقم في جميع الراوترات :

```
R1(config)# router eigrp 100      ! 100 = AS number
```

- Configure one or more network commands to enable EIGRP on the specified interfaces:

```
R1(config-router)# network 10.0.0.0
R1(config-router)# network 172.16.0.0
R1(config-router)# network 192.168.1.1 0
```

- Disable auto summarization (Optional):

يقوم بروتوكول eigrp باختصار تلقائي لعناوين الشبكات المتشابهة لتصغير حجم جدول عرض الشبكات المتعرف عليها من قبل البرتوكول , لتعطيل هذه الخاصية نستخدم الامر الاتي :

```
R1(config-router)# no auto-summary
```

EIGRP Verification:

لمعرف عمل البرتوكول و فحص الاوامر:

- Shows routes learned via EIGRP only:
• لعرض العناوين المتعرف عليها من قبل (EIGRP) فقط .

```
R1# show ip route eigrp
```

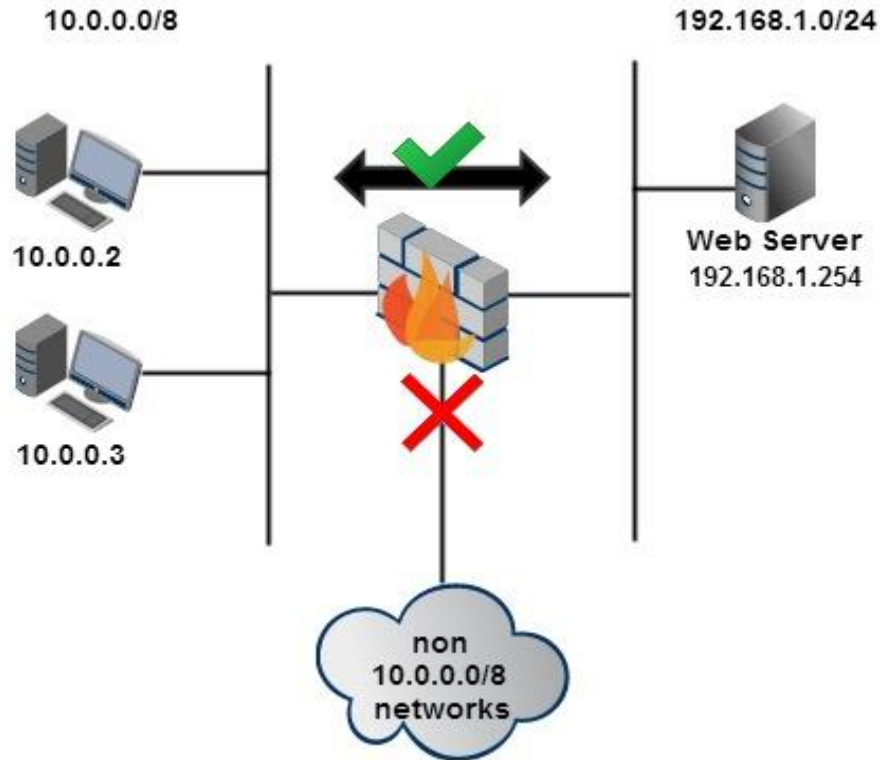
- Shows EIGRP neighbors and status:
• لعرض عناوين الراوترات المجاورة المتعرف عليها من قبل البرتوكول

```
R1# show ip eigrp neighbor
```

- Shows interfaces that run EIGRP:
• لعرض المداخل التي يعمل عليها بروتوكول EIGRP :

```
R1# show ip eigrp interface
```

Access Control Lists: (ACL)



الـ Access Control List او ما يسمى بالـ (ACL) هي عبارة عن قائمة بها تعليمات وشروط تتحكم وتصنف البيانات أو الـ Packet على أن يتم تطبيق إجراء معين على هذه الـ Packet ونقصد بالإجراء هنا إما تمرير الـ Packet عبر الـ Interface (بغض النظر عن نوع الـ Interface) أو رفض تمريرها.

أهم استخدام للـ Access List هو عمل فلترة أو Secure للبيانات أو الـ Packets الغير مرغوب بدخولها للشبكة أو خروجها من الشبكة.

ماذا يمكن أن نمنع بواسطة استخدام نظام الحماية { ACL } ؟.....!

- ❖ يمكن أن نمنع عدة جهاز أو أجهزة من الدخول لشبكة معينة
- ❖ ويمكن أن نمنع شبكة من الدخول لشبكة أخرى
- ❖ ويمكن نمنع جهاز أو أجهزة من الاتصال بالإنترنت
- ❖ ويمكن أن نمنع أجهزة من خارج الشركة أن تدخل لشبكة الشركة أو جزء من شبكة
- ❖ أيضاً على العكس من كلمة نمنع، فإنه يمكننا أن نستبدل كلمة نمنع بكلمة نسمح

كيف يعمل نظام (ACL) Access Control Lists ؟

طريقة عمل ال Access Control List هي أشبه بالبرمجة، نعم هي نوع من أنواع البرمجة بحيث البرمجة تتبع طريقة الفحص المتسلسل للتعليمات والشروط، ■

مثال تشبيهي

مثلاً: إذا حضر المدير فافتحوا له الباب !

نلاحظ هنا أن إجراء فتح الباب مشروط بحضور المدير، ولكن ماذا لو لم يحضر المدير ؟؟ الجواب بسيط، الباب سيبقى مقفلاً ما لم نعدل بشرط فتح الباب كأن نضيف مثلاً: إذا حضر المدير أو مساعده فافتحوا الباب، وهنا نلاحظ أننا أضفنا مساعد المدير كشرط ثاني من شروط فتح الباب، وبالتالي فإن ال Access List هي بحد ذاتها برمجة لأوامر مشروطة إذا توافر الشرط فيها فإن إجراء ما سيحدث، وإن لم يتوافر الشرط فإن الإجراء لن يحدث على الإطلاق.

طريقة عمل نظام (ACL) Access Control Lists :

ال Access List يتم بنائها في ال *Global Configuration Mode* الخاص بالراوتر أو السويتش، ولكن تطبيق هذه ال Access List يتم على الإنترنت (مدخل الراوتر)، بمعنى لو

أنك قمت بعمل مليون (ACL) لكي تمنع البيانات من دخول الشبكة ولم تقم بتطبيق هذه (ACL) على ال *Interface* فإنك لن تستطيع أن تمنع البيانات من دخول الموقع على الإطلاق، وهذه نقطة مهمة جداً، إنشاء ال Access List يتم في ال *Global Mode* و تطبيقها يتم على الإنترنت (مدخل الراوتر) ■

(ACL) يتبع طريقة الفحص المتسلسل للتعليمات والشروط، بمعنى أن كل Access List يتكون من عدد من النصوص (Statements)، أو عدد من الشروط والتعليمات، عندما تأتي Packet معينة للراوتر وتحديداً لل *Interface* الذي طبقنا عليه ال Access List فإن هذه Access List تقوم بفحص ال Packet وتمريه على ال Statements أو الشروط بالترتيب من الأعلى للأسفل، ال Router يقوم بامساك ال Packet ويقارنها بالشرط الأول وسيسأل الراوتر نفسه: هل الشرط ينطبق على هذه ال Packet أم لا ؟؟؟

يرجى الانتباه بأنه في نهاية كل Access List نقوم بإنشائها يوجد إجراء أو Action مخفي ولا يمكن رؤيتها أو حتى قراءتها، هذا الإجراء يقول ((إمنع الكل)) ، مثلاً: قلنا لبواب العمارة: يا بواب إمنع فقط علي و خالد وعمر من دخول البناية، يوجد هناك أمر مخفي في ال Access List يقول: إمنع الجميع، وبالتالي لو حضر مصطفى فلن يتمكن من الدخول، ليس بسبب أن إسم مصطفى مدرج من ضمن أسماء الأشخاص المحظور دخولهم، كلا ، ولكن بسبب أنه يوجد تعليمة مخفية تقول إمنع الكل، يعني تلقائياً (by default) ال Access List يقوم بعمل Block لكل يعني. Deny وبالتالي إسم مصطفى هو من ضمن الكل صحيح؟؟ وبالتالي تم منع مصطفى على هذا الأساس.

أنواع نظام الحماية Access Control List (ACL):

1 - النوع الأول: " Standard Access List "

هذا النوع يستخدم عنوان أو IP Address للجهاز المرسل أو ال Source Address فقط، وبالتالي فإن الشرط هنا هو العنوان أو ال IP Address للجهاز المرسل فقط لا غير .

بمعنى ان هذا النوع يستطيع فقط يمنع على اساس ال IP Address و لا يستطيع منع أي نوع من انواع التطبيقات التي تعمل على الكمبيوتر ال Application وهو يعمل على المستوى الثالث من الطبقات السبعة Network Layer .

يتم إنشاء هذا النوع عن طريق الدخول إلى ال Global Configuration Mode ومن ثم إعطاء الأمر Access-list ومن ثم كتابة رقم، يوجد لل Standard Access List مجال من الأرقام المستخدمة، وهي من 1 الي 99

مثلاً: عند كتابة الرقم 49 يقوم الراوتر بتنفيذ النوع الاول (Standard ACL) :
Router(config)#access-list 49 deny 192.168.0.0 0.0.255.255

2- النوع الثاني: " Extended Access List "

هذا النوع يستخدم في تقييمه لل Packet العديد من الأمور، مثل: عنوان المرسل، عنوان المستقبل، نوع بروتوكول معين في المستوى الرابع أو Transport Layer ، و رقم Port للجهاز المرسل، رقم البورت للجهاز المستقبل. وبالتالي نلاحظ هنا أنه يمكننا التحكم بمستويين من مستويات الطبقات السبعة وهما Network Layer و Transport Layer لان هذا النوع يعمل في المستويين الثالث و الرابع من مستويات (IOS Layer) .

وهذه الخواص يعطي ال Extended Access List قوة أكبر في إمكانية التفصيل بشكل أكبر في تحديد الشروط .

يتم إنشاء هذا النوع عن طريق الدخول إلى ال Global Configuration Mode ومن ثم إعطاء الأمر Access-list ومن ثم كتابة رقم، وكما في ال Standard فإنه أيضاً يوجد مجال أو Range لهذا النوع وهو ال Extended Access List ، ويمكن ان نكتب مجال الارقام من 100 الي 199 .

مثلاً , عند اختيارنا للرقم 115 يفعل في الراوتر تلقائياً ACL من النوع الثاني
Router(config)#access-list 115 deny tcp any host 172.16.16.1 eq 80

3- النوع الثالث : (ACL) " Named Access Control List "

هذا النوع صراحة لا يمكن اعتباره نوع !!! ولكن اعتبره طريقة لتسمية ال Access List بإسم يدل على مضمون هذه ال Access List وبالتالي يسهل علينا كمسؤولين عن جهاز الراوتر أو السويتش أن نعرف: لماذا أنشأنا نظام حماية (ACL) مثلاً لو أردنا منع التصفح على الإنترنت فبإمكاننا أن نكتب باستخدام (Named Access List) ونسميها { No Internet } أو { STOP_INTERNET } ومن ثم نطبقها على الإنترنت (مدخل سلك الراوتر) بنفس الإسم. وبالتالي لو عدنا للأكسس لست (ACL) في وقت لاحق فإننا سنعرف أن هذه الأكسس لست (ACL) أنشأت لمنع الوصول للإنترنت .

علما ان النوع الثالث يستخدم في انشاء كلا من النوعين السابقين وهما Standard Access List و Extended Access List ولا يكتب اي رقم معها حيث يذكر فقط كلمة Standard في حال تفعيل النوع الاول و كلمة Extended في حال تفعيل النوع الثاني

مثلاً : Router(config)#ip access-list standard NO_INTERNET
أو Router(config)#ip access-list extended STOP_INTERNET

وعندما نريد أن نطبقها على المنفذ نستبدل الرقم بالإسم الذي كتبناه.

مثلاً :

Router(config-if)#ip access-group (access list name) (in or out)

ماذا نقصد بكلمة In و Out ؟

كما علمنا سابقاً أن ال Access List عديمة الفائدة ما لم تطبق على ال Interface ، وتطبيقها كما شرحنا سابقاً يتم على أن مدخل على الإنترنت ومن ثم تصدر الأمر ip access-group و نتبعه برقم الأكسس لست، ومن ثم نتبعه ب in أو out ، كل هذا في سطر واحد.

(in هي إختصار ل (Inbound Access Lists) و out هي إختصار ل Outbound Access list

يعنى ال Access List تطبق على ال Packets (البيانات) الداخلة للراوتر أو الخارجة منه، طبعاً تحديد الإتجاه هو من العوامل المهمة جداً في نجاح تطبيق ال Access List ، ولكي نعرف كيف نطبق ال Access List في الإتجاه الصحيح دعونا نتبع هذه القاعدة السهلة جداً، ولو فهمتوا هذه القاعدة فلن ولن تخطؤا الإتجاه بعون الله على الإطلاق.

افضل طريقة لتحديد إتجاه ال: Access List

أول شيء نضع عيننا على ال Interface الذي سنطبق عليه ال Access List ونلاحظ الاتي :

*** إذا كانت ال Packet موجودة داخل الراوتر ونريد منعها أو السماح لها بالخروج من الرواوتر عبر ال Interface نقول: من >===== إلى ، أي من داخل الراوتر إلى خارجه ، أي من In إلى Out ، دائماً نختار الشق الثاني، وفي هذه الحالة هو. Out

*** اما إذا كانت ال Packet موجودة خارج الراوتر ونريد منعها أو السماح لها بالدخول للراوتر عبر ال Interface نقول: من >===== إلى ، أي من خارج الراوتر إلى داخله ، أي من Out إلى In ، دائماً نختار الشق الثاني، وفي هذه الحالة هو In .

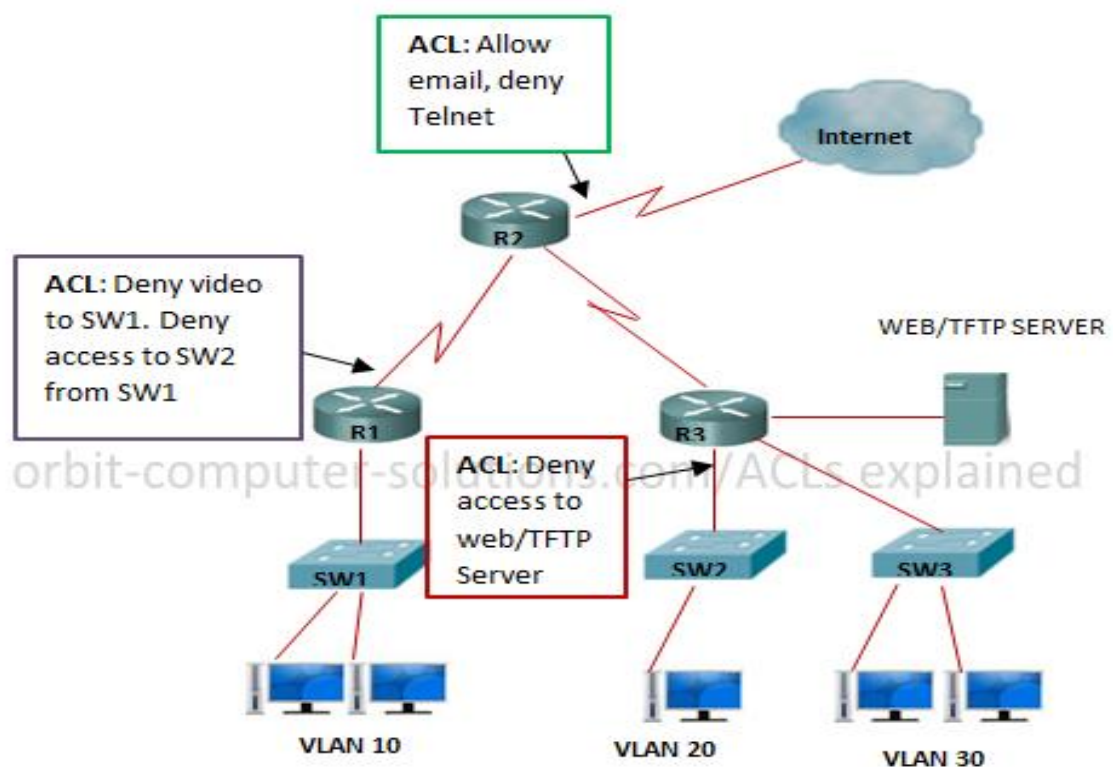
إذا أنطبق الشرط فإن الراوتر يتوقف ليقراً الإجراء المنصوصة على الشروط حين انشاء ACL

يتبع ال ACL طريقة الفحص المتسلسل للتعليمات و الشروط بمعنى ان كل Access List كما تم ذكره سابقا تتكون من عدد من النصوص Statement و التعليمات لذلك يقوم بفحص البيانات المرسله و تمريرها على الانترنت بالترتيب من الاعلى الي الاسفل و يقارنها بالشرط الاول , و يسال الراوتر نفسه هل الشرط ينطبق على تلك البيانات المرسله او المستلمة ام لا !! و في حال انطبق الشرط فان الراوتر يتوقف ليتخذ الاجراء المنصوص عليه في ACL

مع الاخذ في الاعتبار بان في نهاية كل امر حماية نقوم بنشائها يوجد اجراء او Action مخفى ولا يمكن رؤيتها او حتى قراءتها هذا الاجراء يقول (امنع الكل)

مثلا :

لوقلنا لبواب العمارة: يا بواب إمنع فقط علي و خالد وعمر من دخول البناية، وفي حال وجود هناك أمر يقول: (أمنع الكل) وبالتالي لو حضر مصطفى فلن يتمكن من الدخول، ليس بسبب أن اسم مصطفى مدرج من ضمن أسماء الأشخاص المحظور دخولهم، كلا ، ولكن بسبب أنه يوجد تعليمة مخفية تقول أمنع الكل، يعني (by default) وبالتالي اسم مصطفى هو من ضمن الكل صحيح؟؟ وبالتالي تم منع مصطفى على هذا الأساس



في ما يلي اوامر تفيل النوع الاول من ACL

Standard ACL Configuration: 1 - 99 and 1300 - 1999

```
R1(config)# access-list 2 deny 192.168.1.77
R1(config)# access-list 2 deny 192.168.1.64 0.0.0.31
R1(config)# access-list 2 permit 10.1.0.0 0.0.255.255
```

```
R1(config)# access-list 2 deny 10.0.0.0 0.255.255.255
```

```
R1(config)# access-list 2 permit any
```

- Enable the ACL on the chosen router interface in the correct direction (in or out):
 - يجب تفعيل نظام الحماية في مدخل معين من مداخل الراوتر ليعمل بشكل محدد , وعلينا ايضا تحديد عمله في حالة الدخول ام الخروج :

```
R1(config-if)# ip access-group 2 out
```

تفيل النوع الثاني من ACL

Extended ACL Configuration: 100 - 199 and 2000 - 2699

```
R1(config)# access-list 101 remark MY_ACCESS_LIST
```

```
R1(config)# access-list 101 deny ip host 10.1.1.1 host  
10.2.2.2
```

```
R1(config)# access-list 101 deny tcp 10.1.1.0 0.0.0.255 any  
eq 23
```

```
R1(config)# access-list 101 deny icmp 10.1.1.1 0.0.0.0 any
```

```
R1(config)# access-list 101 deny tcp host 10.1.1.0 host  
10.0.0.1 eq 80
```

```
R1(config)# access-list 101 deny udp host 10.1.1.7 eq 53 any
```

```
R1(config)# access-list 101 permit ip any any
```

```
R1(config)# interface fastEthernet 0/0
```

```
R1(config-if)# ip access-group 101 in
```

Verifying ACLs:

لمعرف عمل ACL و فحص الاوامر:

- Shows all ACLs configured on a router with counters at the end of each statement:

```
R1# show access-lists
OR
R1# show ip access-list
```

```
R1#show access-lists
Extended IP access list 101
10 deny ip host 10.0.0.1 any
20 deny icmp 10.0.0.0 0.0.0.255 any
30 deny tcp host 10.1.1.7 eq domain any
40 permit ip any any
    permit ip any any
```

- Shows only the specified ACL:

• لعرض نظام ACL معين دون غيره نكتب رقمه في اخر الامر :

```
R1# show ip access-list 101
```

```
R1#show access-lists
Extended IP access list 101
10 deny ip host 10.0.0.1 any
20 deny icmp 10.0.0.0 0.0.0.255 any
30 deny tcp host 10.1.1.7 eq domain any
40 permit ip any any
```

- Includes a reference to the ACLs enabled on that interface either in or out:

• لفحص مدخل الراوتر ما اذا كان تم تفعيل نظام الحماية فيه ام لا :

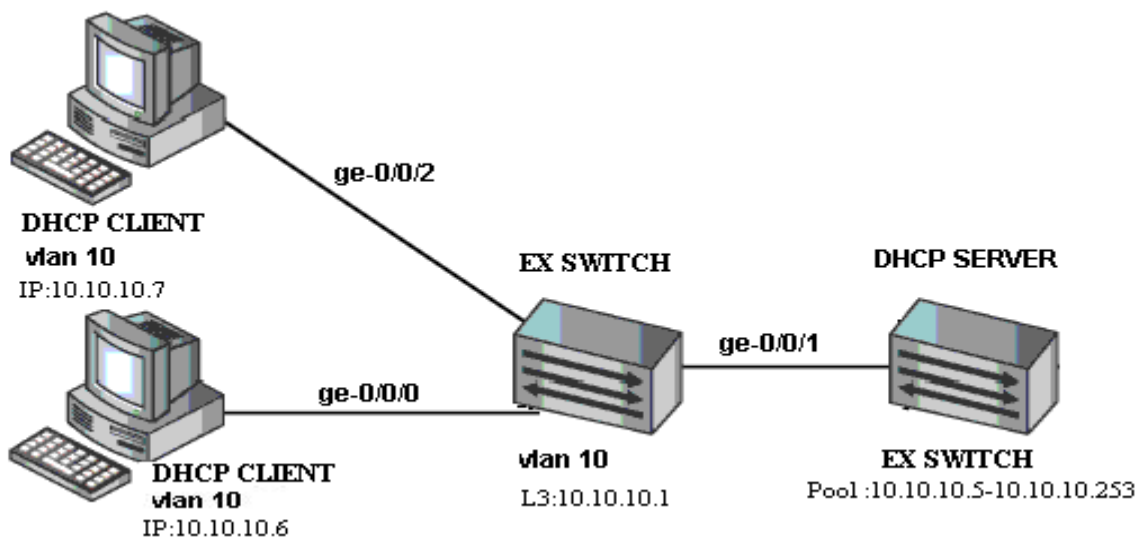
```
R1# show ip interface f0/0
```

DHCP

بروتوكول توزيع العناوين (Dynamic Host Configuration Protocol (DHCP)

البروتوكول الذي يقوم بتوزيع عناوين IP وملحقاتها على أجهزة الشبكة حيث انه من المعروف أن عنوان IP يمكن تعريفه بطريقتين أما يدويا أو تلقائيا

حيث أن التعريف اليدوي لعنوان الـ IP يكون سهلا عندما تكون الشبكة صغيرة لكن كلما اتسعت الشبكة و كلما كانت أجهزة الشبكة غير مستقرة فمثلا أن كانت الشبكة عامة ففي كل فترة زمنية يدخله جهاز جديد وبعد فترة قد يخرج منها ليعود إليها لاحقا أو قد لا يعود لذا يصعب استخدام الطريقة اليدوية لتعريف العناوين لذا فيفضل استخدام الطريقة التلقائية والتي تستخدم بدورها بروتوكول DHCP .



حيث أنه يقوم بذلك في أربع خطوات وهي :

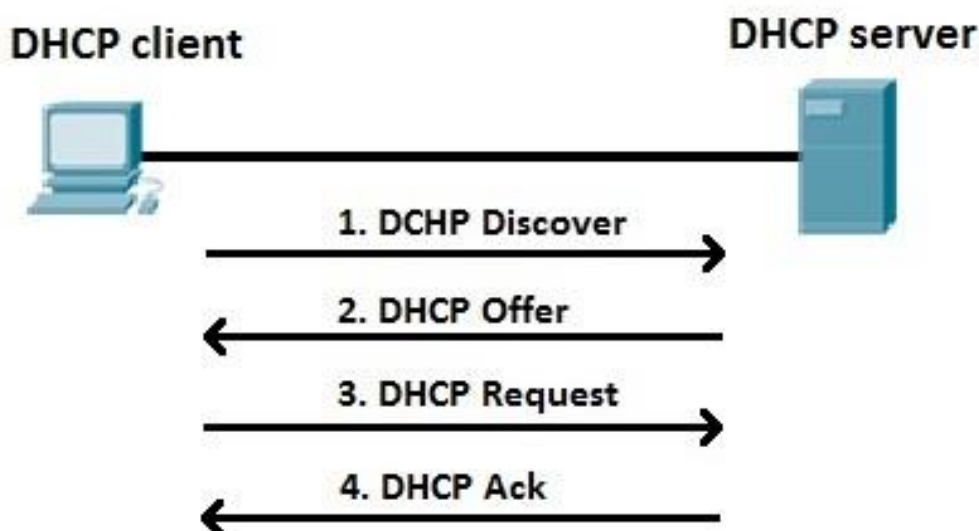
1- يتم إرسال رسالة من جهاز المستخدم "Client" يتم بها طلب عنوان IP وبما أن الجهاز لا يمتلك عنوان IP في هذه اللحظة فيقوم بإرسال هذه الرسالة بالـ IP التالي 0.0.0.0 إلى العنوان 255.255.255.255 وتحتوي هذه الرسالة على اسم الجهاز وعنوان كرت الشبكة حتى يعرف (DHCP server) كيف يرد على الطلب وتسمى هذه العملية بـ IP lease request

2- يقوم (DHCP server) بالرد على الطلب عن طريق عرض خدماته بإرسال broadcast يحتوي على عنوان IP وقناع الشبكة "subnet mask" وتسمى هذه العملية بـ IP lease offer

3- بعد أن يستلم المستخدم عروض DHCP server وعنوان IP المقترح يقوم بإرسال رسالة إلى (DHCP server) تعلمه أنه قد تم اختيار عنوان الـ IP المقترح وتسمى هذه العملية بـ IP lease selection .

4- يقوم بعد ذلك DHCP server بإرسال ما يسمى بـ "ask" إلى المستخدم للتأكيد على أنه قد تم تعيين عنوان IP لهذا المستخدم من قبل DHCP server ، وإذا استقبل المستخدم "unsuccessful ask" بمعنى فشل في الإرسال فيعمل جهاز المستخدم على إرسال طلب آخر.

وهذا الشكل توضح باختصار طريقة الحصول على عنوان IP



ضبط و تفعيل DHCP Server

Define a DHCP pool and give it a name:

يجب تحديد اي اسم تعريف للبرتوكول :

```
R1(config)# ip dhcp pool MY_POOL
```

- Define network and mask to use in this pool and the default gateway:

• تحديد عنوان الشبكة و المخرج الافتراضي

```
R1(dhcp-config)# network 192.168.1.0 255.255.255.0  
R1(dhcp-config)# default-router 192.168.1.1
```

- Define one or more DNS server (OPTIONAL):

تحديد DNS سرفر ان وجد و هو ليس شرطاً في تفعيل ال DHCP

```
R1(dhcp-config)# dns-server 213.131.65.20 8.8.8.8
```

- Confine the lease time (OPTIONAL):

```
R1(dhcp-config) lease 2 ! Days
```

- Define one or more scopes of excluded (reserved) addresses (OPTIONAL):

كما يمكننا تخزين بعض العناوين لاستخدامها في المستقبل

```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.100
```

DHCP Verification and Troubleshooting:

لمعرف عمل DHCP و فحص الاوامر:

- Shows the status of the specified pool and the leased addresses from that pool:

```
R1# show dhcp lease
```

- Shows all the leased ip addresses from all configured DHCP pools:
- Shows any conflicts that occurred:

```
R1# show ip dhcp conflict
```

```
R1#SHoW IP DHcp Conflict
```

IP address	Detection method	Detection time
VRF		
192.168.1.1	Ping	???? 1 1993 12:26 am

Network Address Translation (NAT)

ترجمة عناوين الشبكات

عند استخدامك للانترنت يقوم موزع الخدمة باسناد عنوان لك تكون هذه العناوين ديناميكية فيتيح لك هذا العنوان بالتواصل مع المواقع او الخدمات الاخرى. تكمن المشكلة في حال المؤسسات او المستخدمين لعدة اجهزة لا نه يجب ان يكون هناك عنوان لكل جهاز في الانترنت فيكون الحل شراء خط انترنت لكل جهاز

لكن لهذه الطريقة عيوبها:

- مكلفة جدا
- صعوبة الصيانه
- صعوبة التحكم او مراقبة استخدامات تلك الاجهزة

الحل الاسهل استخدام خط انترنت واحد وتوزيعه على جميع الاجهزة ولحل مشكلة العناوين نستخدم تقنية النات

network address translation

بعد زيادة نسبة المستخدمين للـ Internet واحتياج كل مستخدم لـ IP Address خاص به للاتصال عبر الانترنت في حين أن IPv4 لم يعد يلبي هذه الاحتياجات بسبب سوء التوزيع مما يؤدي إلى نقص في توفر public IP Address لكل مستخدم تم اللجوء حل يسمى Network Address Translation أو الـ NAT وهذا الحل يمكننا ببساطة من لو كان عندنا فرضا شركة تتكون من 10 أفراد يستخدموا الـ internet في عملهم . قبل هذا الحل كان لابد من شراء public ip من الـ ISP لكل فرد ليتمكنوا من استخدام الانترنت في نفس الوقت أما مع هذا الحل فيمكننا شراء Public IP واحد فقط ليستخدمه الجميع وسوف نفهم فيما بعد كيفية عمل ذلك وله مميزات أخرى

أنواع الـ NAT :

-1 Static NAT :

وهذا النوع من الـ NAT يمكنك الاختيار بنفسك لكل Private IP من الموجودين Public IP عندما يخرج إلى شبكة أخرى أو إلى الانترنت مثلا يعني 192.168.1.10 لما يحاول الاتصال بالـ Internet يظهر على الـ Internet بـ 214.12.59.1 وهكذا مع باقي الأجهزة .

مثال : ان وجد لدينا web server لموقع من المؤكد ان الـ web server موجود في شبكة داخلية وله private IP ولكن يظهر للشبكات الخارجية بـ public IP ليتم الاتصال به .

-2 Dynamic NAT :

في هذا النوع من الـ NAT يتم اختيار مجموعة من الـ Private IP ليظهروا عبر الشبكات الخارجية بمجموعة من الـ Public IP وهنا لا يشترط أن يظهر مثلا 192.168.1.10 في الشبكات الخارجية بـ 225.20.12.5 بل يأخذ أول Public IP حر أو بمعنى لا يكون مستخدم حين , اما ان وجد public ip قد تم استقلاله من قبل private ip اخر في هذه عليه الانتظار حتى يتفرق من الطلب الاول و من ثم يخرج إلى الشبكة الخارجية في صورته . وهنا طبعا يكون عدد الـ private ip اكبر من عدد الـ public ip .

-3 NAT Overloading :

وهذا النوع هو المنتشر بكثرة ومن اشهر الأمثلة عليه هو DSL Modem وهو عبارة عن مجموعة من الـ private IP تظهر للشبكات الخارجية بـ Public IP واحد فقط ويتم التفرقة بينهم باستخدام الـ TCP/UDP port number بمعنى أن 192.168.1.10 و 192.168.1.11 يظهران للشبكات الخارجية بـ 224.12.59.1 ولكن يتم التفرقة بينهم باستخدام TCP/UDP port number، حيث أن

192.168.1.10 يظهر بـ 224.12.59.1:101 أي عن طريق ال port 101 و 192.168.1.11
عن طريق 224.12.59.1:102 أي عن طريق tcp port 102

مصطلحات ال NAT :

Inside & Outside Networks -1

كل جهاز موجود في ال Inside Network أو الشبكة الداخلية يعتبر Inside Device سواء كان pc, switch, وأي جهاز موجود في Outside Network أو الشبكة الخارجية يعتبر Outside Device

Local Address -2

وهو أي IP Address يظهر في الشبكة الداخلية

Global Address -3

وهو أي IP Address يظهر في الشبكة الخارجية

Inside Local Address -4

وهو كل جهاز له private IP موجود بالشبكة الداخلية

Outside Local Address -5

وهو أي جهاز خارجي يظهر للشبكة كأنه جهاز داخلي بمعنى آخر لو ال router عندي استلم packet من pc وليكن له ip 171.16.86.1 وأنا عندي Network ID 10.1.1.0 ال router يعمل translate أو ترجمة لـ source Address ليظهر كأنه موجود في الشبكة عندي فيظهر في الشبكة الداخلية بهذا الشكل ip 10.1.1.X

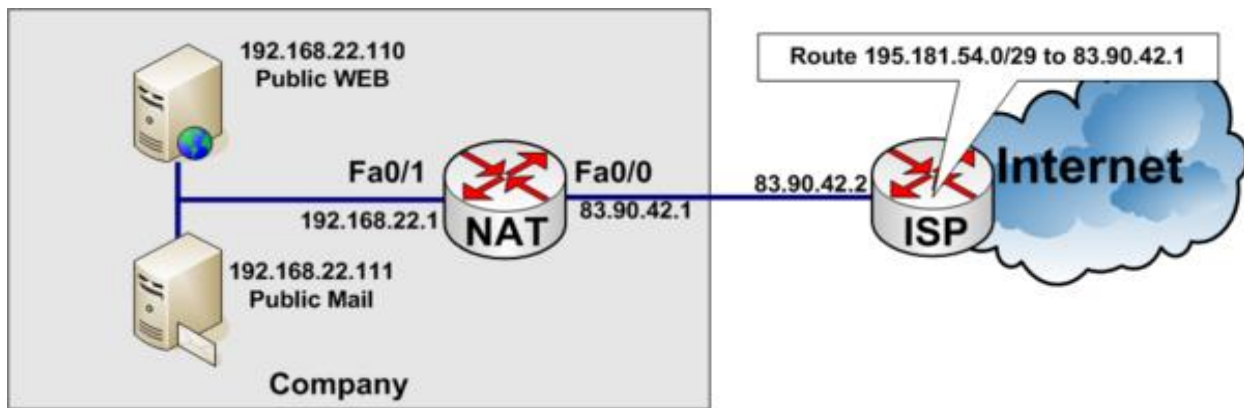
Inside Global Address -6

وهو أي جهاز داخلي له private ip ها يظهر للشبكات الخارجية بـ Public IP

Outside Global Address -7

وهو أي جهاز خارج الشبكة الداخلية وله public IP

الشكل يوضح مجموعة من الاجهزة الداخلية وقد تم ترجمتها من خلال تقنية NAT ليصلوا الي الانترنت مستخدمين Public ip address واحد .



Network Address Translation (NAT):

Static NAT :

لتفعيل NAT على سيسكو راوتر اولا يجب تحديد مداخل الراوتر ايهما مقابل الانترنت اي (Public ip) و (private ip) وذلك بالخطوات التالية :

- Define the outside and inside interfaces:

```
R1(config)# interface serial 0/0
R1(config-if)# ip nat outside
R1(config)# interface FastEthernet 1/1
R1(config-if)# ip nat inside
```

- Configure static NAT statement:

```
R1(config)# ip nat inside source static 192.168.1.10 200.1.1.1
```

Dynamic NAT:

- Define the outside and inside interfaces
- Create an ACL that determines the IP addresses that are allowed to be translated

- لاستخدام Dynamic NAT يجب اتباع الخطوات الآتية :
- تحديد مدخل الكابل الداخلي (اي مقابل الشبكة الداخلية)
- تحديد مدخل الكابل الخارجي (اي مقابل الانترنت)
- انشاء نظام ACL لمطابقة العناوين الداخلية المراد ترجمتها عن طريق NAT

```
R1(config)# access-list 3 permit 192.168.1.0 0.0.0.255
```

- Create a pool of public IP addresses:

```
R1(config)# ip nat pool PUB 192.168.1.1 192.168.1.150 netmask  
255.255.255.0
```

- Configure NAT statement:

```
R1(config)# ip nat inside source list 3 pool PUB overload
```

NAT verification and Troubleshoot:

لمعرف عمل NAT و فحص الاوامر:

- Useful in viewing the configuration of NAT pool and the inside and out-side interfaces:

```
R1# show running-config
```

- Shows counters for packets and NAT table entries, as well as basic configuration information:

```
R1# show ip nat statistics
```

- Displays the NAT table:

```
R1# show ip nat translations
```

السويتش Switching

تاريخ السويتش

لفهم أهمية السويتشات في يومنا هذا ، تحتاج إلى فهم كيفية استخدام الشبكات قبل اختراع السويتش . خلال منتصف عام 1980 كان 10 BASE2 إيثرنت (Ethernet) المعيار المستخدم حيث كان الحد الأقصى للإرسال آنذاك 10 Mbps / (عشرة ميغابايت في الثانية) . هذا المعيار تستخدم الكابلات المحورية coaxial ... مع الحد الأقصى لطول الكابل 185 متر و ويمكن توصيل 30 كمبيوتر خلال مرور الكابل .

Hub و switch على الرغم من انهما متشابهين تماما من حيث الشكل الا ان عملهم مختلف تماما

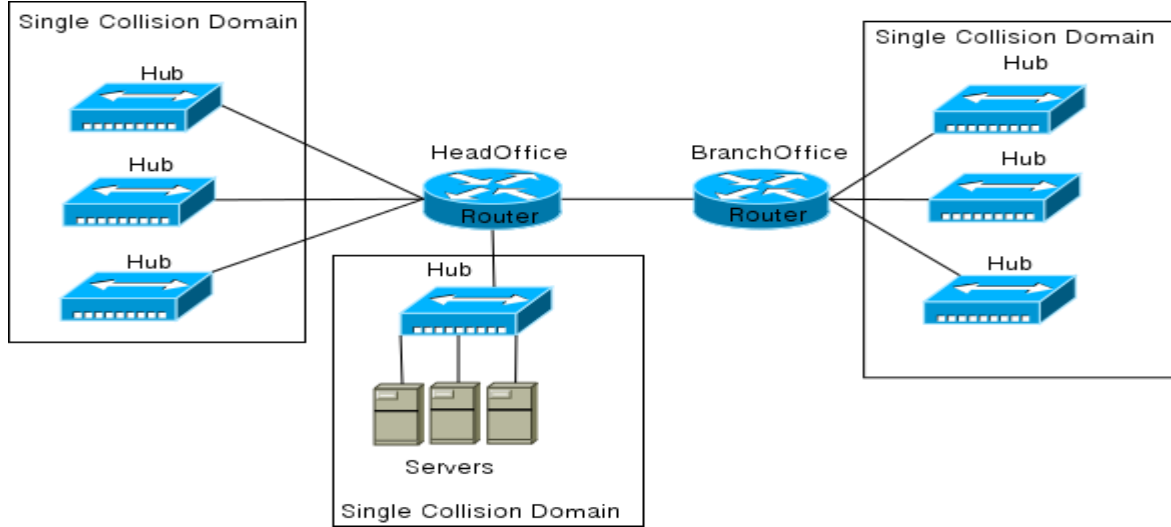
الهاب (hub) :

الهاب , يستخدم كما هو معروف لربط مجموعة كمبيوترات فيما بينها اي ان عمله مشابه لعمل تقسيم الكهرباء الذي يستخدم لربط عدة اجهزة على مقبس واحد ولكنه اضافة الى ذلك يقوم بتقوية الإشارة لان فيه repeater وذلك يزيد المسافة الى الضعف من 100 متر الى 200 متر ،

عيوب الهب :

- Collision domain معنى ذلك ان يشارك حزمة الشبكة مع الجميع . اي اذا ارسل كمبيوتر رقم واحد رساله الى كمبيوتر رقم اثنين فانه يقوم بارسال الرسالة الى جميع الكمبيوترات المربوطة على هذا الهب (Hub) او الهبات المجاورة له , وهذا يؤدي الى بطء الشبكة بشكل كبير لانه لا يمكن من حدوث اكثر من نقل واحد .
- هذا يعني اذا كان لدينا 100 كمبيوتر و قد تم ربطه على هب او مجموعة هبات وكانت سرعة النقل 100 Mbps و ارادوا الاتصال في نفس الوقت هذا سوف يقلل سرعة النقل الى 1 Mbps و الاو (تصور وجود 1000 كمبيوتر) وهو عدد طبيعي في الشركات

الشكل يوضح كيفية عمل الهب في الشبكات .



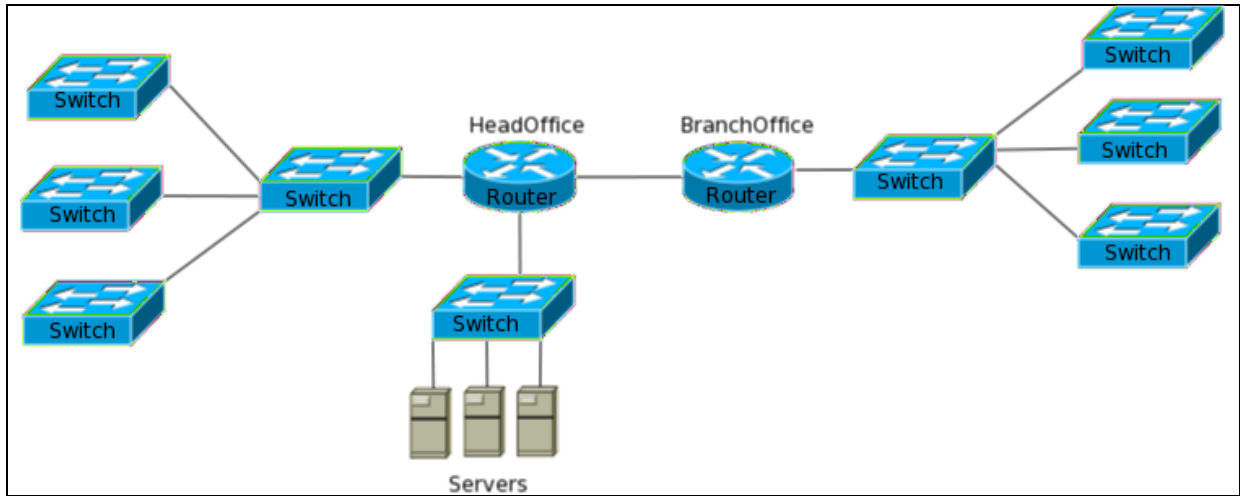
ما هو السوتش switch ؟

السوتش جهاز يوجه المعلومات حسب الطلب فقط (بعكس ال hub الذي يوجه المعلومات الى كل البوابات) , فلدى ال Switch معرفة مسبقة بالأجهزة الموصولة الى البوابات . فهو يرسل المعلومات أو حزم البيانات فقط الى البوابات المناسبة , وبالتالي فإن ال Switch يستطيع أن يخفض مقدار عبور الحزم ويحسن أداء الشبكة إذاً ال Switch يصل ال Hubs الى بعضها البعض أو يزود (يقدم) اتصالات محددة مسبقاً ليزيد من أداء محطات العمل

(السويتش switch): جاء السويتش ليحل مشاكل الهب الرئيسة المذكورة اعلاه اذ يقوم السويتش بتعلم مواقع الكمبيوترات حيث يرسل المعلومات الى الكمبيوتر المعين وليس الى الجميع مما يمكن من تخاطب اكثر من كمبيوتر في نفس الوقت مما يمكن من استغلال الحزمة بكاملها فاذا كان هناك 100 كمبيوتر وكانت سرعة النقل 100 Mbps تبقى السرعة كما هي اي ان النقل يبقى باعلى سرعة بغض النظر عن عدد الكمبيوترات المربوطة وهذا ايضا يزيد من امن المعلومات اذ انه اذا تم التصنط على الكيبل فلا يرى الا المعلومات المنقولة الى الكمبيوتر المربوط الى ذلك الكيبل وليس كل الشبكة

هذه ابسط مزايا السويتش وهي متوفرة بارخص وابسط انواع السويتشات هناك سويتشات معقدة وتحتوي امور كثيرة مثل Cisco switch .

الشكل يوضح ربط السوتش في الشبكات



لا يمكننا ضبط المبدلات إن لم تكن مُهيئة بعد؛ سوف اشرح في هذه المرحلة عملية بدء تشغيل نظام سيسكو IOS للمبدلات (Cisco Switch) واساعدك في التعرف على الخطوات بالنظر إلى مخرجات الإقلاع "configuration Out Put". ثم سأدخل إلى المبدل ونضبطه عبر واجهة سطر الأوامر، ثم سنتأكد من عمله عبر استخدام أوامر **show** المناسبة.

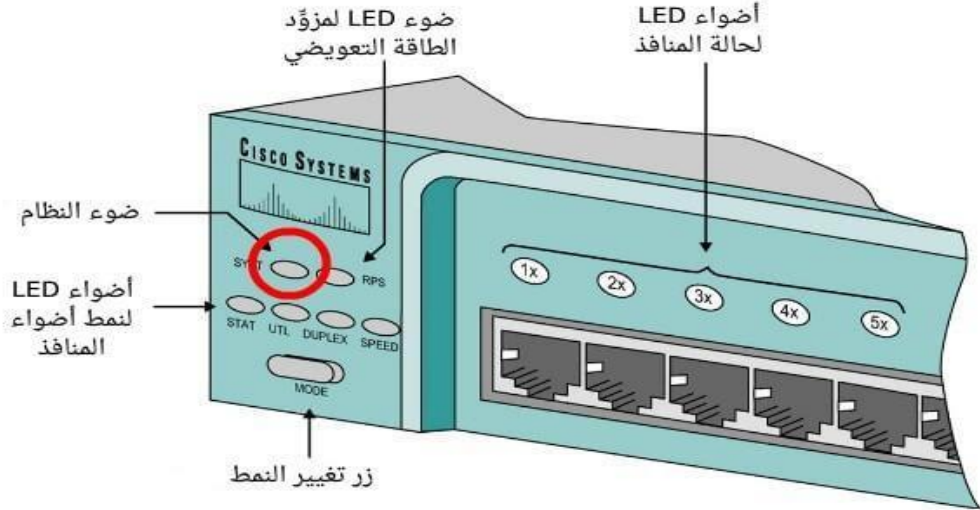
الضبط الابتدائي لمبدلات Cisco Catalyst

تكون مبدلات سيسكو جاهزة لتوفير قابلية الاتصال ووظائف الطبقة الثانية عند إقلاعها. تتضمن عملية الإقلاع سلسلة من إجراءات الإقلاع لتهيئة النظام وجعل وظائفه متوفرة. وتعريف أساس للمنافذ (أو البطاقات) ؛ وإذا أردت مراقبة العملية، فتأكد من أنك تملك اتصالاً للمبدل عبر منفذ (console)، أو أن لديك احدى البرامج المستخدمة لتهيئة السوتش مثل HyperTerminal أو PuTTY.

في المبدلات البسيطة يؤدي وصل شريط الطاقة الكهربائية مباشرة إلى تشغيل المبدل وبدء عملية التهيئة. وفي هذه المبدلات البسيطة، لن تجد زر «on» أو «off» كما في المبدلات الأكثر تعقيداً مثل المبدلات في طبقة التوزيع (distribution layer) والمبدلات الأساسية (core layer switches)؛ يمكنك مراقبة تسلسل عملية الإقلاع خارجياً بالنظر إلى المبدل وملاحظة أضواء LED في هيكل المبدل، وأيضاً عبر اتصال console cable و بالنظر إلى مخرجات نظام IOS، التي تعرض معلوماتٍ عن التشخيص وعملية التهيئة بأكملها.

لاحظ أن هذه الكتاب التدريبي مبني على المبدل Catalyst 2960، وقد تختلف المخرجات أو الأوامر عن غيرها من المبدلات في المستقبل

إشارات أضواء LED في مبدلات Catalyst 2960



تُظهر الصورة أضواء LED في Catalyst 2960، تعرض الأضواء المختلفة معلومات قيمة عن حالة وإمكانيات المبدل. فضاء النظام (system LED) سيضيء بالأخضر لو كان النظام مشغلاً ويعمل عملاً سليماً، ولكنه سيصفر إذا كانت هنالك أخطاء عند الإقلاع أو مشكلة في النظام؛ وسيظهر لوناً أصفر في ضوء مزود الطاقة (power supply LED) إن فشل مزود الطاقة الرئيسية بإمداد المبدل بالطاقة وأصبح مزود الطاقة التعويضي يعمل بدلاً عنه. أما أضواء المنافذ فلها معانٍ مختلفة.

مهمة زر «النمط» (mode) هي التبديل بين الأنماط المختلفة التي تُعطي معانٍ مختلفة لأضواء المنافذ؛ على سبيل المثال، إذا اخترت نمط «stat» أو «الحالة» فهذا سيجعل أضواء المنافذ تظهر باللون الأخضر إن كان هنالك اتصال وكان ذاك الاتصال نشطاً؛ لكنها ستصفر إن أغلق المنفذ من المدير أو حُجِبَ بواسطة بروتوكول (spanning tree protocol)؛ ومثلاً، لو بدلت إلى نمط «الاستعمال» (utilization)، فإن عدداً من المنافذ ستضيء بالأخضر، مُظهرةً حجم مرور البيانات في المبدل؛ فمثلاً، عندما تُظهر كل أضواء LED لوناً أخضرًا فهذا يعني أن المبدل يعمل بنسبة 50% من قدرته، ويشير عدد أضواء آخر إلى نسبٍ أخرى.

مخرجات الإقلاع

سيُظهر نظام IOS معلومات أكثر تحديداً، فيعرض -بالإضافة لغير ذلك من الأمور- عنوان MAC للمبدل ومختلف مراحل عملية التهيئة؛ ويُظهر أيضاً مسار صورة نظام التشغيل IOS الذي تُحمّل منه، وحالة عملية التحميل؛ وبعد إتمام عملية التهيئة، سنحصل على وصول إلى واجهة سطر الأوامر؛ لكن

إن كانت ملفات ضبط المبدّل فارغة، فسيحوّل مباشرةً إلى نمط الإعداد الذي سيبدأ بسؤالنا أسئلةً عن الضبط الأساسي؛ يمكنك الانتقال إلى نمط الإعداد في أيّ وقتٍ باستدعاء الأمر `setup`.

الدخول إلى المبدّل والتحويل إلى نمط EXEC

ستكون في نمط EXEC عندما تدخل إلى واجهة سطر الأوامر، حيث يسمح لك ذلك النمط بمراقبة وعرض وصيانة المبدّل، لكنه يعتمد على الدور المُسنَد لك؛

ولكي تنتقل من نمط المستخدم العادي Enabe Mode إلى نمط المستخدم ذو الامتيازات User Mode، فعليك استخدام الأمر `enable`؛ ثم سيُطلب منك إدخال كلمة المرور إن كانت موجودة؛ إذ لا توجد كلمة مرور افتراضياً، ويمكنك معرفة أنك انتقلت إلى نمط المستخدم ذي الامتيازات باختلاف شكل المبحَث (prompt).

```
User Access Verification
Username: admin
Password:
Switch>enable
Password:
Switch#
```

حيث يظهر في نمط المستخدم العادي إشارة «أكبر من» كمحث، أما نمط المستخدم فيظهر فيه إشارة المربع؛ ولأسباب أمنية، لن تظهر كلمة المرور التي تكتبها على الشاشة؛ لكن إن كنت تتصل عبر جلسة Telnet، فستُرسل كلمة المرور بنص صريح دون تشفير؛ ولهذه يُنصح بشدة استخدام بروتوكولات فيها تشفير مثل SSH لتوفير خصوصية وأمان نقل البيانات.

ضبط المبدّل Switch Configuration

يمكنك استخدام أوامر المراقبة والصيانة مثل الأمر `copy` في نمط المستخدم؛ إذا أردت ضبط المبدّل، عليك أن تدخل إلى وضع الضبط؛ وهناك عدّة طبقات من أنماط الضبط؛ أكثرها شموليةً هو نمط الضبط العام، الذي يمكنك الدخول إليه بكتابة الأمر `configure terminal`، ثم ستشاهد المبحَث يتغيّر لكن إشارة المربع ستبقى موجودةً فيه لتخبرك أنك في نمط المستخدم ذي الامتيازات، وستجد اسم طبقة نمط الضبط التي أنت فيها مكتوبةً في المبحَث بين قوسين.

```
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

فمثلاً، يمكنك تغيير المبحَث، ويمكنك تفعيل كلمة المرور للجهاز أو تغييرها إن كانت مُفعَّلة، وتستطيع عرض لافتات (banners) للمستخدمين الذين يسجلون الدخول إلى السوتش . وإذا أردت ضبط مكونات مخصصة، فعليك الانتقال من وضع الضبط العام إلى وضع الضبط لذلك المكوّن؛ فمثلاً، لو أردت ضبط المنافذ، فعليك كتابة الأمر interface متبوعاً برقم مرجع المنفذ أو Interface ID، وفي هذه الحالة، مثلاً سندخل إلى منفذ fast Ethernet في الفتحة (slot 0) ، والمنفذ (port 1) ؛ و يكتب مختصراً Fast ethernet 0/1 ؛ وستعرف أنّك في وضع ضبط المنفذ وذلك بتغيّر المبحَث ليعرض الكلمة «config-if».

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#
```

ويمكن أيضاً ضبط وصلة VTY لوصول Telnet أو الدخول إليها من نمط الضبط العام. وإذا أردت العودة إلى النمط السابق؛ فأدخل الأمر exit؛ الذي سيأخذك -على سبيل المثال- من نمط ضبط المنافذ إلى نمط الضبط العام. وإذا أردت العودة مباشرةً إلى طبقة User Mode ، فيمكنك الضغط على Ctrl-Z أو end وستذهب إلى أول طبقة، التي هي نمط المستخدم User Mode.

أولى المهام في نمط الضبط العام هي تسمية المبدّل؛ يسمح لك الأمر hostname بإعطاء اسم للمبدّل، وسيتغيّر المبحَث لأن اسم السوتش سيصبح جزءاً منه. ويمكن أيضاً أن يُستعمل اسم السوتش لأغراض إدارية، للتعرف بسرعة إلى السوتش بالنظر إلى المبحَث، أو لغيرها من الأغراض بما في ذلك تفعيل DNS في السوتش

```
Switch(config-if)#^Z
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname DSTR2
DSTR2(config)#
```

يمكنك أيضاً توفير عناوين IP Address للسوتش بالذهاب إلى منفذ معيّن بالأمر interface من نمط الضبط العام ثم استخدام الأمر ip address كما هو موضّح في المثال لتعريف عنوان IP وقناع الشبكة الفرعية (subnet mask)؛ وفي هذه الحالة، نحن نستعمل سوتش في الطبقة الثانية في 2960 ولذا ستكون منافذ الطبقة الثالثة المتوفرة هي منافذ VLAN ، نحتاج عناوين ip address في السويتش لأغراض إدارية فقط .

يمكنك أيضًا أن ترى بعض الاستعمالات للأمر shutdown؛ يمكننا استخدام الأمر مع الكلمة المحجوزة «no» وهذا شائع في أغلبية أوامر سيسكو؛ بمعنى آخر، تنفيذ الأمر shutdown سيعطل البطاقة إداريًا، لكن تنفيذ الأمر no shutdown سيعيد تفعيلها. وبهذه الطريقة يمكنك إزالة عناوين IP التي أسندتها عبر استخدام الأمر no ip.

```
DSTR2 (config) #vlan 10
DSTR2 (config-vlan) #name Management
DSTR2 (config-vlan) #exi
% Applying VLAN changes may take few minutes. Please wait...
DSTR2 (config) #int vlan 10
DSTR2 (config-if) #ip address 192.168.0.10 255.255.255.0
DSTR2 (config-if) #
```

ضبط البوابة الافتراضية في المبدل Default Gateway on the Switch

سيتمكّل ضبط IP في مبدّلات الطبقة الثانية Layer 2 Switch عند ضبط البوابة الافتراضية. ليس لدى المبدّل جدول توجيهات Routing table ، ولهذا سيحتاج إلى عنوان IP للبوابة الافتراضية (إلى منفذ الراوتر) ، مثله مثل أية جهاز كمبيوتر في الشبكة المحلية . يمكنك تحديد عنوان IP للبوابة الافتراضية (default gateway) باستخدام هذا الأمر في نمط الضبط العام؛ وبهذا يكون المبدّل قادرًا على الوصول إلى الوجهات البعيدة. وهذا يُستعمل عادةً لأغراضٍ إدارية لتمكّن من الاتصال عبر Telnet و SNMP للوجهات البعيدة.

```
DSTR2 (config) #ip default-gateway 192.168.0.1
DSTR2 (config) #
```

حفظ الضبط

علينا أن نتذكّر أن تلك الأوامر مُفعّلة وتعمل على السوتشس ؛ لكنه موجودة في الضبط التشغيلي فقط "NVRAM Memory" ؛ أي أنها لم تُحفظ إلى الضبط الإقلاعي "Flash Memory" ، الذي سيقراه السوتشس بعد إعادة الإقلاع. حفظ الضبط هو عملية يدوية والأمر المستخدم هو:

```
copy running-config startup-config
```

وسنُسال عن اسم الملف الهدف، الذي هو مضبوط افتراضياً؛ يمكنك ببساطة الحفظ إلى ملف ضبط موجود مسبقاً اسمه **startup-config** موجود في NVRAM ؛ مما يضمن أن الضبط جاهز ومتوفر لكي يقرأه السوتشس بعد الإقلاع القادم؛ إذا لم تفعل ذلك، فستفقد الضبط التشغيلي في ذاكرة RAM عندما يفقد السوتشس الطاقة الكهربائية أو عندما تُعيد تشغيل السوتشس .

عرض حالة التشغيل المبدئية للمبدل

يمكنك التأكد من ضبطك والحالة الإجمالية وإمكانات المبدل بالأوامر الآتية:

```
show running-configuration
```

الذي -كما ذكرنا سابقًا- يعرض الضبط الفعال حاليًا في المبدل؛ بينما الأمر:

```
show startup-configuration
```

سيُظهر الضبط المحفوظ في NVRAM، و `show version` يُظهر الإعدادات الإجمالية وإمكانات السوتش بما في ذلك العتاد وإصدار البرمجيات، وملفات الضبط وصور الإقلاع. تسمح الأوامر الأخرى لك برؤية حالة المنافذ مثل الأمر `show interfaces`، الذي لا يُظهر الحالة فقط، بل وإحصائيات متعلقة بالبطاقات.

هذا مثالٌ عن ناتج الأمر `show version`، الذي يُظهر خصائص نظام IOS بما في ذلك أرقام الإصدارات ومجموعة الميزات، ويعرض النسخة المُصغَّرة من IOS (mini IOS) الموجودة في ROM، ومحمّل الإقلاع الذي قد يكون إصداره مختلفًا؛ وزمن التشغيل (uptime). ثم ستُعرض صورة IOS التي تم تحميلها من ذاكرة flash (وهذا ما يتم افتراضيًا)، لكن يمكن أن يكون السوتش قد حمّل الصورة من الشبكة.

```
Switch#show version
Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M),
Version 15.0(1)SE1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.

Compiled Thu 01-Dec-11 14:53 by prod_rel_tea

ROM: Bootstrap program is Alpha board boot loader
BOOTLDR: C2960S Boot Loader (C2960S-HBOOT-M) Version
12.2(55r)SE, RELEASE SOFTWARE (fc1)

Switch uptime is 28 weeks, 2 days, 6 hours, 15 minutes
System returned to ROM by power-on
System restarted at 18:16:59 EET Wed Dec 14 2011
```

```
System image file is "flash:/c2960s-universalk9-mz.150-1.SE1.bin"
...
cisco WS-C2960S-48TS-L (PowerPC) processor (revision F0) with
131072K bytes of memory.
Processor board ID XXXXXXXXXXXX
Last reset from power-on
2 Virtual Ethernet interfaces
1 FastEthernet interface
104 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

ثم ستظهر إعدادات العتاد الإجمالية، بما في ذلك كمية الذاكرة، التي تُعرض على هيئة رقمين: الذاكرة المشتركة (shared memory) والذاكرة المتوفرة لبقية النظام؛ إذا جمعت هذين الرقمين، فستحصل على كمية ذاكرة RAM الإجمالية الموجودة في السوتش.

ويظهر أيضاً العدد الإجمالي للمنافذ الفيزيائية، وتُظهر بقية الناتج (التي لم تُعرض هنا) كمية ذاكرة flash وقيمة مسجل الضبط (configuration register).

يُستخدم الأمر `show interfaces` عادةً للضبط الدقيق، لكنه يستعمل أيضاً للمراقبة واستكشاف الأخطاء وإصلاحها؛ يمكنك استعمال الأمر `show interfaces` لإظهار معلومات عن جميع المنافذ، أو يمكنك تحديد المنفذ الذي تريد عرض معلوماتها. يُعرض الأمر حالة الطبقة الأولى Physical Layer، وحالة الطبقة الثانية Data Link Layer التي تتضمن عنوان MAC وحالة duplex وسرعة المنفذ متبوعةً بسلسلة من الإحصائيات تتضمن آخر إزالة للعدادات (counters)، واستراتيجية الطابور (queuing strategy)، ومعدلات الدخول والخروج في آخر 5 دقائق بوحدة «بت في الثانية» و «رزمة في الثانية»، ثم إحصائيات متعلقة بالترزم الإجمالية والأخطاء المتعلقة بعدة تصنيفات.

وكجهاز في الطبقة الثانية، ستحافظ المبدلات على جدول عناوين MAC، حيث ستتعلم عناوين MAC ديناميكياً بالنظر إلى ترويسات الإطارات ثم ستتمكن من تحديد أماكن تلك العناوين وربطها مع المنافذ لتمكين تمرير الرزم أو الإطارات بشكلٍ ذكي. يمكنك عرض جدول عناوين MAC بالأمر:

```
show mac address-table
```

الذي سيُظهر عناوين MAC ونوعها والمنفذ الذي تتصل الأجهزة حاملةً عناوين MAC السابقة منه. قد تكون بعض عناوين MAC ثابتة، فجزءٌ منها متعلقٌ بالاستخدام الداخلي لمبدلات Catalyst 2960؛

ملاحظة :

تذكر أن بعض المدخلات في الجدول ستنتهي صلاحيتها، وتُحذف، ثم ستُضاف مرة أخرى

ضبط رمز دخول للسوتش: Configuring passwords:

(هذا الأمر يستخدم لوضع رمز دخول ذات شفرة سرية يصعب الحصول عليه)

```
1 SW1(config)# enable secret cisco ! MD5 hash
```

(أما إذا أردت استخدام رمز الدخول بدون شفرة عليك استخدام الأمر أعلاه)

```
SW1(config)# enable password notcisco ! Clear text
```

حماية مدخل الكونسول للسوتش: Securing console port:

```
SW1(config)# line con 0
SW1(config-line)# password cisco
SW1(config-line)# login
```

حماية الدخول من بعد للأجهزة: Securing telnet lines:

```
SW1(config)# line vty 0 4
SW1(config-line)# password cisco
SW1(config-line)# login
```

استخدام شفرة حماية الرمز السري الشامل: Encrypting passwords:

```
SW1(config)# service password-encryption
```

وضع رسالة تنبيهية للمستخدمين: Configuring banners:

تستخدم رسائل التبيه غالبا من اجل تحذير دخول الغير مصرح لهم من استخدام السوتش و ذلك لا يمنع احدا من الدخول لكن فقط للتحذير مثل لافتات , ممنوع الدخول , و ممنوع التدخين , .. الخ

```
SW1(config)# banner motd $
-----
```


UNAUTHORIZED ACCESS IS PROHIBITED

\$

تعيين عنوان للسويتش: Giving the switch an IP address:

في العموم جهاز السويتش يعبر من اجهزة الطبقة الثانية انه لا يقبل عنوان ip يعمل على اساس MAC address فقط لكن من اجل الدخول للسويتش من داخل الشبكة او الخارج لابد من عنوان IP له , وذلك في مدخل الشبكة الافتراضية VLAN 1 ثم يكون العنوان من نفس الشبكة و نضيف عنوان الراوتر default gateway ليتثنى لنا الدخول من خارج الشبكة

```
SW1(config)# interface vlan 1
SW1(config-if)# ip address 172.16.1.11 255.255.255.0      !
or DHCP
SW1(config-if)# no shutdown
```

حفظ الضبط في ذاكرة التخزين Saving configuration:

في نهاية كل عمل يجب حفظ الضبط في ذاكرة السويتش و لا سنفقد كل الضبط بمجرد اعادة تشغيل السويتش او فصل التيار الكهربائي من السويتش

```
SW1# copy running-config startup-config
Destination filename [startup-config]?      ! Press enter to
confirm file name.
Building configuration...
[OK]
```

```
! Short for write memory.
SW1# wr
Building configuration...
[OK]
```

انواع مداخل الكايل و السوتش :

Haf Duplex

ينقل البيانات حتى سرعة 10 mbps و ميزة هذا المدخل يعتبر Haf Duplex اي انه لا يرسل و يستقبل في نفس الوقت

Full Duplex

ينقل البيانات بسرعة عالية و يمكنها ان ترسل و تستقبل في نفس الوقت

ضبط السرعة و الإرسال و إنشاء Description, speed and duplex: وصف المدخل:

```
SW1(config)# interface fastEthernet 0/1
SW1(config-if)# description LINK TO INTERNET ROUTER
SW1(config-if)# speed 100      ! Options: 10, 100, auto
! The range keyword used to set a group of interfaces at
once.
SW1(config)# interface range fastEthernet 0/5 - 10
SW1(config-if-range)# duplex full (options: half, full, au-
to)
```

Verify Basic Configuration:

لمعاينة الضبط السابق:

- Shows information about the switch and its interfaces, RAM, NVRAM, flash, IOS, etc.
- لمعرفة حجم الذاكرة و نوع الفلاش و رقم إصدار نظام التشغيل و بعض المعلومات العامة
SW1# `show version`
- Shows the current configuration file stored in DRAM.
- لعرض الضبط الحالي المخزن في الذاكرة
SW1# `show running-config`
- Shows an overview of all interfaces, their physical status, protocol status and ip address if ما إذا كان لديه عنوان أي عرض حالة مدخل الكابل و حالة البروتوكول و بي أمر لا و ما نوعه
- SW1# `show ip interface brief`
- Shows detailed information about the specified interface, its status, protocol, duplex, speed, encapsulation, last 5 min traffic.

- عرض جميع حالات المدخل المعني وسرعة إرسال البيانات في المدخل و حالة البرتوكول المستخدم لآخر 5 بيانات أرسلت في ذلك المدخل

```
SW1# show interface vlan 1
```

- Shows information about the leased IP address (when an interface is configured to get IP address via a dhcp server)
- عرض معلومات عن العناوين التي أرسلت من قبل دي اتش سي بي سيرفر لأجهزة الكمبيوتر

```
SW1# show dhcp lease
```

تقسيم الشبكة المحلية إلى أقسام داخلية: VLANs (Virtual LAN):

الشبكة المحلية الافتراضية VLAN تتضمن جميع الأجهزة في نفس نطاق البث (Broadcast Domain)

نطاق البث يشمل مجموعة من الأجهزة المتصلة بـ LAN والتي عندما يرسل أي جهاز إلى إطار بث فإن كل الأجهزة الأخرى يكون لها نسخة من نفس الإطار ؛

بدون الشبكة الافتراضية يتخيل المبدل "Switch" أن كل الواجهات تقع في نفس نطاق البث بمعنى أن الوضع يبدو وكأن كل الأجهزة متصلة بنفس الـ LAN.

* * نطاقات البث التي تنشأ بواسطة المبدل تسمى شبكات افتراضية أو (VLAN)

وضع أجهزة الحاسب في شبكات ظاهرية مختلفة له العديد من الفوائد منها أن

❖ تقسيم البث Broadcast .

يساعد تقنية VLANs على تقسيم حزم البث داخل الشبكة المحلية المرسله بواسطة أحد الأجهزة في شبكة ظاهرية معينة سيستقبل و يعالج بواسطة الأجهزة الموجودة في نفس الشبكة الظاهرية فقط

❖ كلما زاد عدد الأجهزة المضيقة في الشبكة الظاهرية كلما زاد الوقت المطلوب لمعالجة البث و كلما زاد عدد الأجهزة كلما زاد عدد البث الذي يتعرض له الجهاز المضيف و الذي يمكن أن يلتقطه الهاكر بواسطة أحد برامج تحليل الشبكة مما يجعله معرض لهجمة استطلاع

لذلك لابد من تقسيم الأجهزة الى شبكات ظاهرية مختلفة VLAN و يمكن تلخيص الأسباب كالتالي :

- لإنشاء تقسيم أكثر مرونة و الذي يقسم المستخدمين حسب الأقسام و المجموعات و ليس حسب الموقع المادي او الجغرافي .
- تقليل الضغط الناتج عن رسائل البث بواسطة التقسيم إلى شبكات ظاهرية مختلفة.
- لتحسين السرية من خلال عزل الأجهزة ذات المعلومات المهمة السرية على شبكات ظاهرية مؤمنة خاصة.
- لعزل مرور البيانات المرسله بواسطة هاتف IP Phone .

الضبط العملي لتقسيم الشبكة الداخلية: Configuring VLANs:

لإنشاء شبكة داخلية يجب تصميم الشبكة الداخلية بما يناسب حالة العمل و نظام التواصل بين الاجهزة , حيث يقطع vlan التواصل مع جميع الاجهزة التابعة الى شبكة VLAN اخر

- Create a new VLAN and give it a name:

• إنشاء شبكة داخلية و تسميته :

```
SW1(config)# vlan 10
SW1(config-vlan)# name SALES
```

- Assign an access interface to access a specific VLAN:

حين التفكير في انشاء شبكة داخلية يجب اعتبار نوعين من مداخل السوتش اما ان يكون المدخل access port و ذلك في حال المدخل متصل بجهاز كمبيوتر او طابعة او ما شابه اما اذا كان متصل بسوتش اخر او راوتر فيكون المدخل trunk port و ذلك لأن trunk port يحمل بيانات جميع بيانات VLANs ID

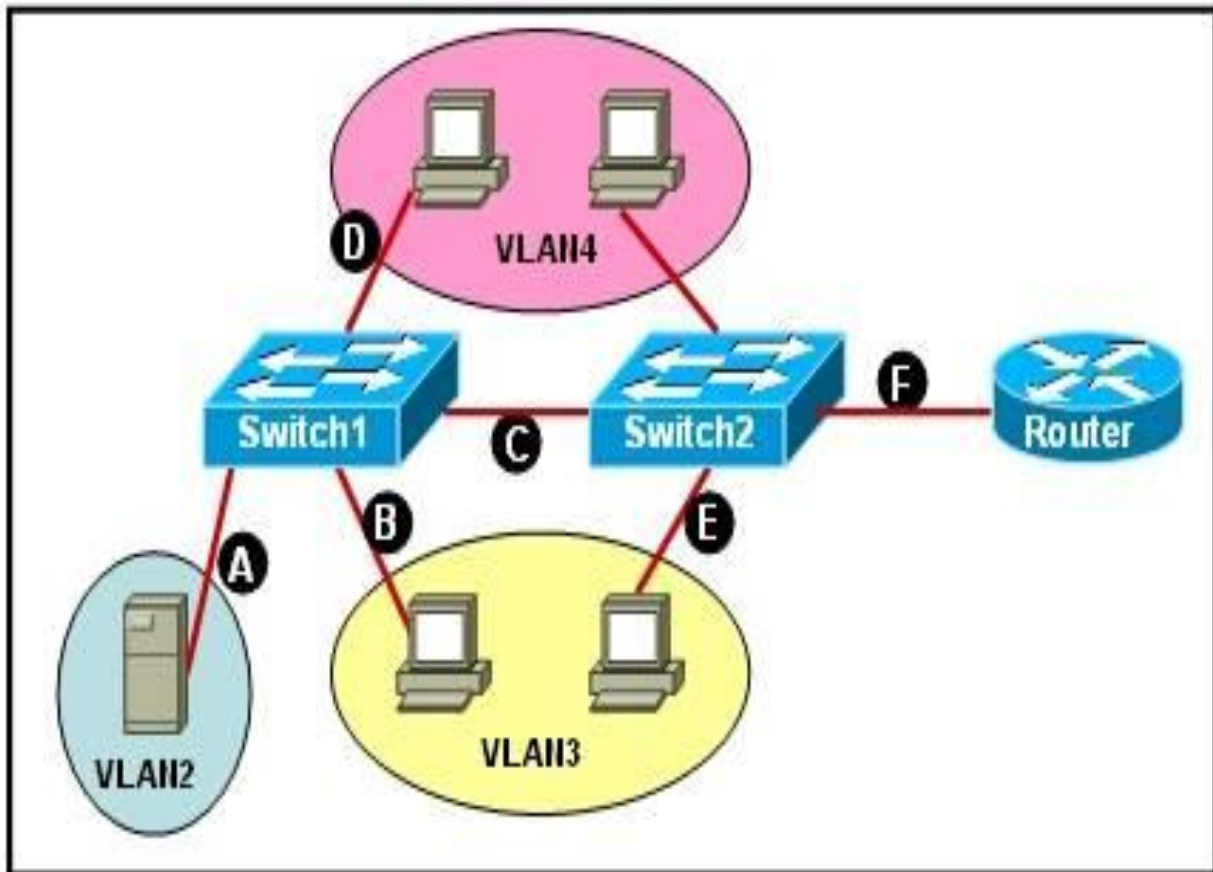
إضافة مدخل السوتش الى شبكة محلية Access port:

```
SW1(config)# interface fastEthernet 0/5
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
```

Configuring Trunks:

إضافة مدخل السوتش الي trunk port :

```
SW1(config)# interface fastEthernet 0/1  
SW1(config-if)# switchport mode trunk
```



طرق حماية الشبكة الداخلية: Securing VLANs and Trunking:

Administratively disable unused interfaces:

إغلاق جميع المداخل الغير المستخدمة في السويتش:

```
SW1(config-if)# shutdown
```

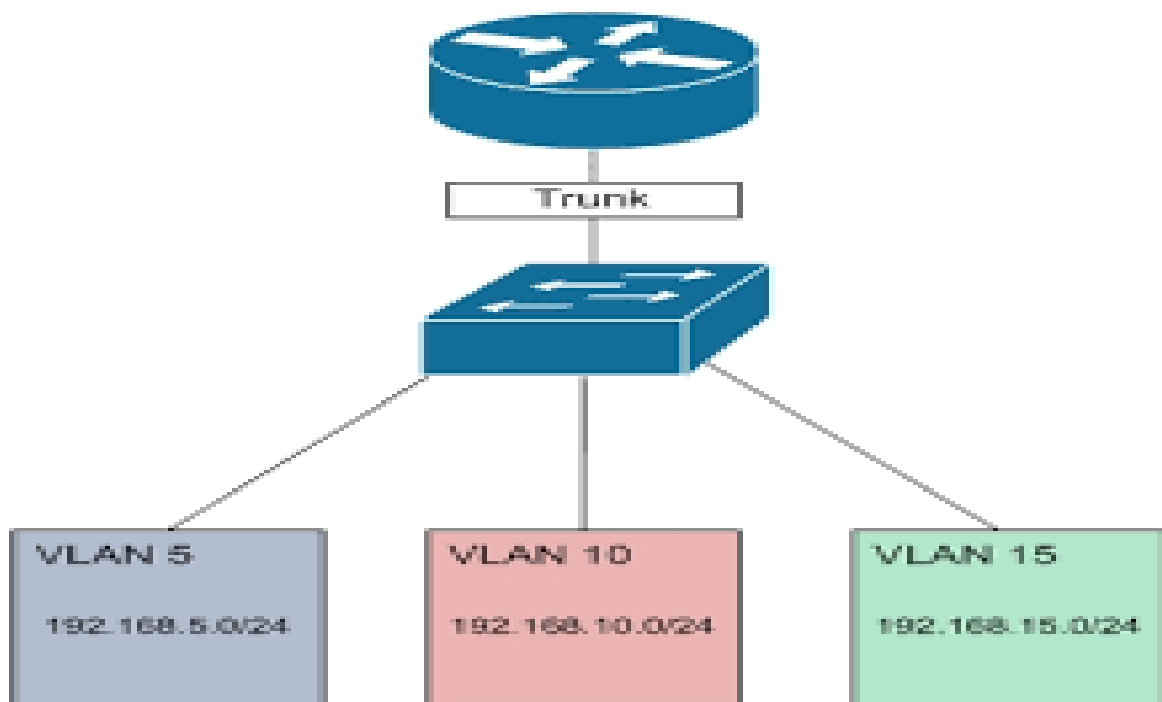
- Assign the port to an unused VLAN:

• انساب المداخل الغير مستخدمة إلي شبكة داخلية وهمية غير مستخدمة

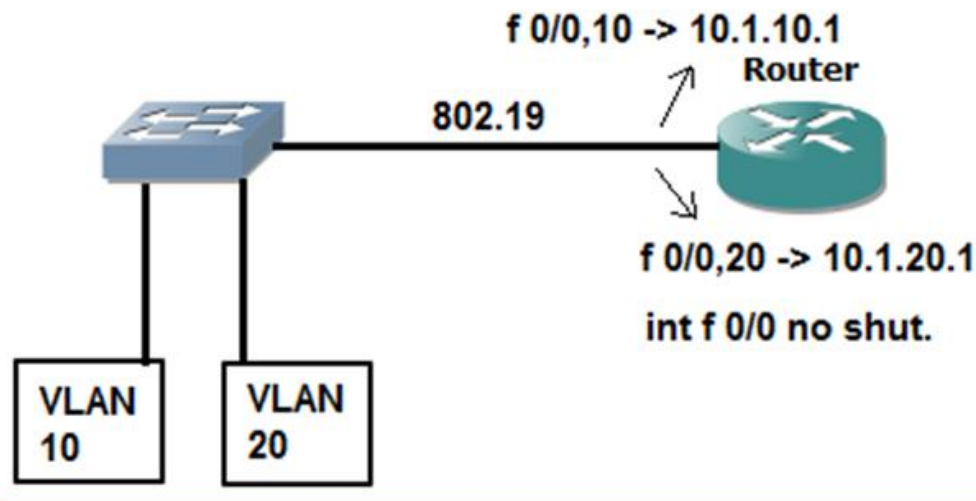
```
SW1(config-if)# switchport access vlan 222
```

INTER-VLAN ROUTING ::

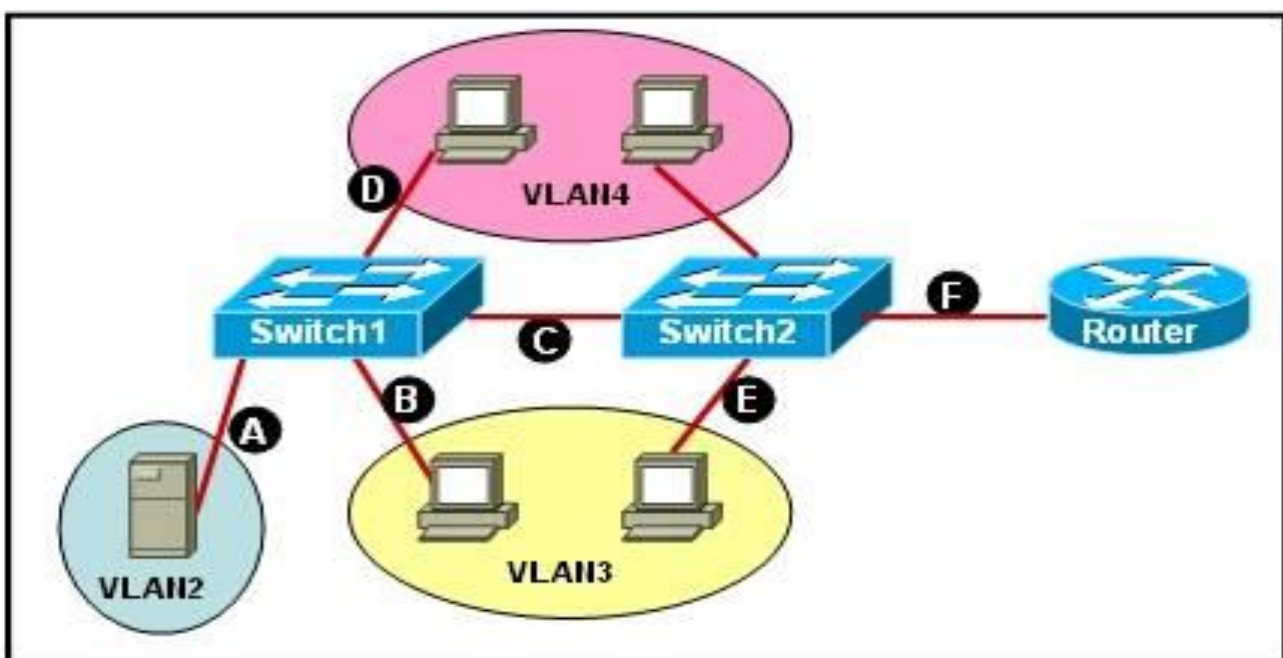
عملية التواصل بين الشبكات المحلية الجزئية



configuring Router-On-Stick for vlan routing:

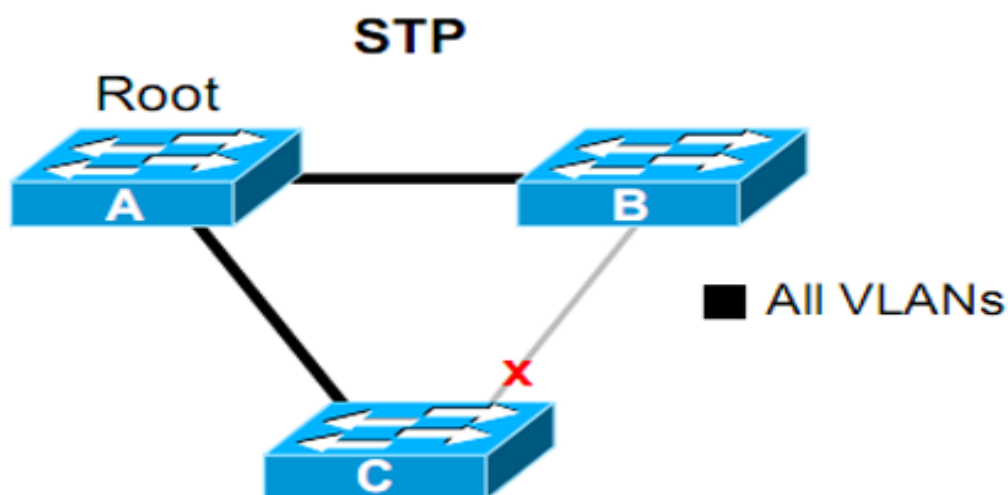


```
R1(config)# interface fastEthernet 0/0
R1(config-if)# no shutdown
R1(config)# interface fastEthernet 0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface fastEthernet 0/0.20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
```

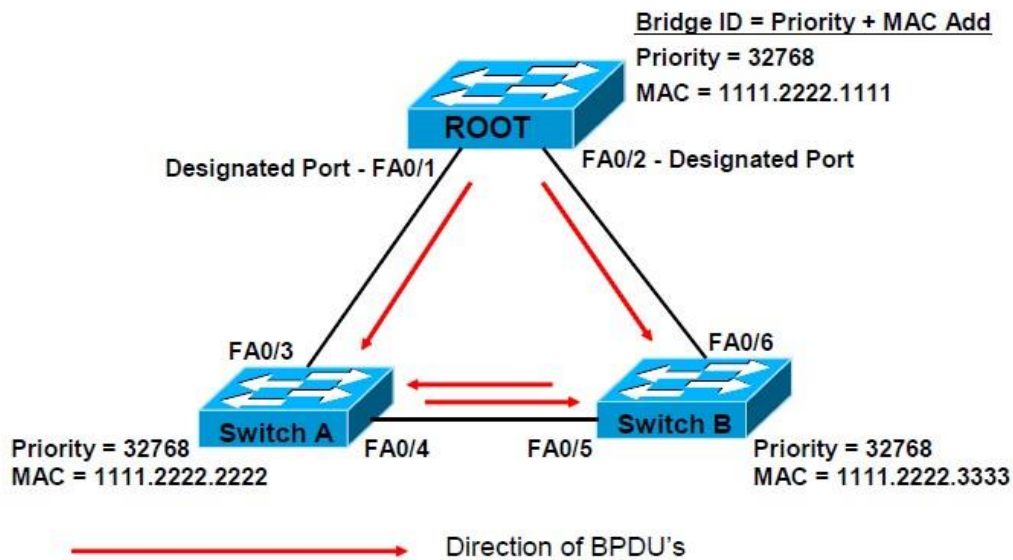


STP (Spanning Tree Protocol)

ال STP الذي يعرف من خلال منظمة IEEE بي 802.1D يتصف هذا البروتوكول بأنه يعمل على كل أنواع الأجهزة سيسكو كانت أم جونيبر وبدون تمييز وما يميزه هو وجود شبكة Spanning Tree واحدة أو One Instance تضم جميع ال Vlanس ويتم تبادل ال BPDUs بين السويتشات من خلال ال Native Vlan وهو يعمل من خلال Instance واحدة تضم كل البورتات وتضم كل ال Vlanس الموجودة في الشبكة (سوف نفهم فكرة ال Instance أكثر عندما تصل إلى MSTP)



Root Election & BPDUs Propagation



STP optimization:

ضبط عملي :

- Hard coding the root bridge (changing bridge priority):
- اختيار السويتش الأساسي يدويا بدلا من اختياره اتوماتيكيا

```
SW1(config)# spanning-tree vlan 1 root primary
SW1(config)# spanning-tree vlan 1 root secondary
! Priority must be a multiply of 4096
SW1(config)# spanning-tree [vlan 1]priority 8192
```

- Bundling interfaces into an ether channel:

دمج عدة مداخل في العمل على انه مدخل واحد

```
SW1(config-if)# channel-group 1 mode on ! options: auto, desirable, on
```

STP verification and troubleshooting:

أوامر المعاينة وحل المشكلات التقنية:

- Shows detailed info about STP state:

- لمعرفة التفاصيل عن البرتوكول

```
1SW1# show spanning-tree
```

- Shows STP info only on a specific port:
• معرفة عمل البروتوكول في مدخل معين :

```
1SW1# show spanning-tree interface fa0/2
```

- Shows STP info only Shows info about the root switch
معرفة عمل البرتوكول في شبكة داخلية معينة :
for a specific VLAN:

```
1SW1# show spanning-tree vlan 1
```

- Show the state of the ether channels
:لعرض حالة المداخل المدمجة في السويتش :

```
SW1# show ether channel 1
```

المراجع :

CBT Nuggets

CCNA Routing &Switching Todd Lammle

Cisco website (www.cisco.com)

المؤلف :

م/طارق على يوسف

بكلاريوس [Bachelor of Computer Applications] BCA

Osmania University Hyderabad India

الجامعة العثمانية – حيدرآباد , الهند

professional degree

University College of Science , Sifabad , Hyderabad – India

CCIE (Routing & Switching) cisco ID NO : CSC012796639