الفصل الثاني IOS Access Commands

بعد أن قمنا بتوصيل الموجه إلى الحاسوب اتصالا مباشرا عن طريق Console Port ، و استخدمنا البرنامج الطرفى مثل برنامج Tera Term حتى نتصل بالموجه، و قمنا بتشغيل الموجه و تابعنا الرسائل المتتالية التى تظهر و دلالة كل منها. وصلنا إلى مرحلة الدخول على الموجه و البدء فى إعداد الخصائص التى تحدد استخداماته فيما بعد.

و أريد أن أكرر معلومة هامة، و هى أن إعداد خصائص الموجه تتم كلها عن طريق إدخال الأوامر، أى أنها ليست بطريقة الواجهة الرسومية GUI Graphical User Interface ، و لكن كلها ستكون كتابةً، و التى سوف نعرض هنا معظمها، و سنبين وظيفة كل أمر و كيف يكتب و فى أى حالة أيضا.

كما قلت سابقا فى المقدمة أن نظام الإعداد IOS هو نفسه على كل أنواع الموجهات باختلاف فئاتها، و نستخدم نفس طريقة الدخول، و تظهر لنا نفس علامة البدء. و الاختلاف يكون فقط فى الخدمات التى يقدمها الموجه باختلاف فئاته و التى يكون لكل خاصية منهم طريقة للإعداد، و تتفق كل الموجهات فى الأوامر الأساسية المستخدمة و طرق التخصيص الابتدائية. و هذا يشعرنا بالراحة لأننا إذا جلسنا أمام أى موجه من أى فئة فسوف نجد نفس الخطوات الأساسية التى نستخدمها على أى نوع آخر مما يسهل التعامل معه.

أولا/ الولوج إلى الموجه Router Login

سوف نبدأ الإعداد بافتراض أن الموجه قد قام بتحميل النسخة المعدة سابقا فى الذاكرة من نظام الإعداد، فتظهر لنا الرسائل التالية بعد انتهاء التحميل:

1- Router Con0 in now available
2- Press RETURN to get started
3- Router>

1- تبين هذه الرسالة أن الموجه قد تم الاتصال به عن طريق منفذ Console، و قد استخدم الرقم صفر أو 0 لأن المنافذ على الموجه تبدأ بالترقيم من 0 و ليس 1 كما هو الحال فى السويتش. بمعنى أنه لو كان هناك منفذ Console آخر موجود على الموجه، فإنه كان سيأخذ الترقيم 1 و يصبح اسمه Con1.

2- هذه الرسالة تظهر بعد الانتهاء تماما من التحميل، و فيها نضغط على مفتاح الإدخال Enter حتى ندخل إلى الخطوة التالية.

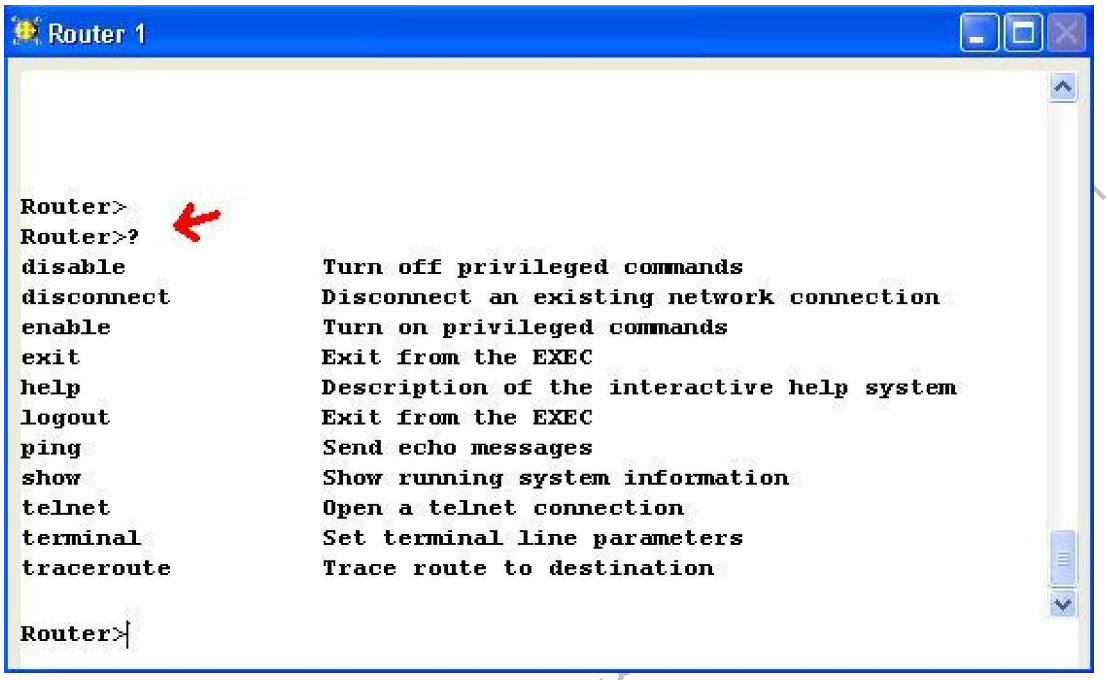
3- هذه العلامة هى أول علامة تظهر لنا فى الموجه و التى يمكن أن نستخدم من خلالها الأوامر للبدء فى التخصيص، و هى تظهر مباشرة بعد الضغط على مفتاح الإدخال كما ذكرنا فى المرحلة السابقة. أنظر إلى الصورة التالية حتى تتضح الرؤية أكثر. حيث تبين أن هناك مقطعان بينهما فاصل، المقطع الأول قبل العلامة ">" و هو اسم الموجه و الذي يحمل هنا الاسم التلقائي "Router" و يمكن تغييره. و المقطع الثاني بعد العلامة الفاصلة و هو المكان الذي نكتب فيه أوامر الإدخال للموجه بواسطة لوحة المفاتيح. كما أن ما يميز حالة المستخدم "User Exec Mode" هي هذه العلامة الفاصلة لأنها تتغير من حال إلى حال إلى أشكال أخرى.

هذه النسخة أمانة فلا تغير فيها و نشرها على الإنترنت

ثانيـا/ أوامر المساعدة:

هناك الكثير من الأوامر المساعِدة الموجودة على الموجه حتى تسهل عملية الإعداد نذكر منها:

1- عند وضع علامة الاستفهام " ؟ " و الضغط على إدخال "enter" سوف تظهر كل الأوامر التى يمكن أن نستخدمها في نطاق الحالة التي وضعنا عليها علامة الاستفهام. كما هو مشار بالسهم الأحمر (أنظر الصورة)



2- يمكن استخدام زر " tab " لاستكمال أمر قد نكون نسينا باقى حروفه. على سبيل المثال أننا سنكتب الأمر Configure فيمكننا فقط كتابة أول ثلاثة حروف ثم الضغط على زر " tab " و سوف يكتمل الأمر تلقائيا.

3- يمكن كتابة الأوامر مختصرة دون الحاجة إلى كتابتها كاملة مثل هذه الأوامر:
أمر enable إلى ena
أمر Configure إلى config أو conf
أمر terminal إلى t

و سوف أذكر اختصارات أى أمر سوف نستخدمه فيما بعد إذا كان متاحا

بداية من هذه المرحلة سوف نحتاج أحد أمرين، إما أن نتمرن على موجه حقيقى، و إما أن نحصل على محاكي الموجه Router Simulator حتى نستطيع اختبار الأوامر التى أوردنا ذكرها. و سوف أحاول أن ألتقط بعض الصور من اتصالى بالموجه الذى لدى بالمنزل أو الموجود بالعمل لإظهار بعض العمليات و لكنها لا تغنى عن استخدام المحاكى أو الموجه الحقيقى.

هذه المذكرة منشورة على الانترنت بدون إذن صاحبها

ثالثـا/ الحالة المتقدمة Global Configuration Mode

هناك ثلاث حالات التي تظهر للموجه:

1- حالة المستخدم User Mode
2- حالة Privileged Mode
3- حالة Global Configuration Mode

1) حالة User Exec Mode :

هذه الحالة هي أول حالة يظهر بها الموجه مثلما اتضح من الفقرة السابقة، و فيها يتم إدخال أوامر بسيطة جدا مثل أمر ال Telnet لعمل اتصال بموجه آخر مثلا، أو Ping لاختبار سلامة الاتصال بجهاز آخر على الشبكة، أو أوامر الإظهار Show لإظهار الكثير من خصائص الموجه، و بعض الأوامر البسيطة الأخرى. و يميزها العلامة الفاصلة ">" بعد اسم الموجه مباشرة. و يكون شكلها كالتالي:

```
Router>
```

2) حالة Privileged Mode :

هذه الحالة يمكن أن نستخدم فيها أوامر متقدمة عن الحالة السابقة، و تظهر هذه الحالة بعد كتابة الأمر enable في حالة User Mode، و من الأوامر التي يمكن استخدامها في هذه الحالة أمر Setup و الذي يمكن المستخدم من إعداد خصائص الموجه في صورة أسئلة يعطيها لك الموجه و تقوم فقط بوضع المدخلات، أو أمر Debug لمراقبة العمليات التي تحدث للموجه، و الكثير غيرها. و يميز هذه الحالة العلامة الفاصلة "#" بعد اسم الموجه مباشرة.

كما يبين الشكل التالي شكل علامة هذه الحالة و كيف تظهر:

```
Router> enable
Router#
```

3) حالة Global Configuration Mode :

و هذه الحالة هي الحالة المتقدمة لإعداد الموجه و فيها يمكننا القيام بمهام أكثر تقدما من سابقتها في الحالتين السابقتين، حيث نستخدم فيها الأوامر الكبيرة في إعداد خصائص كل مخارج الموجه، و تحديد شكل الشبكة، و تحديد البروتوكولات التي ستستخدم على الشبكة و الكثير غيرها.

و من أمثلة التغييرات التي نقوم بها على الموجه في هذه الحالة تغيير كلمات السر، و تغيير اسم الموجه Host Name ، و تغيير خصائص الحماية. و يتم الانتقال إلى هذه الحالة بكتابة الأمر Configure Terminal في الحالة Privileged Mode. و يميزها العلامة الفاصلة "#" أيضا و لكن ليس بعد اسم الموجه مباشرة، و لكن يكون بينهما كلمة (config) لتميزها عن الحالة السابقة. و يكون شكلها كالتالي:

```
Router> enable
Router# configure terminal
Router(config)#
```

إذاً تعلمنا من النقاط السابقة أن للموجه ثلاث حالات، ننتقل بينها باستخدام الأوامر لننتقل من حال إلى حال. و يمكننا الرجوع إلى الحال السابقة بكتابة الأمر Exit في أي من الحالات السابقة. كان هذا عرض أولي لحالات الموجه و استخدامات بسيطة لكل حالة، و لكن في المرات التالية سنذكر الأوامر التي سنستخدمها لإعداد و تشكيل خصائص الموجه في مختلف الحالات. و الصورة التالية تبين شكل هذه الحالات من خلال موجه حقيقي.

هذه النسخة مؤقتة فلا تغير فيها أو تنشرها على الانترنت دون

رابعـــا / تأمين نقاط الدخول Access Points

الخطوة التالية هنا هي كيف نحمي الموجه من الدخول غير المشروع، و بما أن الموجهات هي العمود الفقري الذي تعتمد عليه الشبكات، فإن الحفاظ عليه من الدخول غير المشروع يعتبر من أهم الأمور التي يجب الانتباه لها للحفاظ على ثبات و حضور الشبكة قدر الإمكان و الحفاظ عليها من التلاعب.

و كما بينت سابقا أن طرق الاتصال بالموجه ثلاثة، إما عن طريق منفذ Console، أو عن طريق منفذ Auxiliary، أو عن طريق telnet. و هذه الطرق الثلاثة تسمى بنقاط الدخول، سميت بذلك لأنها المنافذ الأساسية للدخول إلى الموجه و باستخدامها فإننا نخطو الخطوة الأولى على أعتاب الموجهات. و تفعيل كلمات المرور للطرق الثلاثة ستمنع الدخول إلى الموجه تماما منذ البداية و حتى قبل الوصول إلى حالة المستخدم العادي User Mode.

بجانب أن طريقة الاتصال بواسطة ال Telnet لا يتم تفعيلها إلا بعد تمكين كلمة المرور لها. أي أنه قبل تمكين كلمة المرور لن تكون هذه الطريقة متاحة للاستخدام، و لن يقبل الموجه أي اتصال عبرها.

و كما نعلم أن طريقة الاتصال هذه تستخدم للاتصال بالموجه عن طريق الشبكة بدلا من حمل أحد الحواسيب المحمولة للاتصال المباشر بالموجه. و في السطور القادمة سوف أبين طرق تفعيل كلمات المرور و كيفية تشفيرها باستخدام الأوامر لكل الطرق.

خامســا / تمكين كلمات المرور Enable Mode Password

تمنح شركة سيسكو إمكانيات رائعة لتمكين كلمات المرور على الموجهات بأكثر من شكل، و لأكثر من حالة لدعم الأمان التام على الموجه. فهناك ما يسمى ب Enable Mode Password و التي تتيح إمكانية وضع كلمة مرور للانتقال من حالة المستخدم العادي User Exec Mode إلى حالة Privileged Mode، حيث تمنع الدخول إلى الحالة الثانية إلا بعد وضع كلمة السر التي تم تمكينها مسبقا، و ذلك لأهمية هذه الحالة التي تمكن المستخدم من تغيير الكثير من خصائص الموجه بدءا من تغيير أرقام IP و انتهاء بتغيير كلمات المرور نفسها.

برجاء الانتباه أن هذه الطريقة تسمى ب enable mode password لأنه يشار إليها في الامتحان بنفس الاسم لتمييزها عن كلمة المرور المشفرة و التي سيأتي شرحها في النقطة التالية.

سادســا / تمكين كلمة السر Secret Password

هنا قد يحتار الناس بين الأمران، و سيأتي السؤال المتوقع و هو ما هو الفرق بين كلمة المرور و كلمة السر؟ الفرق أن كلمة المرور لا تكون مشفرة بعد تمكينها، أي أنها تظهر للمستخدم عندما يقوم باستعراض خصائص الموجه بعد الدخول إلى الحالة Privileged بشكل واضح، أي تظهر كلمة المرور بوضوح بكل حروفها و أرقامها أو أياً ما يكون شكلها (Clear Text)، و بالتالي فأنت معرض لأن يلتقطها أحد المارين من خلفك و أنت تستعرض هذه الخصائص و يتمكن بعد ذلك من الدخول إلى الموجه إذا تعرف عليها، بينما كلمة السر عند تمكينها تظهر مشفرة، أي بحروف غير مفهومة، و بذلك لن يتعرف عليها أحد سواك.

أما من الناحية الوظيفية، فكلا الطريقتان تؤديان نفس الوظيفة. و إذا تم تمكين الكلمتين كلمة المرور و كلمة السر فإنه ستكون أولوية القبول لكلمة السر و ذلك لأنها أكثر أمنا للدخول على الموجه و لن يقبل كلمة المرور.

هذه النسخة أمانة فلا تنسخها أو تنشرها عبر الإنترنت بدون إذن صاحبها

سابعـا/ كيفية تمكين كلمات السر و كلمات المرور:

في هذا الجزء سوف أبين كيفية تمكين كلمات المرور و كلمات السر، و كيفية تأمين نقاط الدخول أيضا، و لكن سوف أبدأ بتمكين كلمة المرور و كلمة السر أولا، ثم أبين كيفية تمكينها على نقاط الدخول و ذلك وفقا للشكل الذي ننفذ به ذلك و الذي سيتبين من السطور التالية.

1) **تمكين كلمة المرور** enable mode password:

لتمكين كلمة المرور للانتقال من حالة المستخدم User Mode إلى حالة Privileged Mode يمكننا استخدام الأمر التالي لتفعيل ذلك. و إليكم الخطوات بالترتيب مع ملاحظة أن ما سنكتبه هو ما سيكون بعد العلامة الفاصلة، و ما قبلها سوف يكتبه الموجه تلقائيا:

Router> enable	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router (config)#enable password ciscogitex	أمر إدخال كلمة المرور

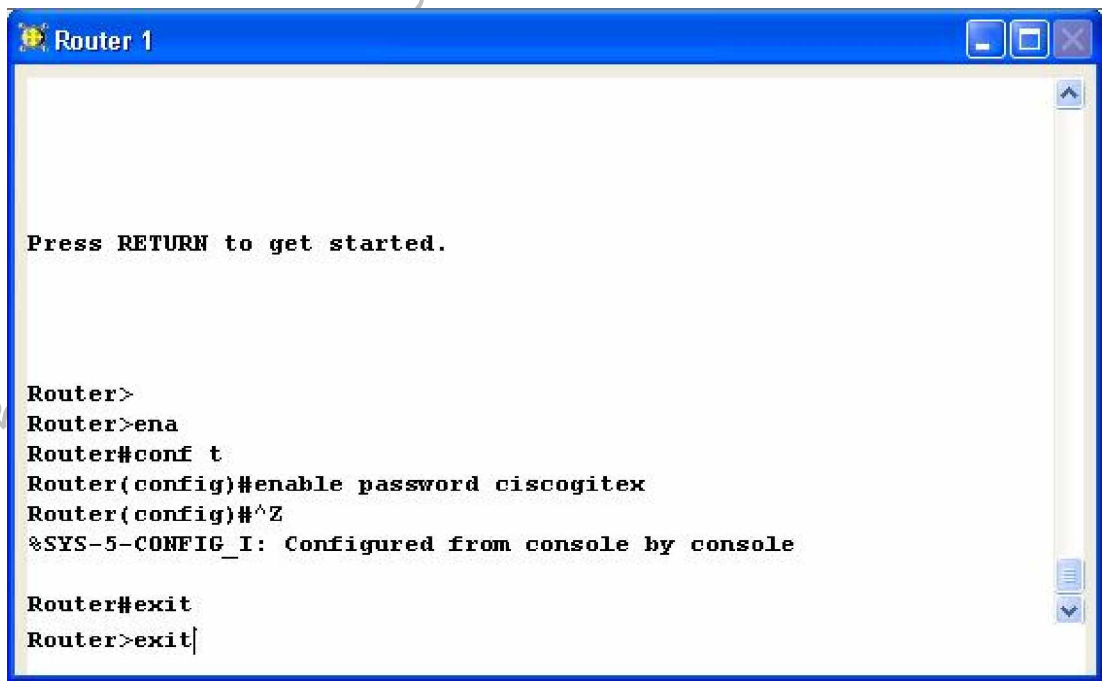
ملحوظة:

- في السطر الأول نحن في حالة المستخدم User Mode، و يميزها العلامة الفاصلة " > " بعد اسم الموجه، و بعد كتابة الأمر enable ننتقل إلى الحالة Privileged.
- في السطر الثاني نحن في الحالة Privileged، و التي يميزها العلامة الفاصلة " # " بعد اسم الموجه، ثم نكتب الأمر config t و هو اختصار الأمر configure terminal فننتقل إلى الحالة المتقدمة.
- في السطر الثالث نحن في الحالة المتقدمة Global Configuration Mode و يميزها كلمة (config) تتبعها العلامة الفاصلة " # ". ثم نكتب الأمر enable password ciscogitex و هو الأمر المستخدم لتمكين كلمة السر و التي اخترتها في هذه الحالة و هي ciscogitex (بالطبع يمكن تغييرها إلى أي شئ آخر).

و بذلك نكون قد قمنا بتمكين كلمة المرور ciscogitex على الموجه و التي سوف تمنع الانتقال من الحالة المستخدم إلى الحالة التالية بدون إدخال كلمة المرور التي قمنا بوضعها. و الشكل التالي يبين الخطوات السابقة قبل و بعد تمكين كلمة المرور، مع ملاحظة أننا استخدمنا الأمر exit للرجوع من وضع إلى وضع سابق إلى الوراء.

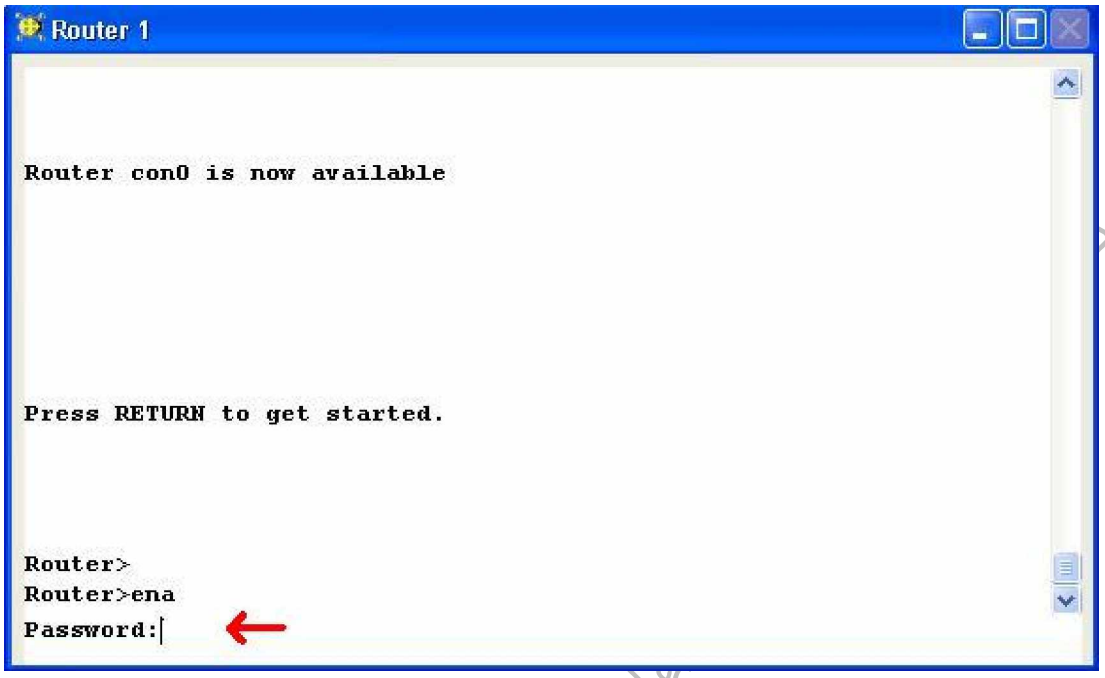
ما قبل تمكين كلمة المرور

نتبع الخطوات السابقة لتنفيذ العملية و التي ننفذها كما هو موجود بالصورة



ما بعد تمكين كلمة المرور

عند إعادة الدخول على الموجه سوف يطلب كلمة المرور كما هو مبين بالشكل



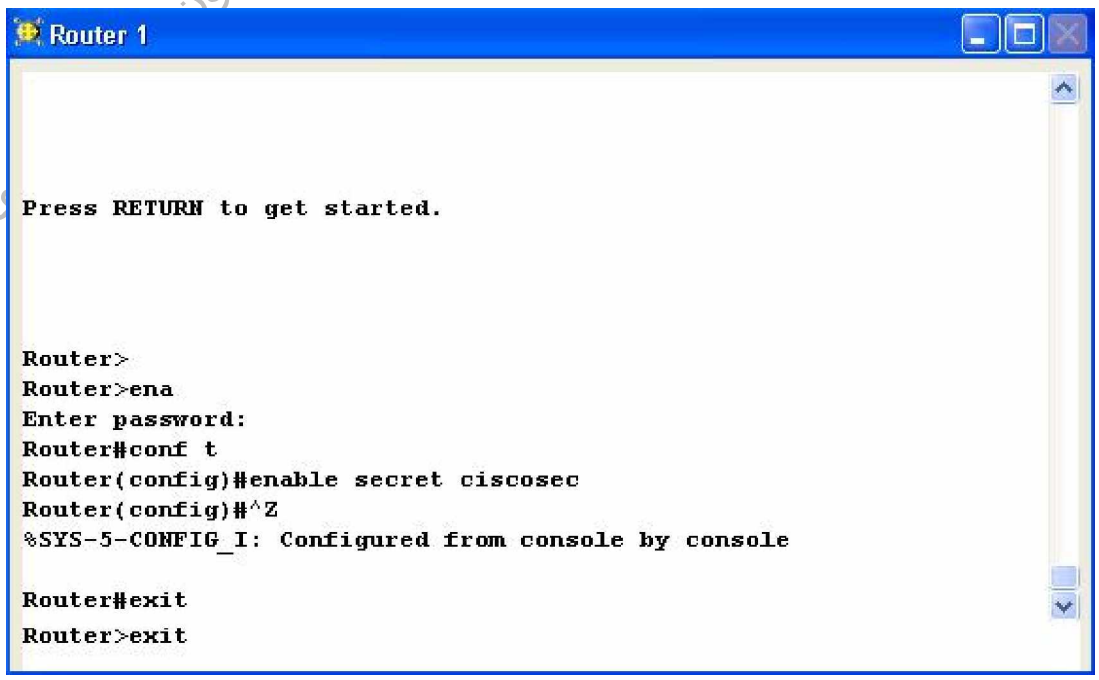
2) تمكين كلمة السر enable secret:

لتمكين كلمة السر سوف نستخدم نفس الخطوات السابقة مع اختلاف بسيط في أمر تمكين كلمة السر، و هو في هذه الحالة enable secret و الخطوات كالتالي:

Router> enable	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router (config)#enable secret ciscogitex	أمر إدخال كلمة السر

و للمزيد و المزيد من التوضيح أنظر إلى الرسم التالي لتوضيح الخطوات المستخدمة لتمكين كلمة السر و التي اخترناها هنا باسم ciscosecret.

خطوات تمكين كلمة السر



ما بعد تمكين كلمة السر

نلاحظ أن الموجه بعد تمكين كلمة السر و كلمة المرور سابقا، و بعد الخروج إلى حالة المستخدم و محاولة الدخول مرة أخرى، طلب الموجه إدخال كلمة السر للانتقال من حالة المستخدم إلى الحالة التالية باستخدام الأمر enable. في المرة الأولى قمت بإدخال كلمة المرور فرفضها، فقمت بإدخال كلمة السر فقَبِلَها و تمت عملية الدخول بنجاح إلى الحالة Privileged J

3) تمكين كلمة المرور لنقاط الدخول Access Points:

كما قلنا أن نقاط الدخول ثلاثة، و لذلك فسوف أبين كيفية تمكين كلمات المرور لكل طريقة على حدة:

- تأمين منفذ Console:

و يتم ذلك بتمكين كلمة المرور على الموجه لكي لا يقبل الدخول إلى حالة المستخدم User Mode إلا بعد إدخال كلمة المرور في حالة أن الاتصال كان عبر منفذ Console. و يتم تنفيذ هذه العملية من خلال الدخول إلى الخط نفسه و تثبيت كلمة المرور عليه كالتالي

Router>ena	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router(config)#line con 0	أمر اختيار نقطة الدخول المراد الدخول عليها
Router(config-line)#login	أمر الدخول إلى خط Console نفسه
Router(config-line)#password console	أمر إدخال كلمة المرور console
Router(config-line)# ^z	اختصار باستخدام زر ctrl و زر z للرجوع إلى المصدر
Router#	

هذه ... او تنشرها على الانترنت بدون اذن صاحبها

خطوات تمكين كلمة المرور للمنفذ Console العملية

```
Router 1

Press RETURN to get started.

Router>
Router>ena
Router#conf t
Router(config)#line con 0
Router(config-line)#password console
Router(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
Router>exit
```

ما بعد تمكين كلمة المرور

بعد الخروج تماما من الموجه و إعادة الدخول مرة أخرى عبر منفذ Console سوف يطلب الموجه كلمة السر التي تم إدخالها للخط مسبقا كما هو مبين بالشكل

```
Telnet 192.168.10.254

User Access Verification

Password: _
```

- تأمين منفذ AUX:

و يتم ذلك بتمكين كلمة المرور على الموجه لكي لا يقبل الدخول إلى حالة المستخدم User Mode إلا بعد إدخال كلمة المرور في حالة أن الاتصال كان عبر منفذ AUX. و يتم تنفيذ هذه العملية من خلال الدخول إلى الخط نفسه و تثبيت كلمة المرور عليه كالتالي

Router>ena	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router(config)#line aux 0	أمر اختيار نقطة الدخول المراد الدخول عليها
Router(config-line)#login	أمر الدخول إلى خط Console نفسه
Router(config-line)#password aux	أمر إدخال كلمة المرور aux
Router(config-line)#^z	اختصار باستخدام زر ctrl و زر z للرجوع إلى المصدر
Router#	

و خطوات تطبيق هذه الطريقة كما هي مبينة تنفذ عمليا بنفس الطريقة السابقة مع تغيير فقط اسم الخط و الذي سيكون في هذه الحالة aux0 بدلاً من con0 تعبيرا عن أننا نريد الدخول على الخط Aux. و عند الاتصال بالموجه عبر منفذ Aux فسوف يطلب الموجه كلمة المرور، و سنقوم بإدخال كلمة المرور التي قمنا بتثبيتها في الخطوات التالية.

- تشغيل اتصال telnet:

في هذه الحالة استخدمت لفظ تشغيل و ليس لفظ تمكين كلمة المرور و ذلك كما أشرنا سابقا أن هذه الطريقة لا تعمل إلا بعد تمكين كلمة المرور لها مسبقا. فلذلك قلت تشغيل. و خطوات تشغيلها كالتالي

Router>ena	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router(config)#line vty 0 4	أمر اختيار عدد خطوط الاتصال المراد تشغيلها
Router(config-line)#login	أمر الدخول إلى خط telnet نفسه
Router(config-line)#password telnet	أمر إدخال كلمة المرور telnet
Router(config-line)#^z	اختصار باستخدام زر ctrl و زر z للرجوع إلى المصدر
Router#	

ملحوظة: المقصود ب vty هو Virtual Terminal بمعنى خطوط اتصال وهمية أي ليست ملموسة مثل الحالتين السابقتين. كما أن عدد خطوط اتصال telnet الوهمية يمكن تزويدها أو تقليلها حسب الاحتياج، فالموجه يدعم ما يقرب من 38 خط لاستخدام هذه الطريقة، بل أن هناك بعض الأنواع التي تدعم 198 خط اتصال وهمي لا أدري لماذا و ما فائدة هذا العدد الضخم و لكنها موجودة على كل حال.

كما أنه يمكن وضع كلمة سر مستقلة لكل خط، بمعنى أنه بدلا من أن نكتب من الرقم كذا إلى الرقم كذا، فإننا نكتب فقط رقم اتصال واحد و نضع له كلمة مرور. و هكذا على باقي الخطوط. و في نفس الوقت عند تزويد الخطوط أو تقليلها فإننا نكتب من رقم كذا إلى رقم كذا حسب عدد الخطوط المطلوبة.

هذه النسخة أمانة فلا تغير رجعها أو تنشرها على الانترنت بدون إذن صاحبها

```
Router 1

Press RETURN to get started.



Router>
Router>ena
Router#conf t
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password telnet
Router(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
Router>
```

4) **تشفير كلمات المرور** Encrypt all passwords :

قلت سابقا أن تمكين كلمات المرور دائما ما يجعل هذه الكلمة ظاهرة عند استعراض خصائص الموجه، بمعنى أنها تظهر على هيئة Clear Text و يستطيع أي شخص يقف خلفك أن يقرأ هذه الكلمة بسهولة لأنها مكتوبة بحروف واضحة. و قد تمكنّا سابقا من تشفير كلمة الدخول للحالة Privileged باستخدام الأمر enable secret.

أما الآن فنحن بصدد تشفير جميع كلمات المرور التي قمنا بإدخالها سواء لنقاط الدخول أو للحالة Privileged أو حتى أي كلمة مرور يمكن إدخالها بعد ذلك في كل الأحوال التي تتيح لنا شيئين:

- إخفاء كلمات المرور مما يمنع الاطلاع عليها.
- إخفاء كلمات المرور الأخرى المتاحة على الموجه من ظهورها للشخص الذي سنُعيِّنُه مراقب و مدير للموجه، و نتيح له فقط فرصة استخدام كلمة المرور الخاصة به.

و يتم ذلك كالتالي:

Router>ena	أمر الدخول للحالة Privileged
Router#config t	أمر الدخول للحالة المتقدمة
Router(config)# service password-encryption	أمر تشفير كلمات المرور كلها

و بذلك نكون قد تعلمنا أمر جديد و هو service password-encryption و الذي يمكنا من استخدامه لتشفير جميع كلمات المرور المتاحة على الموجه (يمكنكم تجربته عمليا). و جدير بالذكر أن هذا الأمر متاح استخدامه فقط في الإصدارات الثلاث الأخير فقط من نظام التشغيل IOS ، و في حالة استخدامه على إصدار ما قبل ذلك فلن يتعرف عليه الموجه و سيعتبره أمر خاطئ.

هكذا إخوتي الأفاضل أكون قد انتهيت من كتابة الفصل الثاني من الجزء الأول في هذه الدورة، و استقبل استفساراتكم في أي وقت على بريد gitex@forislam.com. فمن لديه أي سؤال في الجزأين السابقين فلا يتردد في مراسلتي و سأحاول أن أرد على جميع الاستفسارات بأسهل طريقة ممكنة حتى يصل المعنى بشكل واضح بإذن الله. و نسألكم الدعاء بظهر الغيب J

هذا لا تغير فيها ولا تنشرها على الانترنت بدون إذن صاحبها