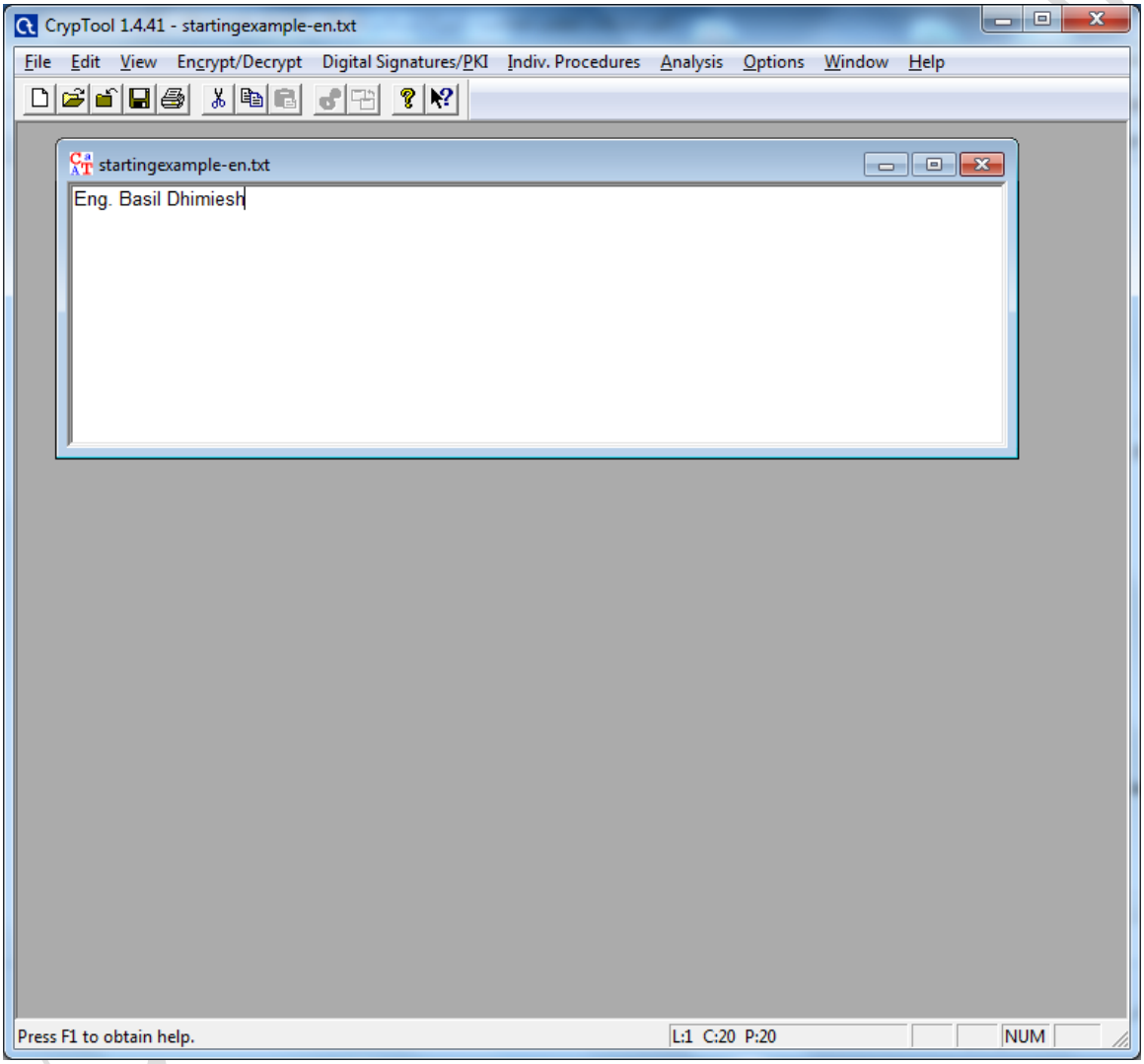
تطبيق خوارزمية RSA في برنامج Cryptool

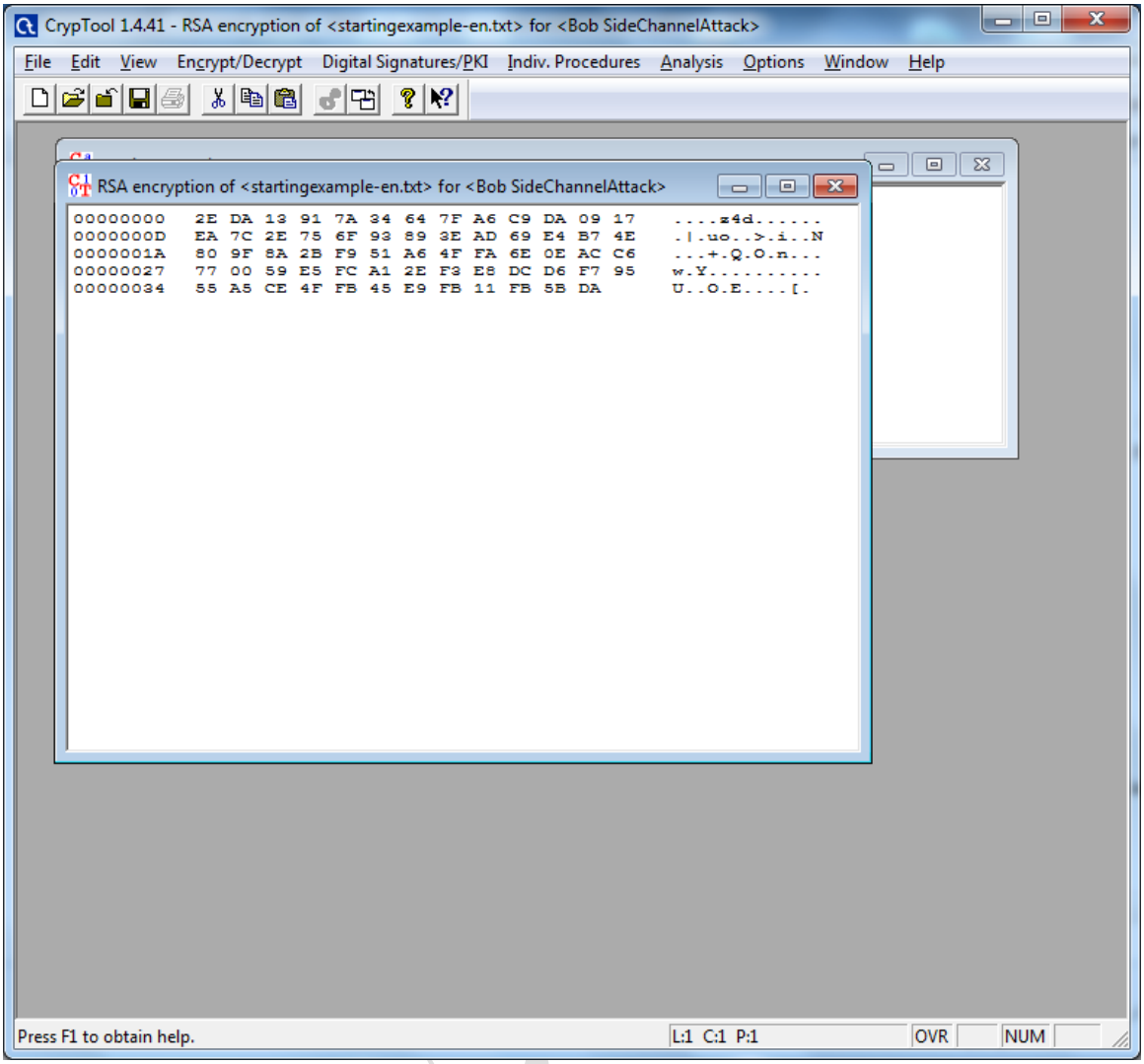
في هذا القسم سنطبق التشفير وفك التشفير في خوارزمية RSA

أولا: التشفير وفك التشفير في خوارزمية RSA اعتماداً على مفاتيح موجودة مسبقاً في برنامج cryptool

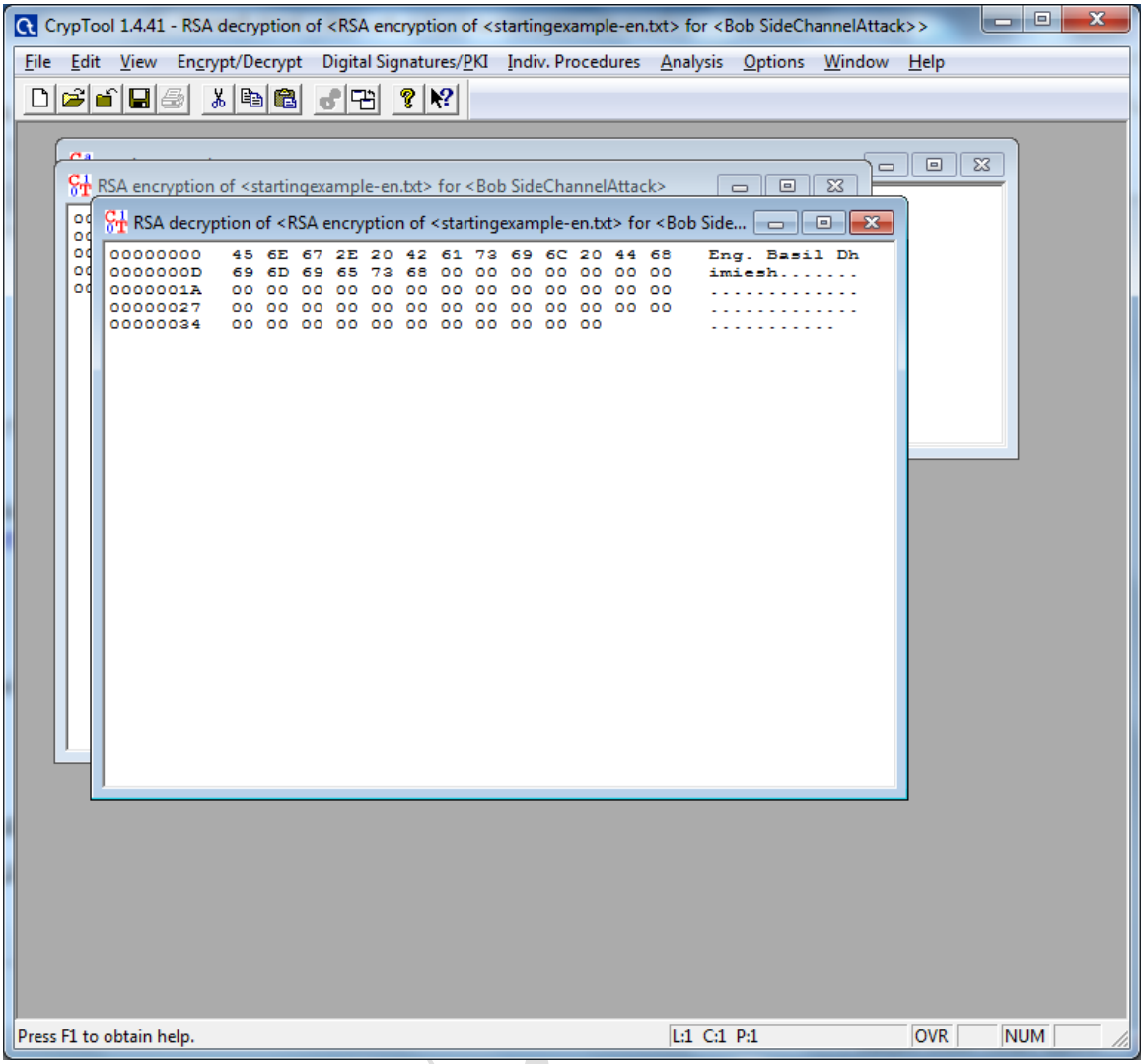
في مساحة العمل نكتب النص الصريح المراد تشفيره أو نقوم باختيار ملف مخزن مسبقاً من قائمة File ثم نفتحه بواسطة Open



للتشفير تختار قائمة Encrypt/Decrypt ثم Asymmetric. ثم RSA Encryption. نختار المفتاح العام والخاص لخوارزمية RSA-512 الموجود مسبقاً في برنامج Cryptool باسم Sidechannel Attack ثم نضغط على زر Encrypt فيظهر النص المشفر التالي:



يمكن أن تتم عملية فك التشفير بواسطة القائمة Encrypt/Decrypt ثم Asymmetric ثم RSA Decryption ثم اختيار المفتاح الخاص Sidechannel Attack مع رمز pin code إن وجد.

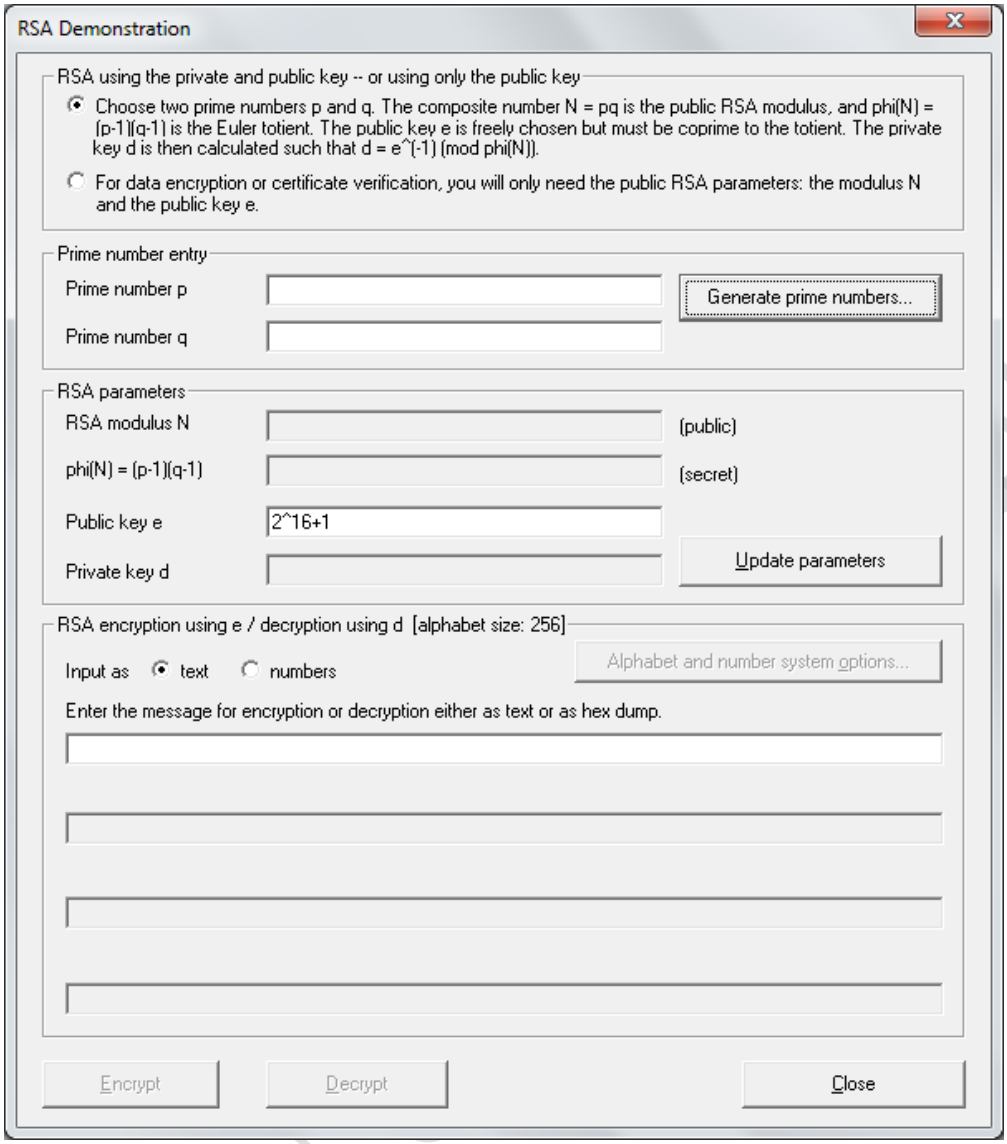


ثانيا: التشفير وفك التشفير في خوارزمية RSA اعتماداً على مفاتيح يقوم المستخدم بإنشائها:

هذه الفقرة تتكون من ثلاثة أجزاء هي:

- توليد مفاتيح خوارزمية RSA Key
- تشفير وفك تشفير الرسائل
- تجريب تحليل العدد N لمعرفة العديدين p و q وكسر الخوارزمية.

لتوليد المفاتيح نختار تبويبة Encrypt/Decrypt ثم Asymmetric ثم RSA Demonstration فتظهر النافذة التالية:



يجب ادخال عددين أولين p و q في الحقول المخصصة، أو يمكن توليد العددين الأوليين عشوائياً. فيتم حساب قيم N و $\varphi(n)$

يتم بعدها اختيار قيمة العدد e الممثل للمفتاح العام، وينصح برنامج cryptool بأن يكون العدد دائما هو القيمة 2^16+1= 65537 بغض النظر عن الشروط السابقة لاختياره.

تقبل الخوارزمية تشفير الأعداد فقط، وبالتالي يمكن تحويل أي نص إلى عدد بشيفرة Ascii مثلاً.

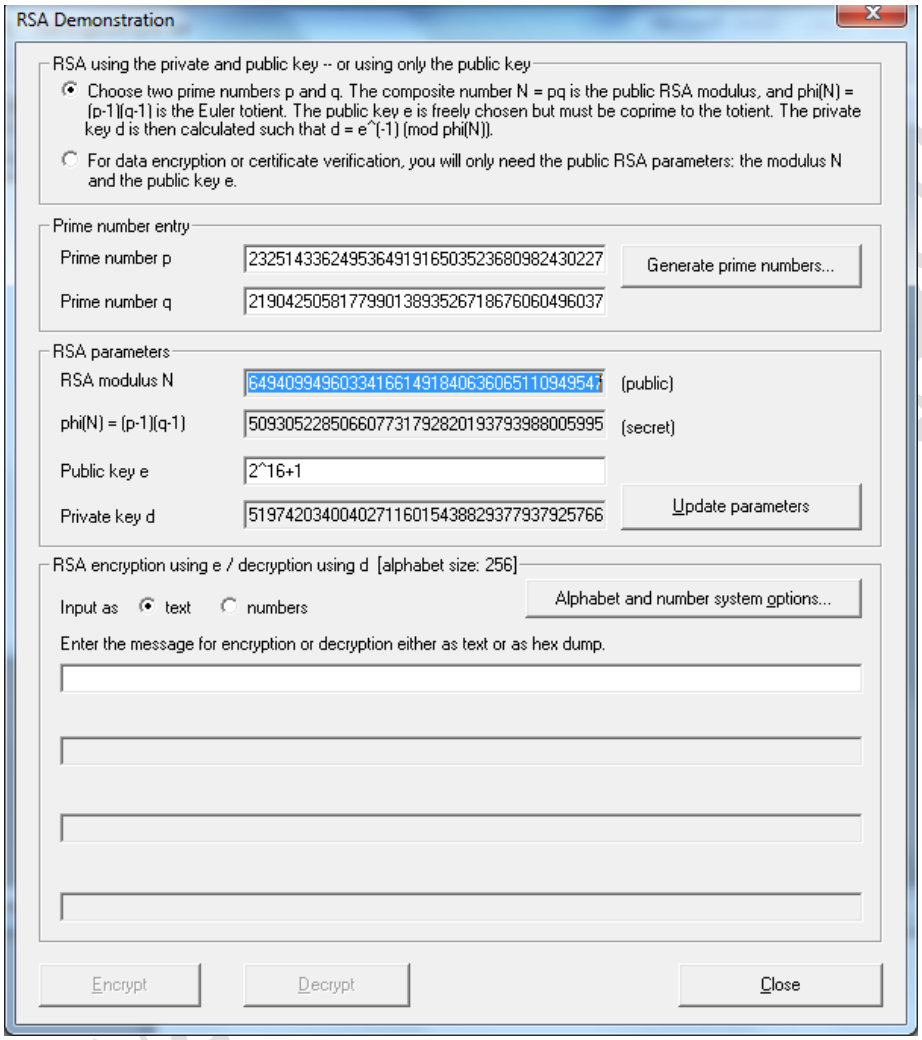
قم بتشفير نص ما ثم قم بفك تشفيره

لتحليل العدد N إلى p و q سنتبع ما يلي

قم بتوليد عدد p و q من رتب صغيرة مثلا 2^27 ثم اوجد N وانسخه. ثم اذهب إلى تبويبة Indiv.Procedures ثم RSA Cryptosystem ثم اختر Factorization of Numbers ثم الصق N

واضغط continue لمشاهدة عملية كسر الخوارزمية وتحليل N إلى عوامله الأولية p و q طالما أن p و q صغيرين.

أعد توليد العددين p و q من رتب كبيرة مثلا 2^512 وأعد عملية التحليل للعدد N الكبير.



هذا هو مثال لعدد N من رتب كبيرة بطول 1024 بت

5093052285066077317928201937939880059950622640193040093804427268969
7265978564324718758961776767234544059437297915425235542203159269032
1159671604085749312719014571724333258213373486792243132324840915726
1065935218600821329985693113103102838689158609414968655406850470266
8464940994960334166149184063606511094954 7

نلاحظ أنه يتعذر حسابياً تحليله والعودة منه إلى العددين p و q.

برنامج CrypTool 1.4.40

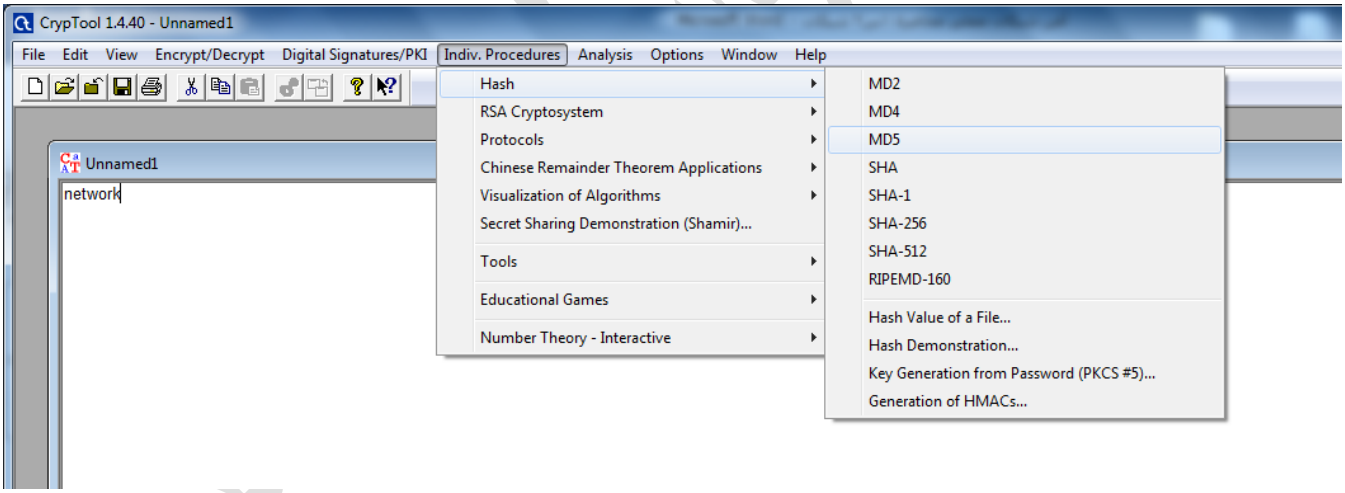
في هذه الجلسة سنطبق خوارزميات الاختزال، ثم سنرى كيفية الاستفادة منها في التواقيع الرقمية. أيضاً سنقوم بتطبيق التشفير المختلط.

أولاً: استخدام خوارزميات الاختزال (Hash Functions)

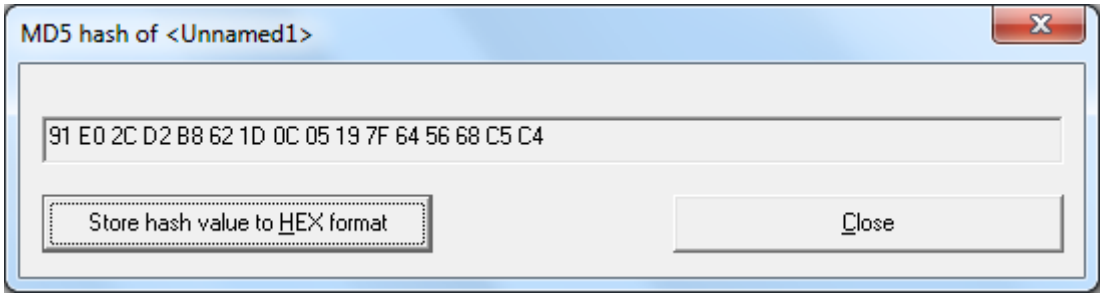
هي خوارزميات باتجاه واحد، أي لا يمكن العودة من النص المشفر إلى النص الأصلي. تستخدم للتأكد من أن محتوى الرسالة موثوق ولم يتم التعديل عليه، وذلك بمقارنة البصمة المرسلة بالرسالة مع البصمة التي ولدها المستقبل من نص الرسالة بنفس الخوارزمية. من أهم أنواع خوارزميات الاختزال:

1. سلسلة خوارزميات MD وهي: MD2، MD4، MD5 وهذه الخوارزميات ذات طول خرج ثابت هو 128بت.
2. سلسلة خوارزميات sha وهي: sha، sha-1، sha-256، sha-512 وهذه الخوارزميات ذات طول خرج ثابت هو 160بت.

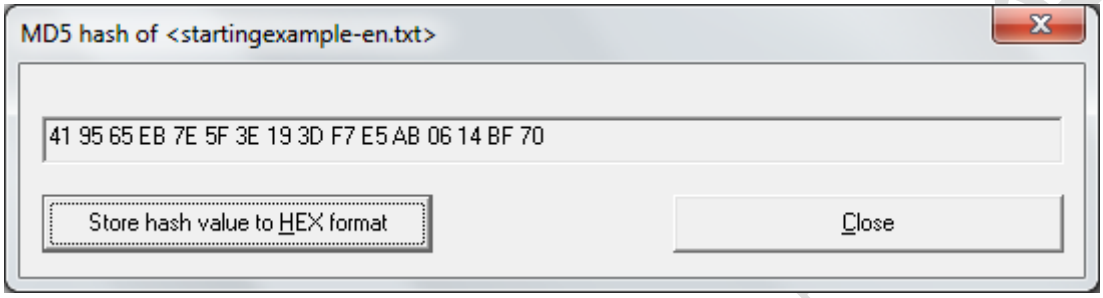
فيما يلي خطوات تشفير نص (في مثالنا هو كلمة network) باستخدام خوارزمية MD5:



فيكون الخرج الناتج هو:



عند تعديل نص الرسالة (مثلاً بإضافة نقطة بعد كلمة network) لتصبح .Network نلاحظ تغير النص المشفر كلياً، كما في الشكل التالي:

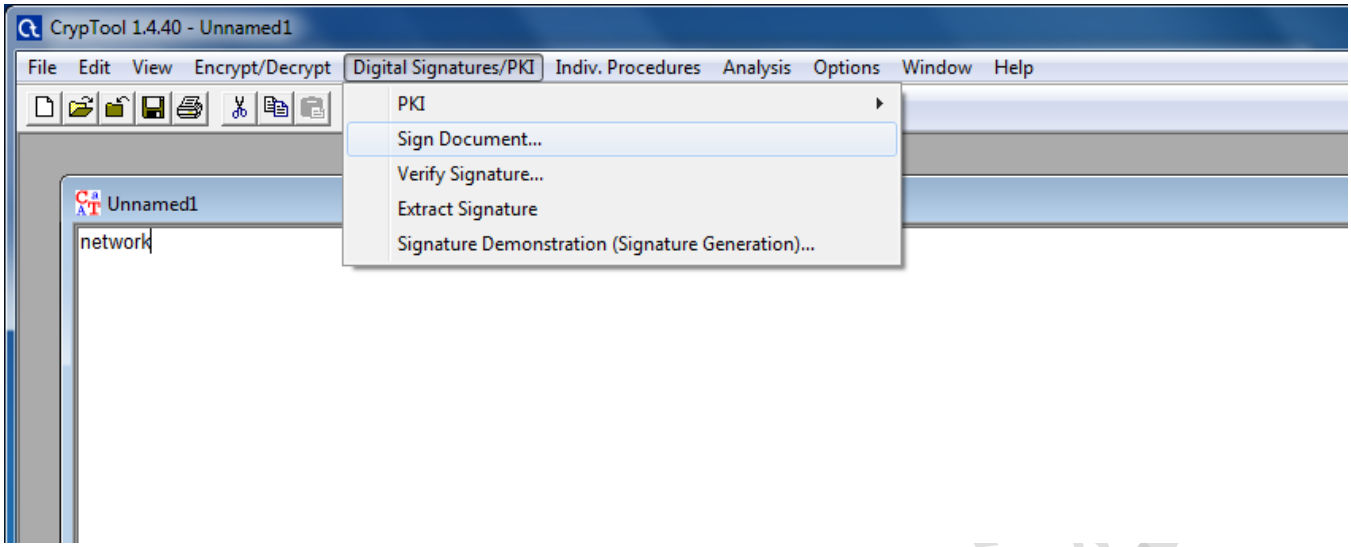


أي أن لكل رسالة بصمة تميزُها عن غيرها

ثانياً: التواقيع الرقمية (Digital Signatures):

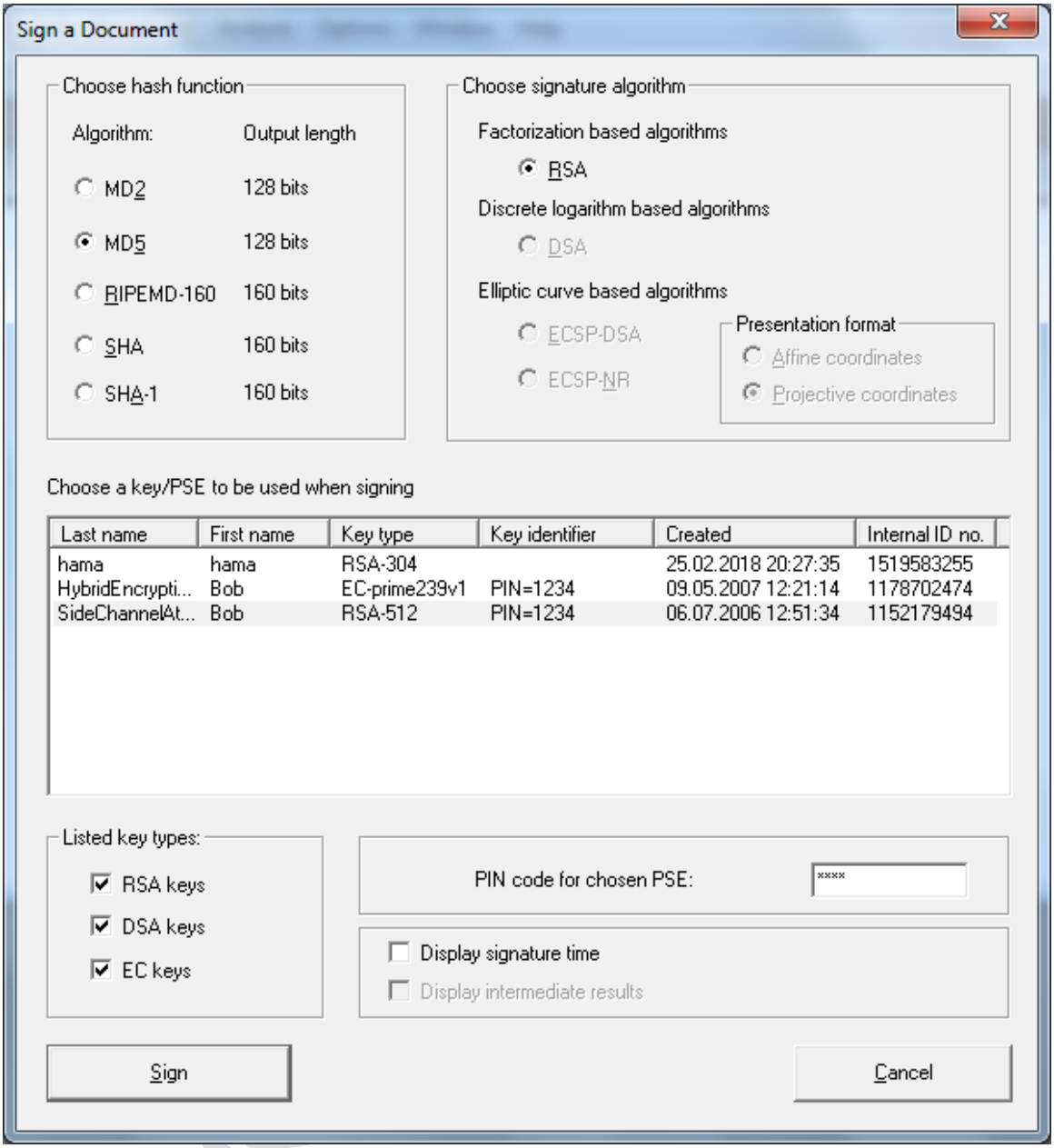
يستخدم التوقيع الرقمي لإثبات هوية المرسل أو الكاتب للملف، وهذه التواقيع من الممكن إضافتها على رسائل مشفره أو بدون تشفير. وطريقه عمله أن يقوم المرسل بحساب الـ (MD5) لرسالته وتشفيره بواسطة المفتاح الخاص به (private key) – فباستخدام خوارزمية RSA نستطيع توليد مفتاحين عام وخاص كل منهما بإمكانه فك تشفير ما شفره المفتاح الآخر – وإرسالها بالإضافة للرسالة إلى المستقبل. عند وصول الرسالة للمستقبل، يقوم بفك التشفير بواسطة المفتاح العام (public key) وحساب الـ(MD5) للرسالة ومقارنتها بـ (MD5) المرسلة، فإذا تشابهت فيعني أن الرسالة سليمة من التعديل أولا وباستخدامه للمفتاح العام يضمن هوية المرسل ثانياً.

لإضافة توقيع (Sign) إلى الملف النصي السابق نطبق الخطوات التالية: من تبويبة Digital Signatures/PKI نختار Sign Document



ثم نختار من النافذة المفتوحة نوع دالة الاختزال المطبقة والمفتاح الخاص من خوارزمية RSA-512[1] الذي سيتم تشفير خرج دالة الاختزال به ثم ندخل PIN Code=1234 كما في الشكل التالي ثم نضغط على زر التوقيع Sign.

[1] المفتاح العام والخاص لخوارزمية RSA-512 موجود مسبقاً في برنامج Cryptool

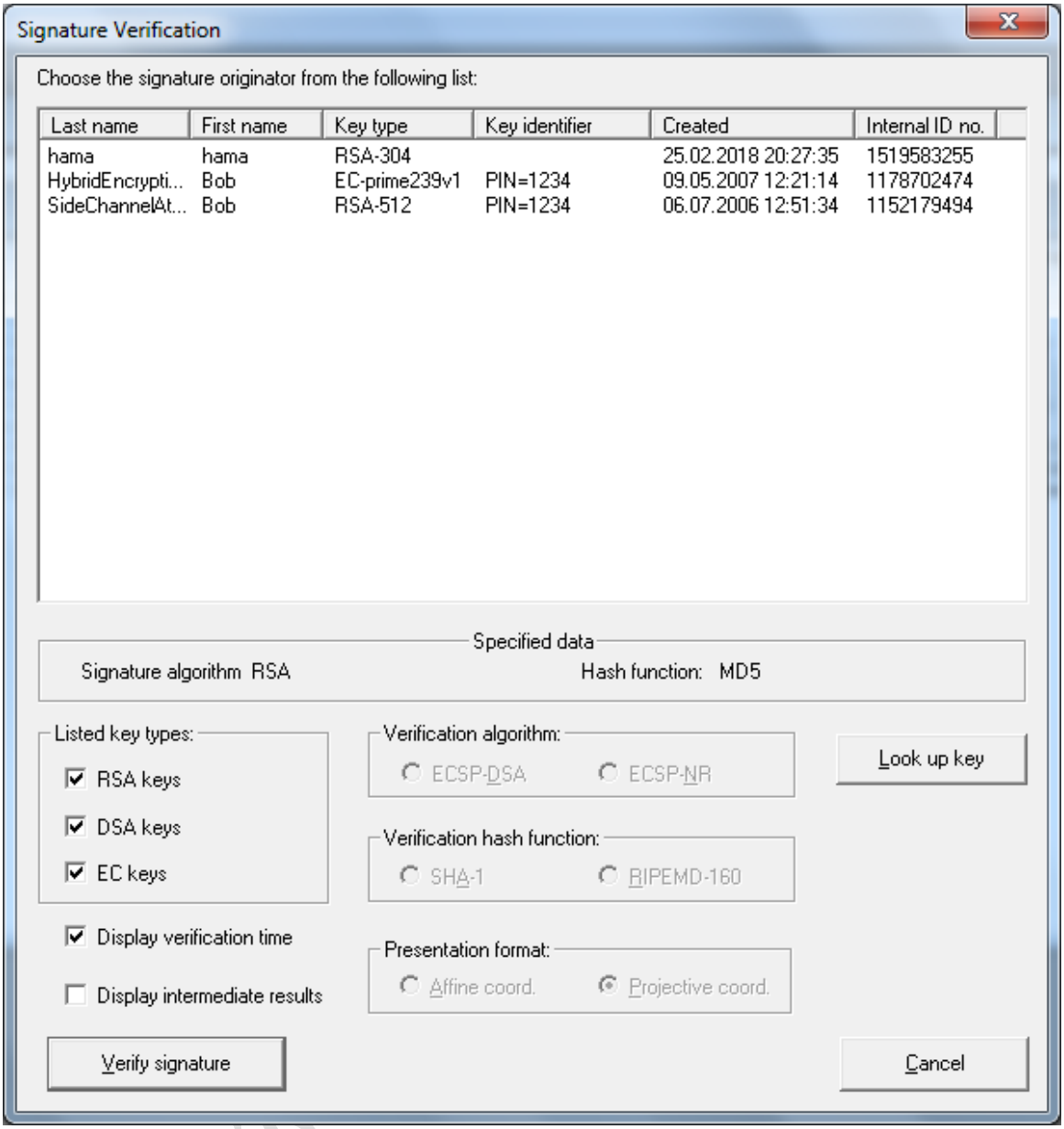


في الشكل التالي يوجد في القسم اليميني: النص الصريح والتوقيع ونوع خوارزمية التشفير المستخدمة واسم خوارزمية توليد المفتاح العام والخاص، بينما يوجد في القسم اليساري: محتويات القسم اليميني بالترميز الست عشري.

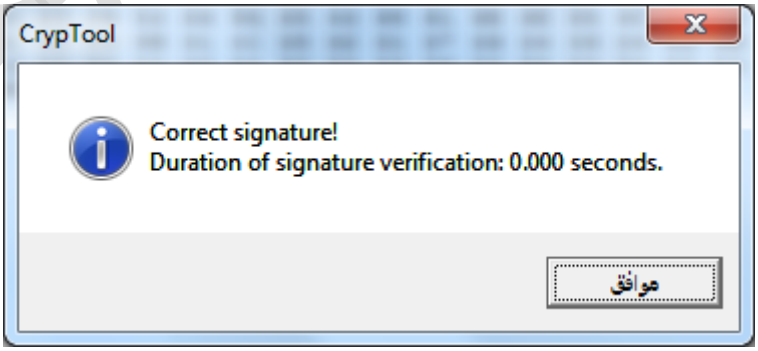
RSA (MD5) signature of <startingexample-en.txt>

```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 E2 70   Signature:        .p
00000013   05 25 2C E5 3F 7A E9 27 C4 CD 51 5B 6B 24 FE 20 6B FC 9B   .%,.?z.'..Q[k$. k..
00000026   47 0F 61 7F AD 25 C7 3F 3C 7F F4 44 5B 31 FE 20 35 D8 FF   G.a..%.?<..D[1. 5..
00000039   6E 8B 3C 26 C6 D9 05 DA 89 BD 29 AA A6 FE 83 89 34 D6 5E   n.<&......).....4.^
0000004C   A0 12 E0 E7 A7 20 20 20 20 20 20 20 20 20 20 20 20 20 20   .....
0000005F   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53                     S
00000072   69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20 35   ignature length:  5
00000085   31 32 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   12
00000098   20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72 69 74               Algorit
000000AB   68 6D 3A 20 20 20 20 20 20 52 53 41 20 20 20 20 20 20 20   hm:       RSA
000000BE   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000D1   20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20      Hash function:
000000E4   20 4D 44 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20    MD5
000000F7   20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20                  Key:
0000010A   20 20 20 20 20 5B 53 69 64 65 43 68 61 6E 6E 65 6C 41 74        [SideChannelAt
0000011D   74 61 63 6B 5D 5B 42 6F 62 5D 5B 52 53 41 2D 35 31 32 5D   tack][Bob][RSA-512]
00000130   5B 31 31 35 32 31 37 39 34 39 34 5D 5B 50 49 4E 3D 31 32   [1152179494][PIN=12
00000143   33 34 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   34]
00000156   20 20 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20            Message:
00000169   20 20 20 20 6E 65 74 77 6F 72 6B                              network
```

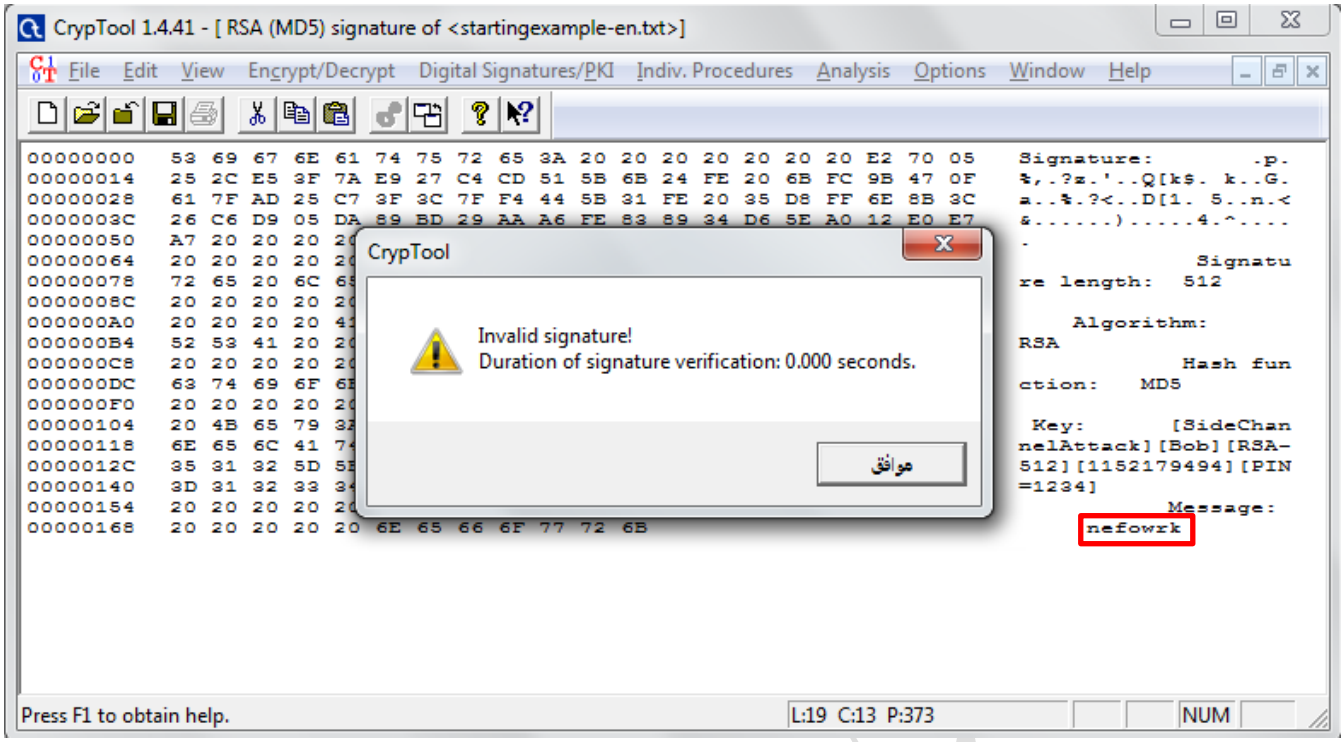
للتأكد من صحة التوقيع والرسالة المستلمة نتبع الخطوات التالية: من تبويبة Digital Signature/PKI نختار Verify Signature ثم نختار المفتاح العام من خوارزمية RSA-512 ثم نضغط Verify Signature.



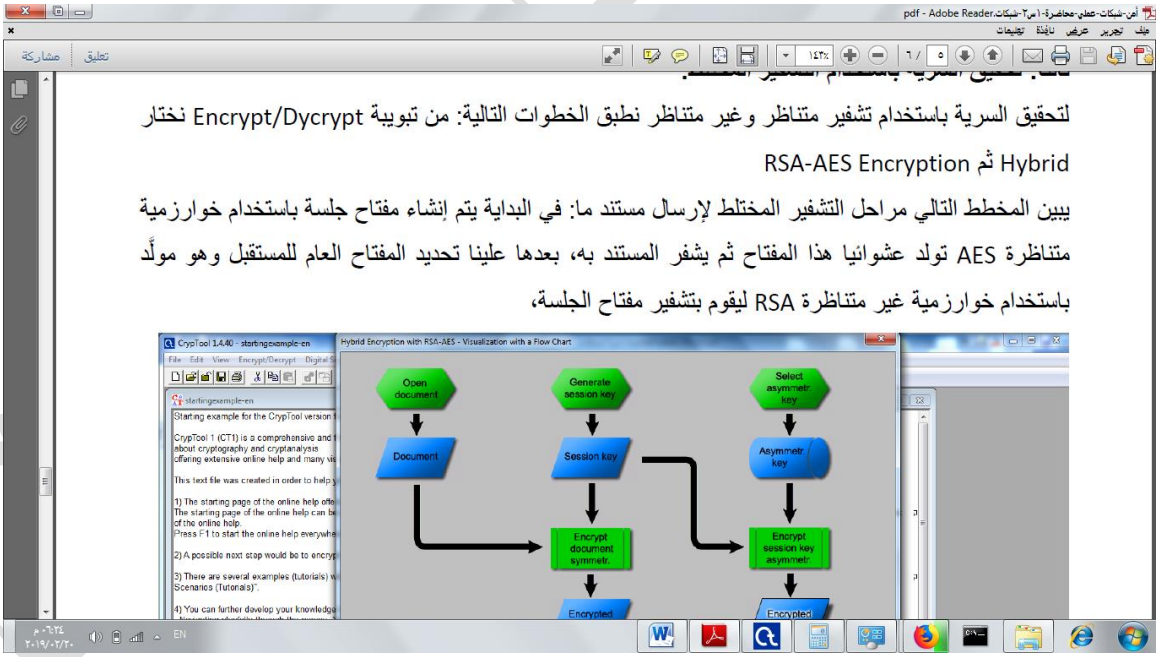
إذا كانت الأمور على ما يرام فستنجح عملية التحقق من التوقيع Signature Correct كما في الشكل التالي:



عند تعديل أي محرف في الرسالة (مثلاً بتغيير كلمة network) لتصبح nefowrk فالتحقق من التوقيع سيكون غير صالح Invalid Signature كما في الشكل التالي:

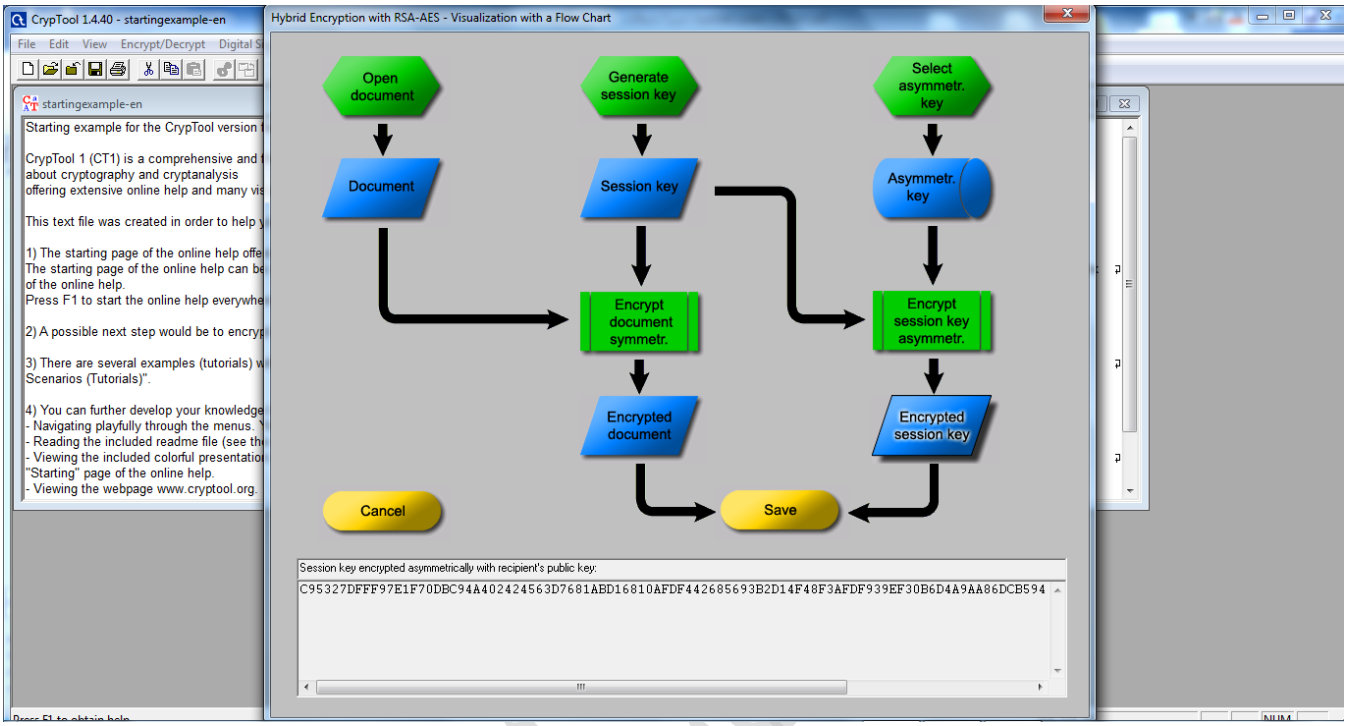


ثالثا: تحقيق السرية باستخدام التشفير المختلط:

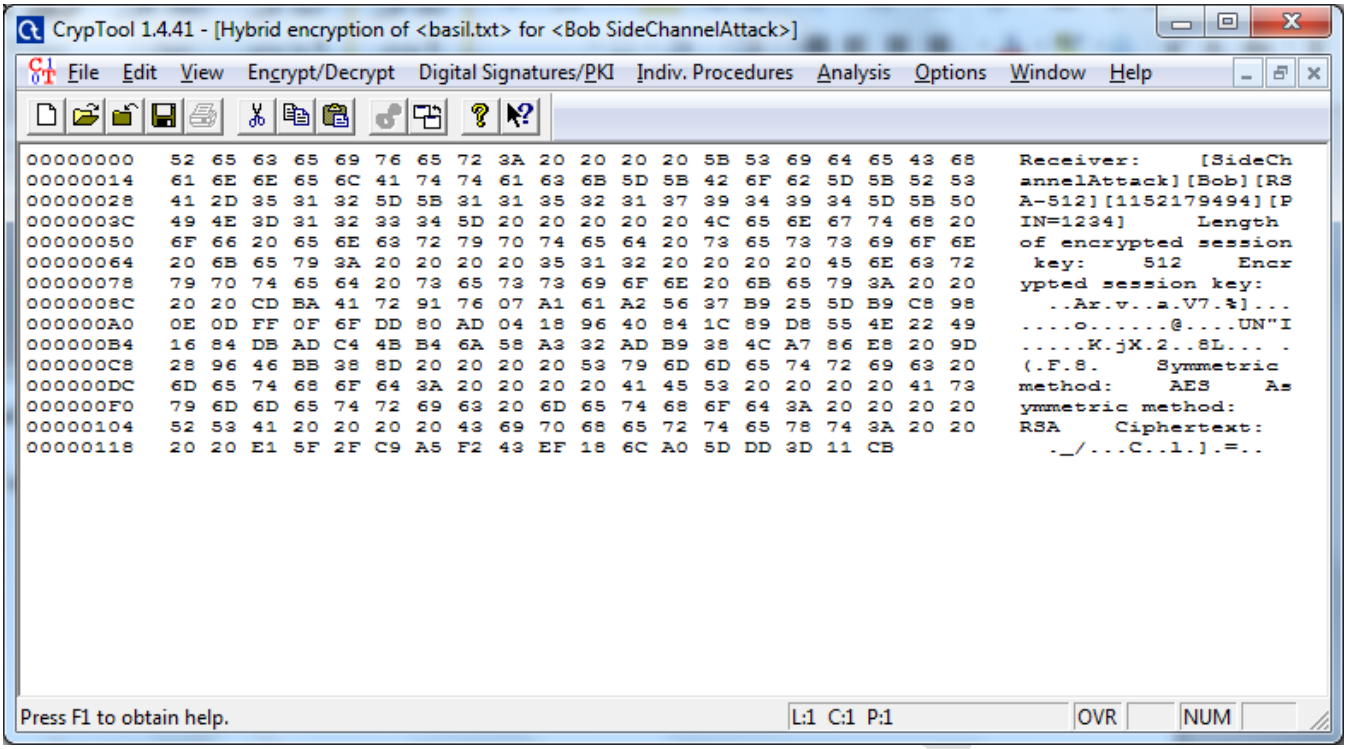


لتحقيق السرية باستخدام تشفير متناظر وغير متناظر نطبق الخطوات التالية: من تبويبة Encrypt/Decrypt نختار Hybrid ثم RSA-AES Encryption.

يبين المخطط التالي مراحل التشفير المختلط لإرسال مستند ما: في البداية يتم انشاء مفتاح جلسة باستخدام خوارزمية متناظرة AES تولد عشوائيا هذا المفتاح ثم يشفر المستند به، بعدها علينا تحديد المفتاح العام للمستقبل المولد مسبقاً باستخدام خوارزمية RSA غير المتناظرة ليقوم بتشفير مفتاح الجلسة.



في الشكل التالي يوجد في القسم اليميني: معلومات عن المفتاح العام الذي تم تشفير مفتاح الجلسة به بالإضافة إلى مفتاح الجلسة المشفر بالإضافة إلى النص المشفر، بينما يوجد في القسم اليساري: محتويات القسم اليميني بالترميز الست عشري.



في طرف المستقبل يتم فك تشفير مفتاح الجلسة باستخدام المفتاح الخاص. ثم فك تشفير المستند بواسطة مفتاح الجلسة.

تدريب: قم بفك التشفير المختلط النتائج من المثال السابق بواسطة تبوبية Encrypt/Decrypt ثم Hybrid ثم RSA-AES Decryption

التعامل مع بعض التجهيزات الشبكة وتأمينها

1.12- مقدمة (Introduction):

جهاز الموجه (Router) هو عبارة عن جهاز الكتروني مؤلف من الدارات الالكترونية التي تجعله يقوم بعدة وظائف من أهمها توجيه (Routing) رزم البيانات من شبكة لأخرى. تتألف هذه الدارات من منافذ (Ports) -تسمى أيضاً واجهات اتصال (Interfaces)- وتستخدم إما لتوصيل الشبكات مع بعضها البعض لتبادل البيانات فيما بينها أو للتحكم بإعدادات الموجه. كما ويحوي الموجه على وحدة معالجة مركزية (Central Processing Unit: CPU)، وذواكر (Memories)، ونواقل (Buses) للنظام لوصل الدارات الداخلية مع بعضها، ووحدة تغذية كهربائية (Power Supply Unit) لتمده بالجهود الكهربائية المطلوبة، ومراوح (Fans) للتبريد، وشقوق توسع (Expansion Slots) لإضافة منافذ إضافية عند الحاجة. يبين الشكل (1.12) موجه من صنع شركة سيسكو الشهيرة موديل 1800.

الشكل (1.12): موجه سيسكو موديل 1800.

2.12- المكونات الرئيسية للموجه (Main Components for Router):

سنسلط الضوء في الفقرات التالية على أهم أقسام الموجه التي سنحتاجها للتعامل معه وإعداده. لا تختلف كثيراً مكونات وإعدادات موجهات سيسكو الرئيسية عن مكونات وإعدادات مبدلاتها، فكل ما سنذكره في هذا الفصل ينطبق على المبدلات أيضاً ما لم نشر لخلاف ذلك.

1.2.12- الذواكر (Memories):

ذاكرة الوصول العشوائي (Random Access Memory: RAM):

وتسمى أيضاً بذاكرة العمل (Working Memory)، وتحوي الإعدادات الحالية التي يعمل بها الموجه مثل جداول التوجيه (Routing Tables) وجداول ARP (ARP Tables) ولكنها تفقد محتوياتها عند انقطاع التيار الكهربائي أو عند إعادة الإقلاع وبالتالي هي ذاكرة مؤقتة تحمل الإعدادات التي تم إدخالها للموجه ويتم حفظ هذه الإعدادات في ملف يدعى ملف الإعدادات الحالية (Running Configuration File).

ذاكرة الوصول العشوائي غير المتطايرة (Non-volatile Random Access Memory: NVRAM):

وهي ذاكرة ثابتة وفيها يتم حفظ ملف يدعى ملف إعدادات الإقلاع (Startup Configuration File) وهذا الملف لا يتواجد إلا بعد إعداد الموجه. نستطيع بواسطة هذه الذاكرة حفظ الإعدادات المخزنة بالذاكرة RAM بشكل دائم وذلك قبل إغلاق أو إعادة تشغل الموجه، لأن هذا النوع من الذواكر يحفظ المعلومات حتى بحالة انقطاع التغذية الكهربائية.

الذاكرة الوميضية (Flash Memory):

تشبه هذه الذاكرة في عملها القرص الصلب في الحاسوب العادي. تقوم هذه الذاكرة بتخزين نظام تشغيل الموجه والذي يسمى بنظام تشغيل الشبكة البيني (Internetwork Operating System: IOS) وهو عبارة عن ملف بصيغة (*.Bin) ويحوي مجموعة الأوامر التي سنستخدمها لعمل إعدادات الموجه ومن الممكن أن تحتوي هذه الذاكرة على أكثر من ملف نظام تشغيل ويتم باستخدام أوامر معينة تحديد الملف الذي سيقلع منه الموجه.

ذاكرة القراءة فقط (Read Only Memory: ROM):

يوجد بهذه الذاكرة برنامج الإختبار الذاتي (Power On Self Test: Post) والذي يعمل بمجرد تشغيل الموجه بفحص المكونات المادية له. كما أن هذه الذاكرة تحوي على جزء من نظام التشغيل IOS الذي سيكون بمثابة نظام بديل بحالة حدوث مشكلة بالنظام الموجود بالذاكرة Flash، ولكن يستخدم هذا النظام فقط للدخول للموجه وعلاج المشكلة وليس للعمل بشكل دائم.

وتحوي ROMMON على نظام تشغيل فرعي بإمكانيات محدودة يستخدم بعدة حالات فعند تلف النظام IOS الأساسي، سيستخدم ROMMON لإعادة تنصيب IOS جديد.

تحوي هذه الذاكرة أيضاً على شيفرة الإقلاع (Bootstrap Code) التي تحدد موقع نظام التشغيل الذي سيقوم الموجه بتحميله.

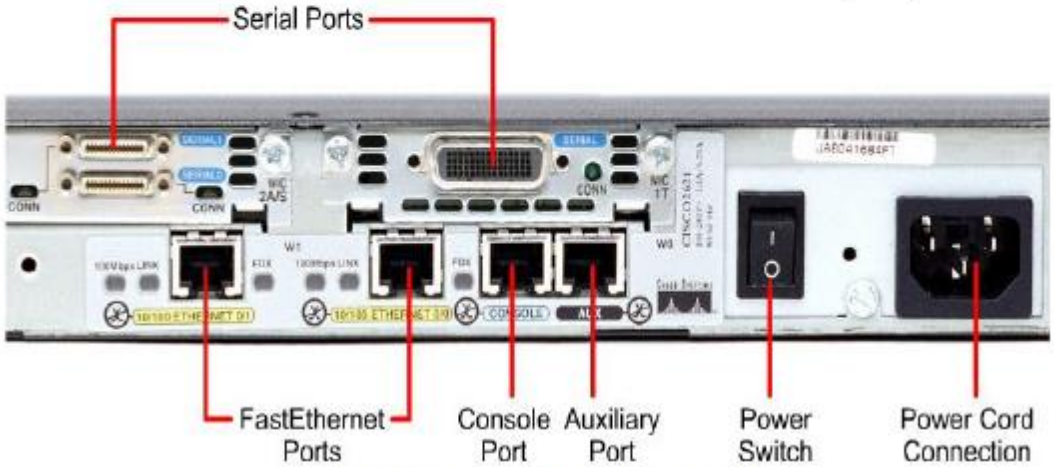
2.2.12- المنافذ (Interfaces):

يحوي الموجه في خلفيته على مجموعة من منافذ التحكم، وأخرى لمنافذ التوصيل. بعض منافذ التوصيل خاص للاتصال مع شبكات LAN وبعضها الآخر خاص للاتصال مع شبكات WAN. عادة تسمى المنافذ بأسماء أنواعها، فمثلاً يسمى المنفذ التسلسلي بـ (Serial)، وهكذا.. أما في حال وجود أكثر من منفذ نفس النوع فإنها تتميز عن بعضها بترقيمها، ويكون الترقيم بشكل عام كالتالي:

X/Y: حيث يدل الحرف X على رقم الشق (Slot) –ويسمى أيضاً بالصف (Raw)–، والحرف Y يدل على رقم المنفذ (Port) حسب ترتيبه.

ملاحظة: في حالة وجود شق واحد فقط فإما أن يستغنى عن ذكر رقم الشق ويكتفى بذكر رقم المنفذ، أو أن يعتبر رقم الشق بهذه الحالة هو " 0". يعتمد اختيار أي الحالتين على حسب دعم واعتماد نظام التشغيل لها.

يبين الشكل (4.12) منافذ الموجه وتسمياتها.



الشكل (4.12): أشكال و أسماء منافذ الموجه.

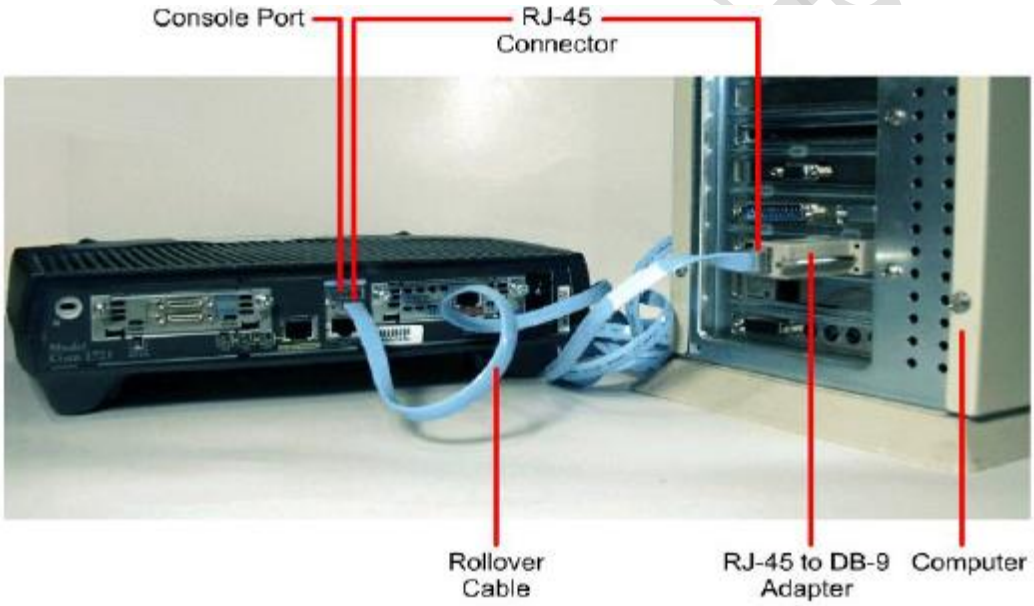
1.2.2.12- منافذ التحكم (Control Ports):

وهي عدة أنواع:

1- Consol Port: ويكون عادة رقمه " 0" وهو من النوع RJ-45 ويستخدم لتوصيل جهاز الحاسوب مع الموجه للتحكم بالموجه وإعداده بواسطة ذلك الحاسوب. الكبل المستخدم بعملية التوصيل من النوع Roll-Over، الطرف الأول يستخدم محول (من منفذ RJ-45 إلى منفذ Serial) ويوصل المحول على المنفذ التسلسلي لجهاز الحاسوب ويكون من النوع (D-9 Pins) أو من نوع (D-25 Pins) أما الطرف الثاني للكبل فيوصل على منفذ Console للموجه.

هذا المنفذ موجود في جميع فئات الموجه حتى يوفر طريقة للاتصال به اتصالاً مباشراً وهذا المنفذ هو الأكثر استخداماً بين طرق اتصال المستخدمين بالموجهات.

يبين الشكل (5.12) طريقة توصيل الموجه بالحاسوب عبر منفذ Console.

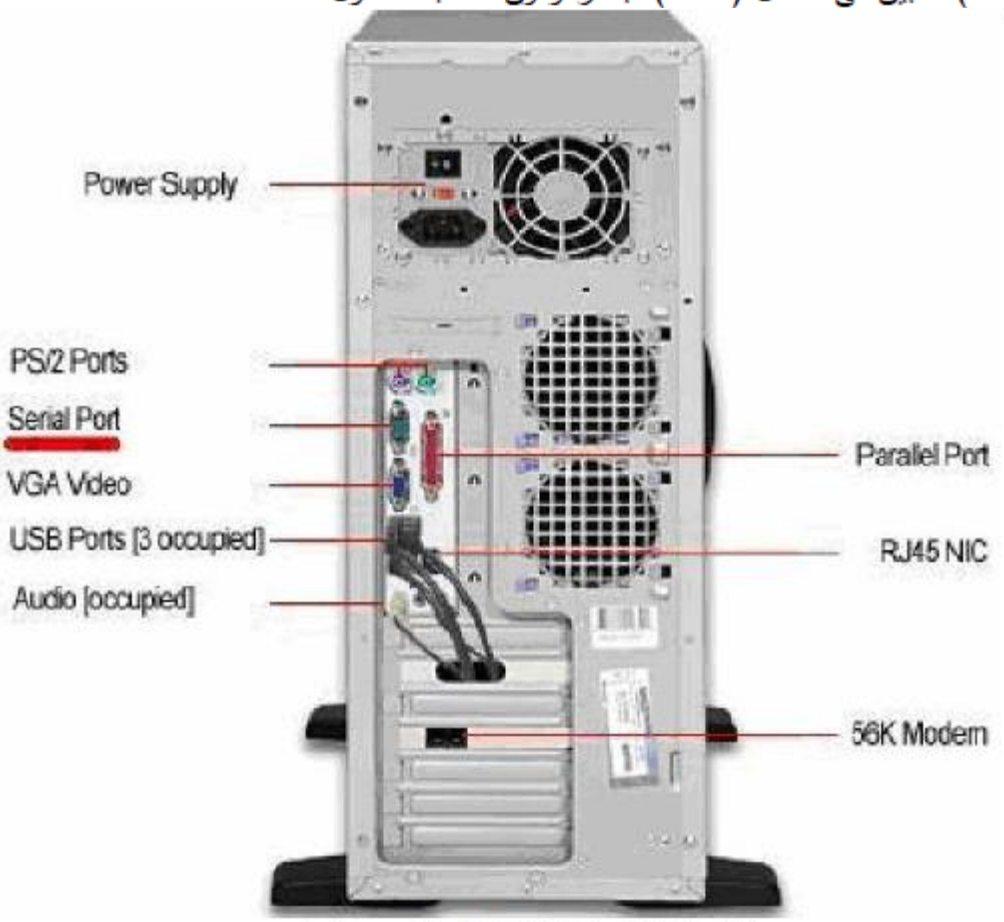


الشكل (5.12): طريقة توصيل الموجه بالحاسوب عبر منفذ Console.

كما يبين الشكل (6.12) الكابل Roll-Over المستخدم لتوصيل الموجه بالحاسوب عبر منفذ Console.

الشكل (6.12): كابل توصيل الموجه عبر منفذ Console.

يستخدم هذا الكابل لتحقيق الاتصال بين الحاسوب والموجه حيث يوصل طرفه الأيمن الموضح في الشكل (6.12) مع الحاسوب عن طريق المنفذ التسلسلي للحاسوب (Serial Port) المبين في الشكل (7.12) مباشرة ودون الحاجة لمحول:

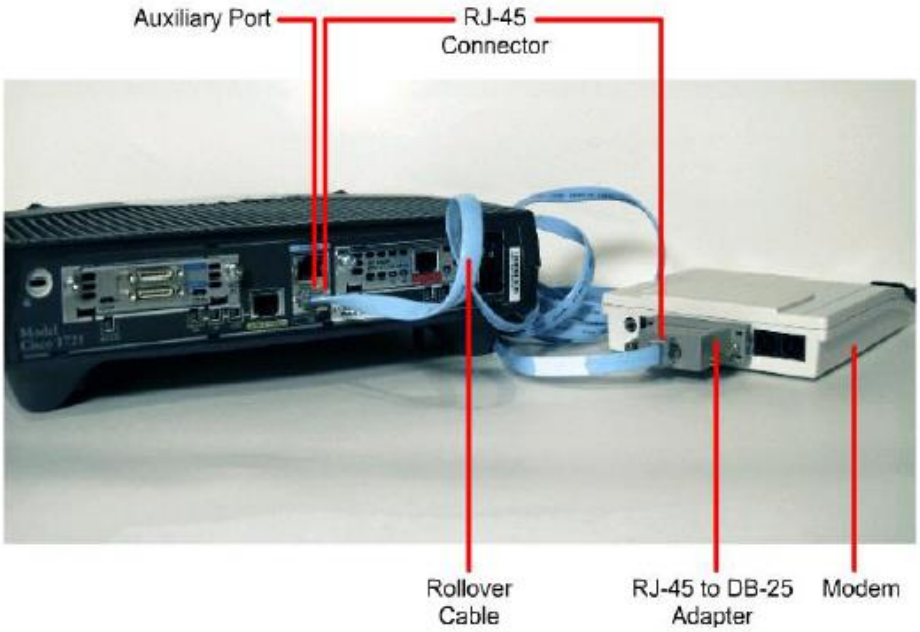


الشكل (7.12): المنفذ التسلسلي الموجود بالحاسوب.

بينما الطرف الأيسر وهو من نوع (RJ-45) فيوصل مع الموجه عن طريق المنفذ Consol كما في الشكل (8.12):

الشكل (8.12): منفذ Consol.

2- المنفذ المساعد (Auxiliary Port): ويكون عادة رقمه " 0" وهو من النوع RJ-45 ويستخدم للتحكم بالموجه عن بعد عبر خط الهاتف حيث يتم توصيل كبل من نوع Roll-Over ، طرفه الأول على منفذ AUX والطرف الأخر على مودم خارجي (External Modem). يوصل المودم إلى خط الهاتف ثم يقوم مدير الشبكة من مكان ما بوصل حاسوب عبر المودم إلى خط الهاتف. تتم عملية الدخول ضمن برنامج سنتعرف عليه لاحقاً، يبين الشكل (9.12) طريقة الوصل هذه.



الشكل (9.12): طريقة توصيل الموجه بالمودم عبر منفذ AUX.

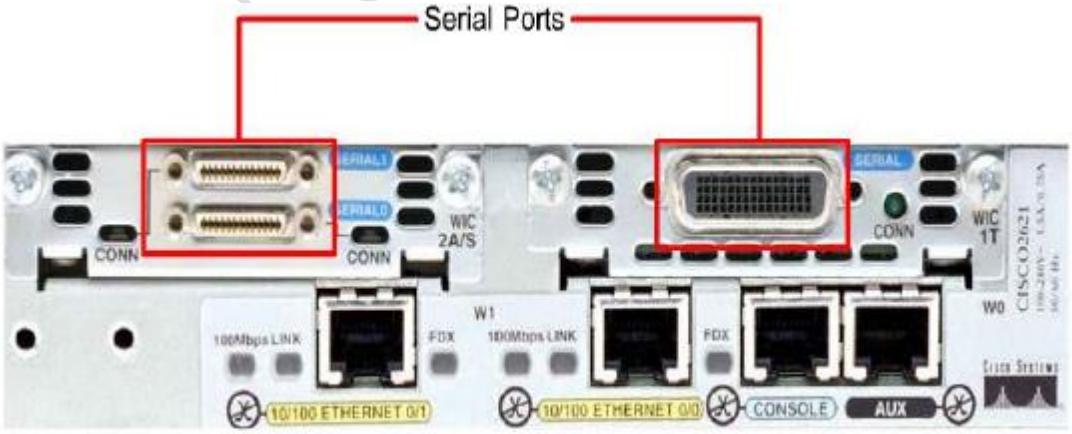
3- المنفذ الوهمي للطرفية (Virtual Terminal Port): يرمز له بالرمز "vty" ويختلف عن سابقيه بأنه منفذ وهمي افتراضي وليس فيزيائي. يستخدم هذا المنفذ للتحكم بالموجه عن بعد عبر منافذ التوصيل وعبر تقنية تسمى "الاتصال عن بعد" (Telnet)، وبواسطته يستطيع جهاز الموجه أن يستقبل عدة اتصالات من النوع Telnet بنفس الوقت. فمثلاً يستطيع الموجه ذو الموديل 2610 استقبال عشرة اتصالات بنفس الوقت أرقامها " 0" إلى " 9". حيث يقوم مدير الشبكة بالدخول إلى واجهة النظام DOS من أي جهاز على الشبكة المتصلة بالموجه، ويقوم بكتابة الأمر Telnet متبوعاً برقم IP لأي منفذ من منافذ التوصيل للموجه كما الشكل (10.12).

2.2.2.12- منافذ التوصيل (Connection Interfaces):

1- Ethernet/Fast Ethernet/Gigabit Ethernet: تستخدم هذه الأنواع الثلاثة عادة لتوصيل الموجه من جهة الشبكة LAN، أي توصيلها مع المبدل (Switch) على أحد منافذه، وفي هذه الحالة يتم استخدام كابل UTP من النوع Straight-Cable. بالنسبة للموجه موديل 1841 مثلاً، يحوي عادةً منفذ واحد Fast Ethernet 0 أو Fast Ethernet 0/0 ونستطيع إضافة منافذ عند الحاجة عن طريق شقوق التوسع.

تحوي المبدلات على عدد كبير من هذه المنافذ، أما الموجهات فتملك عدد قليل منها.

2- Serial/Smart Serial: تستخدم هذه المنافذ لوصل الموجه مع الشبكات الواسعة WAN أو مع جهاز موجه أخر. يحوي منفذ Serial على 60-pins بينما يحوي منفذ Smart Serial على 26-pins. يبين الشكل (11.12) منافذ التوصيل التسلسلية للموجه:



الشكل (11.12): منافذ توصيل الموجه التسلسلية.

الدخول إلى نظام التشغيل IOS والتعامل معه

3.2.12- نظام التشغيل (Operation System):

يحوي الموجه نظام تشغيل (Internetwork Operation System: IOS) وهو عبارة عن ملف مؤلف اسمه من قسمين، يتألف القسم الأول من دلالات معينة خاصة بمواصفات جهاز الموجه والقسم الثاني يكون عادة (Bin). يكون لكل نظام تشغيل إصدار معين يكتب ضمن اسم ملف نظام التشغيل.

3.12- الدخول إلى نظام تشغيل الموجه (Access the Router's Operation System):

نعلم أن طرق الاتصال بالموجه والدخول إلى إعدادات نظام تشغيله هي:

1- عن طريق منفذ Console.

2- عن طريق منفذ Auxiliary.

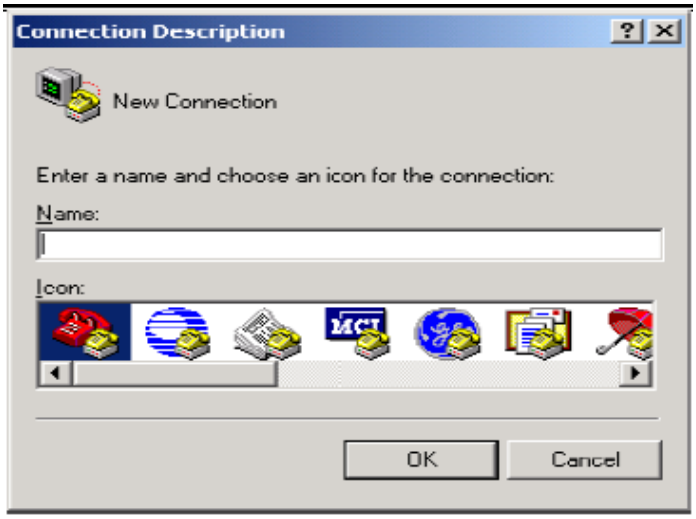
3- عن طريق تقنية تدعى Telnet وهذه الطريقة تتم عن طريق اتصال الشبكة وليس بالاتصال الخاص والمباشر.

يعد الاتصال عن طريق منفذ Console الأكثر استخداماً، حيث يتم الاتصال بالموجه باستخدام حاسوب عادي وكبل اتصال وبرنامج طرفي يستخدم لإجراء العمليات عليه، يدعى هذا البرنامج في أنظمة التشغيل ويندوز بـ " Hyper Terminal"، يقوم هذا البرنامج بالدخول إلى نظام تشغيل الموجه IOS.

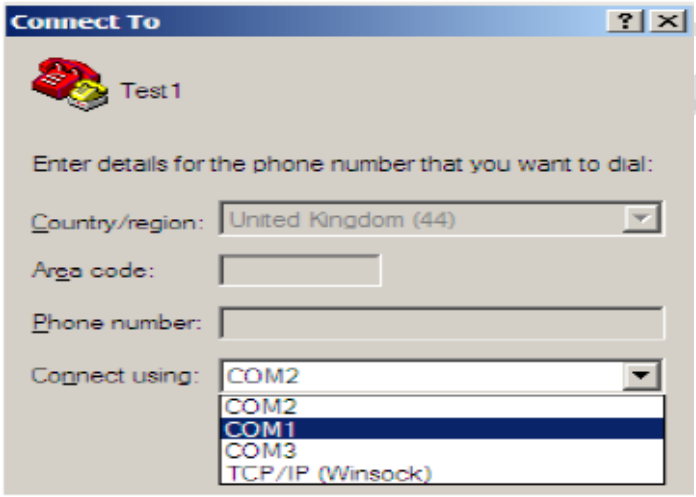
كما ويبين الشكل (13.12) خطوات إعداد برنامج الدخول إلى الموجه:

من قائمة "ابدأ" (Start) نختار "كافة البرامج" (All Programs) ثم "الملحقات" (Accessories) ومن ثم "الاتصالات" (Communications) وأخيراً برنامج "HyperTerminal".

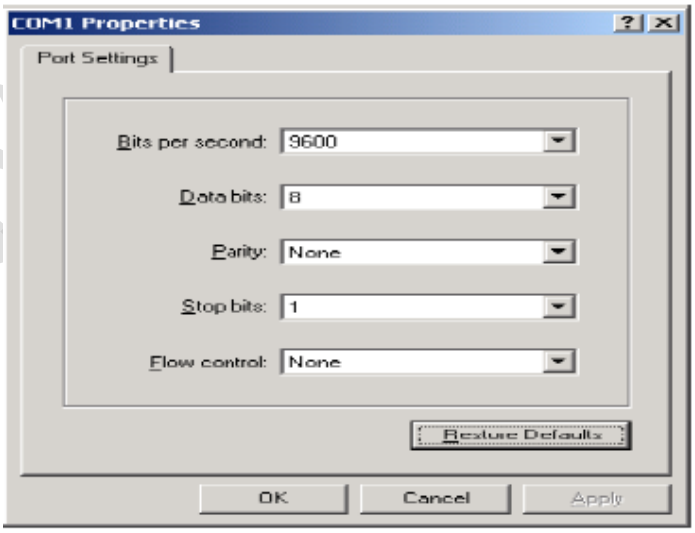
في الشكل (13.12-أ) نضع اسم لتعريف الاتصال مثل " Test 1" أو أي اسم أخر ثم نضغط "موافق" (OK). نختار في الشكل (13.12-ب) رقم منفذ الاتصال وليكن (Com1)، بعد ذلك نضبط إعدادات المنفذ ويفضل استخدام الإعدادات الإفتراضية بالضغط على الزر "استعادة الافتراضيات" (Restore Defaults) كما في الشكل (13.12-جـ) ثم نضغط "موافق" (OK) للدخول إلى الموجه.



(أ): كتابة اسم لتسمية الاتصال.



(ب): إختيار المنفذ.



(جـ): ضبط اعدادات المنفذ.

الشكل (13.12): خطوات إعداد برنامج Hyper Terminal للدخول إلى الموجه.

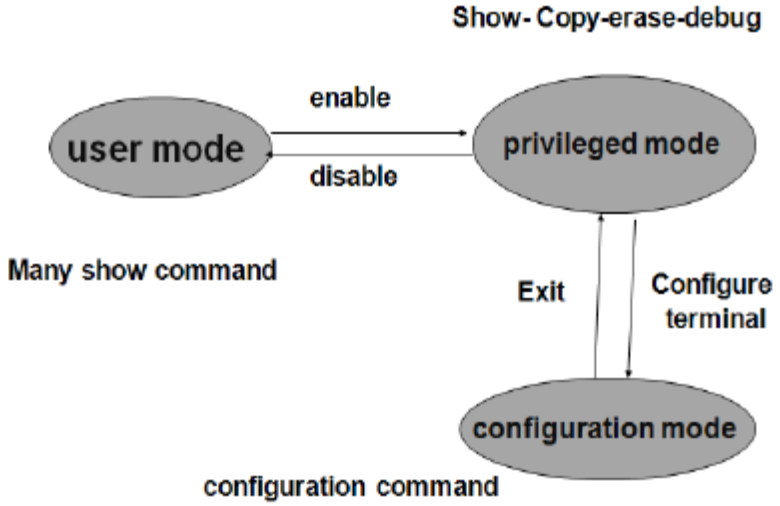
5.12- واجهة سطر الأوامر (Command Line Interface: CLI):

عندما يتم الدخول إلى جهاز الموجه بأي طريقة من الطرق السابقة فإنه يتم عرض الشاشة الرئيسية لنظام التشغيل والتي تسمى CLI ويكون اسم النمط الذي نكون فيه هو وضع المستخدم (User Mode) الذي نستطيع من خلاله تنفيذ عدد محدود من الأوامر، ويكون شكل المؤشر في هذا الوضع هو " >". لكي يتم الانتقال إلى الوضع المتميز (Privilege Mode) نقوم بكتابة الأمر " Enable" فيقوم الموجه عادة بطلب كلمة المرور يتم إعدادها من قبل مدير الشبكة. عند وضع كلمة المرور الصحيحة يتم الدخول إلى الوضع المتميز ويصبح شكل مؤشر الكتابة "#"، عندها يستطيع المستخدم التحكم بكامل إعدادات الموجه.

ولكي يتم الرجوع إلى وضع المستخدم نكتب الأمر "Disable".

للانتقال إلى وضع الإعدادات نكتب الأمر " Configure Terminal" فيصبح شكل المؤشر "#(config)" ولكي يتم الرجوع إلى الوضع (النمط) المتميز نكتب الأمر "Exit".

يبين الشكل (15.12) خطوات الانتقال بين أنماط نظام IOS:



الشكل (15.12): خطوات الانتقال بين أنماط نظام IOS.

للحصول على المساعدة وعرض الأوامر التي نستطيع تنفيذها في أي نمط يمكن كتابة علامة الاستفهام متبوعة بضغطة على مفتاح الإدخال. وبحال كانت الأوامر المتوفرة أكثر من عرض الصفحة نستطيع استخدام مفتاح "الإدخال" (Enter) لعرض الأوامر سطراً سطراً، أو المفتاح "مسافة" (Space Bar) لعرض الأوامر صفحة تلو صفحة.

ملاحظات:

نستطيع من مؤشر الكتابة كتابة جزء من الأمر المطلوب تنفيذه ثم نقوم بضغط المفتاح "جدولة" (Tab) الذي سيقوم بدوره بتكملة الأمر نيابة عنا.

نستطيع في معظم الأوامر كتابة جزء منها فقط وعند الضغط على مفتاح "الإدخال" (Enter) فيقوم الموجه بتنفيذها، مثل الأمر "Enable" يكفي أن نكتب "En".

6.12- أنماط نظام تشغيل الموجه (IOS Modes):

النمط الأول وهو نمط المستخدم (User Executive Mode). في هذا النمط نتمكن من إجراء بعض الأوامر مثل تعليمات Ping وبعض تعليمات الإظهار (Show) المحدودة وتعليمة Enable للانتقال إلى النمط المتميز.

النمط الثاني وهو النمط المتميز (Privileged Executive Mode). في هذا النمط نستطيع إضافة إعدادات واستخدام كامل تعليمات الإظهار بالإضافة إلى التعليمات التي يمكن استخدامها في النمط الأول.

النمط الثالث وهو نمط الإعدادات (Configuration Mode). في هذا النمط نتمكن من تغير أسماء أجهزة الشبكة كالموجة أو المبدّل، ووضع كلمات المرور المختلفة... الخ. يبين الشكل (16.2) أنماط العمل تلك.

كما ويبين الشكل أيضاً أن النمط الثالث وهو نمط الإعدادات (Configuration Mode) والذي يسمى أحياناً بنمط الإعدادات العام (Global Configuration Mode) يتفرع إلى عدة فروع وكل فرع يتخصص بوضع إعدادات معينة ويسم ى هذا التفرع بأنماط الإعدادات المحددة (Specific Configuration Modes)، وهذه الفروع قد تكون:

1- نمط الواجهة (Interface Mode): لوضع إعدادات منافذ التوصيل المستخدمة كواجهات للشبكة مثل Fa0/0 و S0/0/0 ...إلخ.

2- نمط المسار (Line Mode): لوضع إعدادات كلمات المرور لمنافذ التحكم الخاصة سواءً أكانت فيزيائية أو وهمية مثل Console، AUX، VTY.

3- نمط الموجه (Router Mode): لوضع إعدادات بروتوكولات التوجيه، ولا يوجد هذا النمط في المبدلات، فهي لا يستخدم بروتوكولات التوجيه في عملها.

يبين الشكل (17.12) فروع انماط الإعدادات المحددة:

Configuration Mode	Prompt
Interface	Router(config-if)#
Line	Router(config-line)#
Routers	Router(config-router)#

7.12- أوامر نظام تشغيل الموجه (IOS Commands):

الأمر "؟":

يستخدم الأمر "؟" لعرض جميع الأوامر التي يمكن استخدامها في أي نمط مع ذكر وظيفة كل أمر . نبين فيما يلي الأوامر التي يمكن استخدامها في نمط المستخدم عند كتابة "؟" في واجهة سطر الأوامر ، حيث يظهر بجانب كل أمر شرح وظيفة هذا الأمر :

```
Router>?
Exec commands:
<1-99>      Session number to resume
connect     Open a terminal connection
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
show        Show running system information
telnet      Open a telnet connection
terminal    Set terminal line parameters
Router>
```

الانتقال من نمط المستخدم إلى النمط المتميز وبالعكس:

```
Router>enable
Router#disable
Router>
```

أوامر "العرض" (Show):

أوامر العرض (الإظهار) كثيرة ومتنوعة ولكل منها وظيفة معينة. يبين الجدول (4.12)

بعض أهم أوامر الإظهار في الموجه التي يمكن استخدامها في النمط المتميز ووظيفة كل منها:
نلاحظ في الأمر السابق تغير المؤشر "<" إلى "#" كدليل على انتقالنا من نمط المستخدم إلى النمط المتميز .

الانتقال من النمط المتميز إلى نمط الإعدادات والرجوع:

```
Router#configure terminal
Router(config)#exit
Router#
```

الأمر	الوصف
#show clock	يعرض الوقت و التاريخ الحالي للموجه
#show running-config #show run	يقوم بعرض إعدادات الموجه بالذاكرة RAM
#show startup-config #show start	يقوم بعرض إعدادات الموجه بالذاكرة NVRAM
#show flash	يعرض محتويات الذاكرة flash
#show interface {type} {num}	يعرض معلومات عن منفذ معين
#show ip interface brief	يعرض معلومات مختصرة عن المنافذ بالموجه
#show version	يعرض مواصفات جهاز الموجه من وذواكر ومنافذ

الجدول (4.12): أهم أوامر العرض في الموجه.

أوامر لأمان نظام التشغيل IOS

عند إقلاع الموجه نلاحظ ظهور الرسائل التالية

```
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

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]: |
```

الحوار Continue with configuration dialog? [yes/no] يعني انه لا يوجد إعدادات مخزنة بالموجه

نكتب NO لإدخال الإعدادات يدوياً دون مرشد

```
         --- System Configuration Dialog ---

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


  Press RETURN to get started!



  Router>
```

وهنا نكون في وضع المستخدم (User mode) ويسمى وضع المعاينة.

نستخدم التعليمة ؟ لمعرفة الأوامر الموجودة في الوضع الحالي

```
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>
```

Enable للانتقال إلى الوضع المتميز نستخدم التعليمة

```
        --- System Configuration Dialog ---

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


Press RETURN to get started!



Router>enable
Router#
```

لعرض إعدادات العمل الحالية للموجه والمخزنة في الذاكرة RAM

نستخدم الأمر show running-config

```
Router#show run
Router#show running-config
Building configuration...

Current configuration : 489 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
!
!
!
 --More--
```

لعرض إعدادات الإقلاع للموجه و المخزنة في الذاكرة NVRAM

نستخدم الأمر show startup-config

```
Router#
Router#show start
Router#show startup-config
startup-config is not present
Router#
```

لنسخ الإعدادات نستخدم الأمر copy running-config startup-config

```
Router#
Router#show start
Router#show startup-config
startup-config is not present
Router#copy run
Router#copy running-config start
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

أو من خلال الأمرwrite

```
Router#
Router#wr
Router#write
Building configuration...
[OK]
Router#
```

للدخول إلى نمط الإعدادات نستخدم الأمر configure terminal

```
Router>
Router>ena
Router>enable
Router#config
Router#configure t
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

للخروج من أي وضع للوضع السابق نستخدم الأمر Exit

للانتقال من Enable mode إلى User mode نستخدم الأمر Disable

```
Router#
Router#disa
Router#disable
Router>
```

مهما كان المستوى Enable Mode فتعيدنا إلىCRTL+Zأما

لتسمية الراوتر نستخدم الأمرHostname {name}

```
Router(config)#
Router(config)#host
Router(config)#hostname basil
```

- اوامر كلمات المرور :

Enable password: عند الانتقال من User Mode إلى Enable Mode

و تفعل بالأمرEnable password {password}

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable pass
Router(config)#enable password cisco1
Router(config)#
```

يتم عرضها كنص صريح عند استخدام الامر show run أو show start

أما Enable secret تتميز بأنها تكون مشفرة عند استخدام الامر show run أو show start

Enable secret {password}و تفعل بالأمر

```
Router(config)#enable
Router(config)#enable sec
Router(config)#enable secret cisco2
Router(config)#
```

Console password: يتم طلبها عند الدخول الى الراوتر عبر منفذ الكونسول

Config-lineيتم تعيين هذه الكلمة في المستوى

0 للمنفذ ورقمه Console حيث Line console 0عن طريق الأمر

Password {password}ثم الأمر

login ثم

```
Router(config)#line console 0
Router(config-line)#pas
Router(config-line)#password cisco4
Router(config-line)#logi
Router(config-line)#login
```

Service password-encryptionيمكننا استخدام الأمر لتشفير

Show start أو Show runجميع كلمات المرور بحيث تظهر مشفرة عند استخدام الأمر

```
Router(config)#
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#
```

- أوامر عنونة منافذ الموجه :

من مستوى الإعدادات نكتب الأمر interface fastEthernet 0/0 حيث :

نوع المنفذ fastEthernet ورقمه 0/0

ثم الأمر ip address {ip} {mask}

وثم نقوم بتفعيل المنفذ بالأمر no shutdown

```
Router(config)#
Router(config)#inter
Router(config)#interface f
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no sh
Router(config-if)#no shutdown

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

Router(config-if)#
```

TELNET

شروط نجاح اتصال Telnet :

- وجود اتصال فعال TCP/IP بين الموجه والجهاز (أي تحقق نجاح Ping)
- تفعيل خدمة TELNET عند الهدف .
- أن يكون الهدف محمي بـ Enable password أو Enable secret

تفعيل خدمة: TELNET

من وضع الإعدادات نستخدم الأمر Line vty 0 4

التعليمة : Password {password}

ثم Login

```
Router(config)#
Router(config)#line vty 0 4
Router(config-line)#password cisco5
Router(config-line)#login
Router(config-line)#
```

بفرض أن R1 يرغب باتصال Telnet إلى R2

أي R1 هو المصدر

و R2 هو الهدف

فبعد تفعيل Telnet عند الهدف نستخدم الأمر telnet {ip} لإنشاء اتصال Telnet

حيث أن IP{} للهدف حيث تم تفعيل خدمة TELNET

```
R1>
R1>telnet 10.0.0.2
Trying 10.0.0.2 ...Open


User Access Verification

Password:
r2>en
r2>enable
Password:
r2#
```

ولكن ما يعيب اتصال TELNET انه غير مشفر ولحل هذه المشكلة يمكن استخدام اتصال SSH وهو اتصال بعيد مشفر .

SSH

لتفعيل خدمة SSH في الجهاز الهدف يجب :

- وضع username & password أما في اتصال TELNET يمكن الاستغناء عن username

ويتم ذلك في وضع الاعدادات

بالأمر Username {name} password {password}

ثم الانتقال إلى line vty 0 4

وكتابة الأمر login local

```
r2(config)#
r2(config)#username basil password cisco10
r2(config)#line vty 0 4
r2(config-line)#login local
r2(config-line)#
```

- وضع اسم domain في مستوى الإعدادات بالأمر التالي :

IP domain-name {name.com}

```
r2(config)#
r2(config)#ip domain-name basil.com
r2(config)#
```

-إنشاء مفتاح التشفير بالأمر التالي :

crypto key generate rsa

حجم المفتاح يكون ضمن المجال من 360 الى 2048 بت بحيث كلما زاد الحجم ازداد زمن التشفير وتكون القيمة الافتراضية 512 بت

```
r2(config)#cr
r2(config)#crypto k
r2(config)#crypto key g
r2(config)#crypto key generate rsa
The name for the keys will be: r2.basil.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

r2(config)#
```

لإنشاء اتصال SSH للوصول للهدف نستخدم الأمر :

SSh –l {username} {IP}

حيث أن: اسم المستخدم username

عنوان الهدف IP

```
R1>
R1>ssh -l basil 10.0.0.2
Open
Password:


r2>
```

ملاحظة: يمكن تنفيذ أوامر مستوى user mode و enable mode من أي مستوى كان وذلك بكتابة الأمر مسبوقا بالكلمة do

المهندس باسل دهيمش

قوائم التحكم بالوصول (Access Control List: ACL)

تستخدم قوائم التحكم بالوصول لتصفية الرزم وفحصها، ليتم حجب الرزم غير المرغوب بمرورها أو السماح لها بالمرور حسب السياسات الأمنية المطبقة في الشبكة.
تعتبر قوائم التحكم بالوصول مثلاً على جدار النار تصفية الرزم.

أنواع قوائم الوصول

1- القياسية (Standard): تفحص عنوان IP المصدر فقط وتُطبق على منفذ الموجه الأقرب للهدف، وفي مقررنا سنستخدم هذا النوع فقط.
2- الموسعة (Extended): تفحص عنوان IP المصدر وIP الهدف والبروتوكول ورقم المنفذ المصدر والهدف مما يتيح إمكانية تحكم أوسع، وتُطبق على منفذ الموجه الأقرب للمصدر.

القواعد الأساسية

1- تقارن الرزمة مع أسطر القائمة بالترتيب ابتداءً بالسطر الأول ثم الثاني وهكذا..
2- تستمر المقارنة مع الأسطر تباعاً حتى ينطبق على الرزمة أحد الأسطر ثم تتوقف المقارنة.
3- عندما لا ينطبق أي من الأسطر على الرزمة فإنها ستُهمل بشكل افتراضي.
4- يمكن للقائمة أن تسمّى أو تُرقّم. سنركز على القوائم من نوع standard ذات الأرقام ترقم من المجال 1-99 بالإضافة للمجال 1300-1999)
5- يجب تحديد ثلاثة عوامل: وهي
   - تحديد الموجه الانسب لتنفيذ عملية الفحص.
   - تحديد المنفذ الأنسب لتنفيذ عملية الفحص.
   - تحديد اتجاه عملية الفحص للمنفذ، وهو إمّا inbound (أي الرزمة داخلة إلى المنفذ) أو outbound (أي الرزمة خارجة من المنفذ).
6- يمكن وضع قائمة واحدة لكل منفذ ولكل بروتوكول وكل اتجاه (أي يمكن تطبيق قائمة in واحدة وقائمة out واحدة لكل منفذ).

7- عند إضافة سطر جديد للقائمة يندرج بالنهاية دائما.

8- إذا لم تنتهِ القائمة بأمر permit any فإن جميع الرزم التي لم ينطبق عليها أي من أسطر القائمة سوف تُهمل، وهذا ما سبقت الاشارة إليه القاعدة 3.

9- قائمة التحكم بالوصول تفحص الرزم المارة عبر الموجه وليس الرزم التي يولِّدها الموجه فإنها لا تُفحص.

10- عند كتابة أسطر القائمة نستخدم الكلمة deny لمنع مرور الرزمة و permit للسماح بمرورها.

11- تستخدم قوائم التحكم بالوصول القناع العكسي (wildcard mask) بدلاً من القناع العادي للشبكة

12- يتم استنتاج القناع العكسي بطرح القناع العادي من القيمة 255.255.255.255

أمثلة عن القناع العكسي

1- إذا كان عنوان الشبكة: 172.16.16.0 وقناعها 255.255.252.0 يكون القناع العكسي لها 0.0.3.255

2- إذا كان عنوان الشبكة: 172.16.16.0 وقناعها 255.255.248.0 يكون القناع العكسي لها 0.0.7.255

3- إذا كان عنوان الشبكة: 192.168.160.0 وقناعها 255.255.224.0 يكون القناع العكسي لها 0.0.31.255

ملاحظة: إذا أردنا حجب جهاز معين نستخدم القناع العكسي 0.0.0.0

خطوات كتابة وتنفيذ Access List:

الخطوة الأولى: نكتب أسطر القائمة بالترتيب، على هيئة السطر التالي:

```
Router(config)#access-list 1 deny 172.16.40.0 0.0.0.255
```

في التعليمة السابقة تم تسمية قائمة الوصول بالرقم 1 ومهمتها حجب جميع الاجهزة ضمن الشبكة 172.16.40.0 والقناع 255.255.255.0، أي تم حجب الأجهزة 172.16.40.1 و 172.16.40.2 و... حتى 172.16.40.254

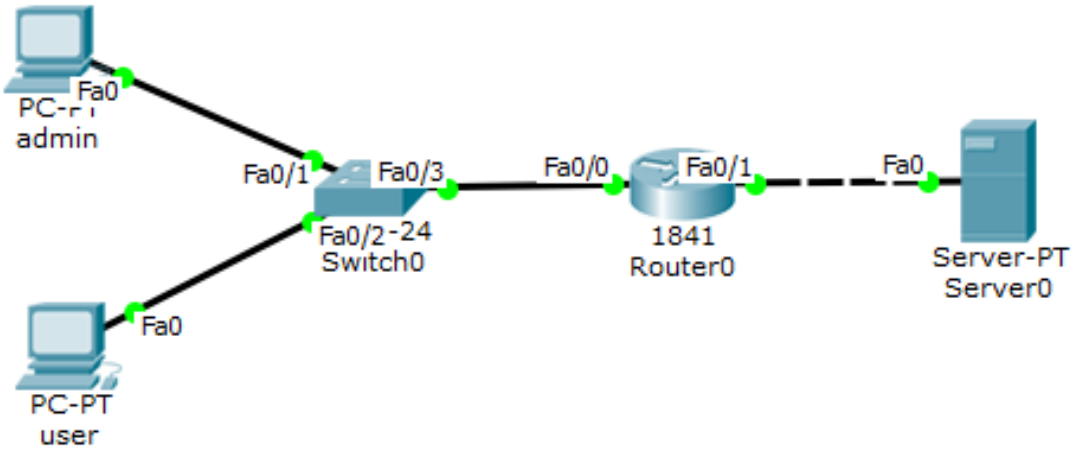
الخطوة الثانية: بعد الانتهاء من كتابة القائمة ندخل إلى المنفذ المناسب ونكتب تعليمة تطبيق القائمة على المنفذ مع تحديد اتجاه عملية الفحص هل هو in أم out.

```
Router(config)#int fa 0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

في التعليمات السابقة تم الدخول إلى المنفذ fa0/0 وتفعيل قائمة التحكم بالوصول ذات الرقم 1. ستتم عملية الفحص على الرزم أثناء خروجها (out) من منفذ الموجه fa0/0.

تدريب: بفرض لديك الشبكة المعطاة بالشكل التالي ويراد وضع لائحة تحكم بالوصول ACL للقيام ببعض عمليات الحجب والسماح، والمطلوب:

1- تحديد المنفذ الأفضل لتطبيقها عليه واتجاه عملية الفحص.
2- حجب المتصل user من الاتصال بالمخدم.
3- السماح للمتصل admin بالاتصال بالمخدم.



الحل:

```
Router(config)#access-list 10 deny 10.0.0.3 0.0.0.0
Router(config)#access-list 10 permit 10.0.0.2 0.0.0.0
Router(config)#int fa 0/1
Router(config-if)#ip acc
Router(config-if)#ip access-group 10 out
Router(config-if)#
```

CCProxy

نقوم بدراسة برنامج CCproxy كمثال عملي على جدر الحماية من نوع عبّارة التطبيقات (Application gateway firewall).

أهم مزايا برنامج CCProxy

- دعم بروتوكولات عديدة منها HTTP و FTP و Telnet و Secure HTTPS.
- دعم الويب المخبئي (Web Cache) والذي يحسن من سرعة التصفح.
- التحكم المرن بعرض الحزمة.
- التحكم بحجب أو السماح بتصفح موقع محدد أو محتوى محدد.
- تقديم عدة أنواع من عمليات توثيق المستخدمين وفق التالي:

  IP address

  MAC address

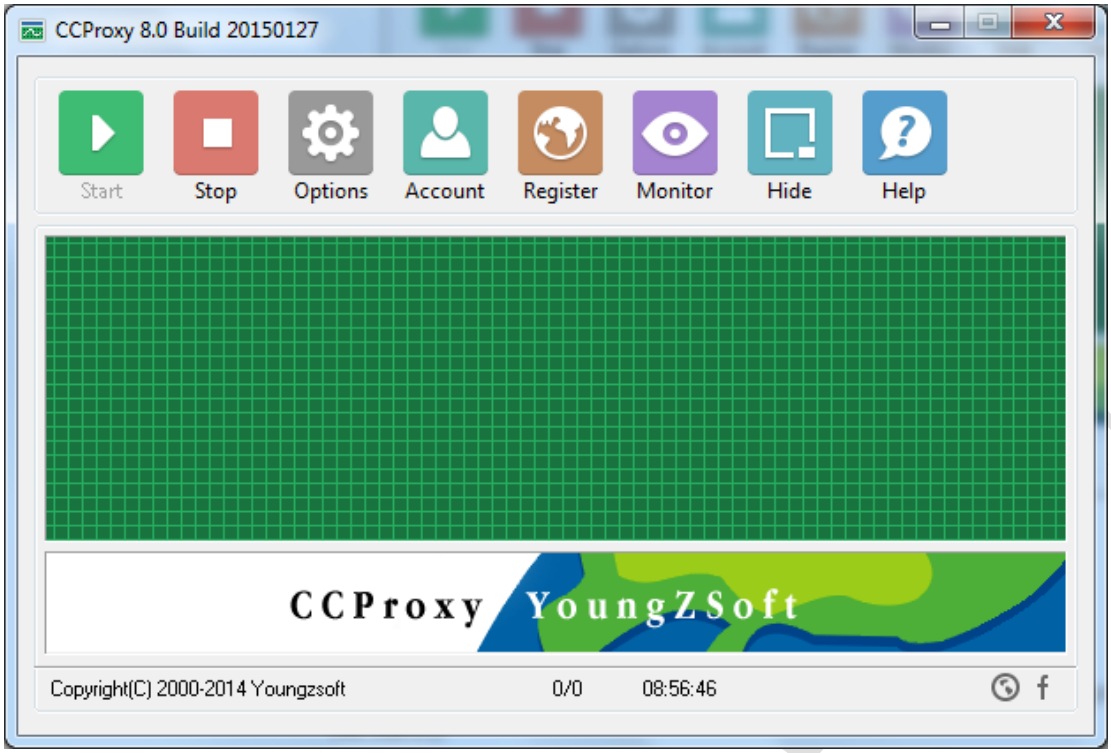
  User Name/Password

  IP + User Name/Password

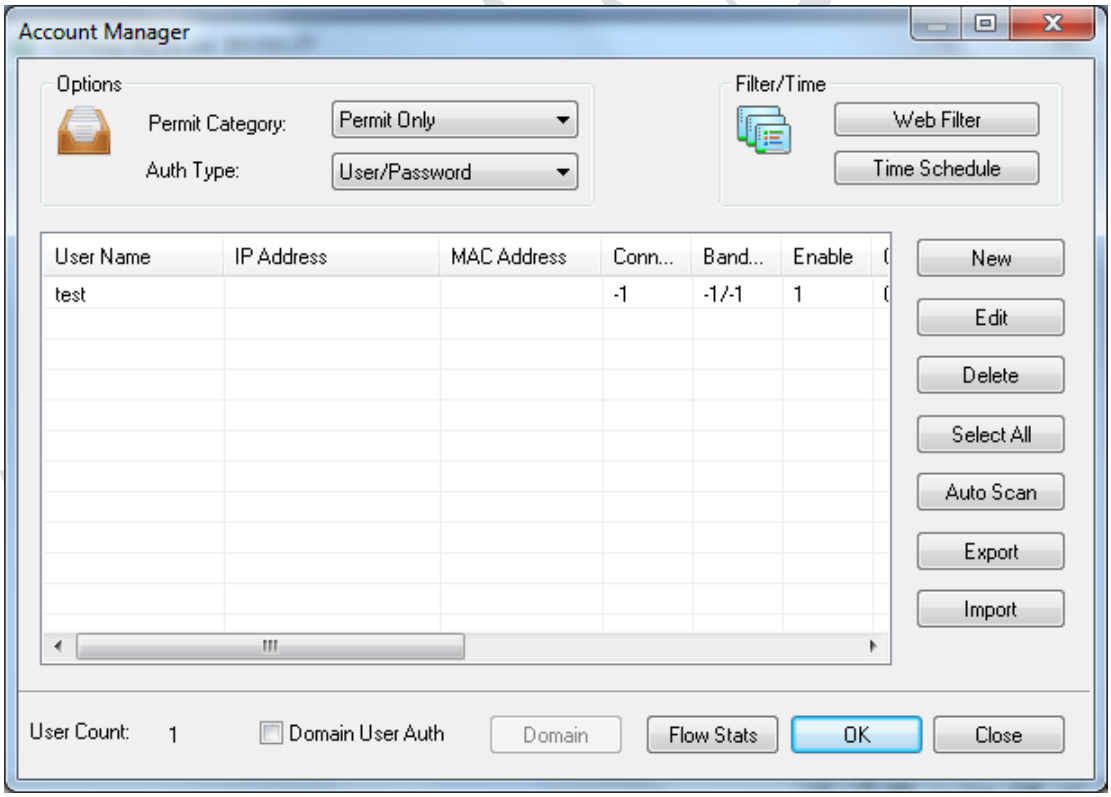
  MAC + User Name/Password and IP + MAC
- تتبع تصفح الزبون.
- التحكم بعرض الحزم لكل زبون.

البدء السريع بالعمل على برنامج

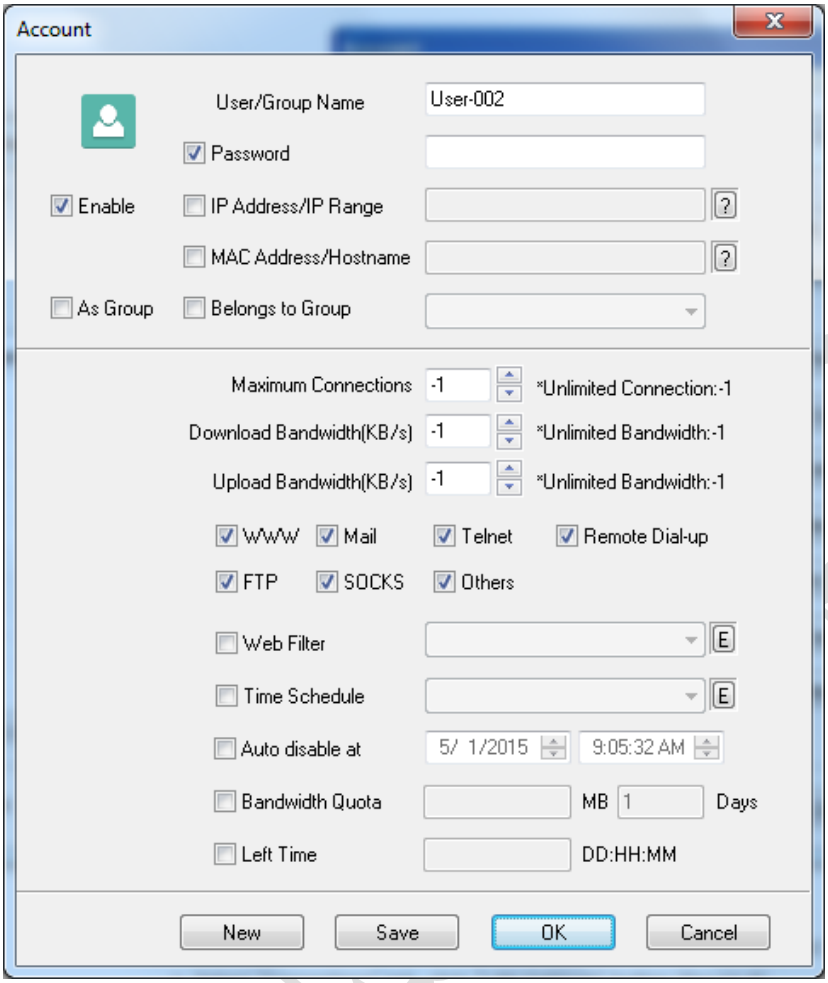
1- تنصيب البرنامج على مخدم ، وعلى المخدم أن يحوي كرتي شبكة أحدهما يؤمن الحصول على الاتصال بالانترنت والآخر يكون موجه لشبكة LAN الخاصة بالمستخدمين المراد إدارة ومراقبة اتصالهم بالانترنت.
يمكن أن يكون كلا كرتي الشبكة فيزيائيين، أو يمكن الاستعانة ببرنامج إضافي كبرنامج MyPublicWiFi يقوم بإنشاء كرت شبكة منطقي وهمي مع كرت الشبكة الفيزيائي ليصبح لدينا كرتي شبكة.



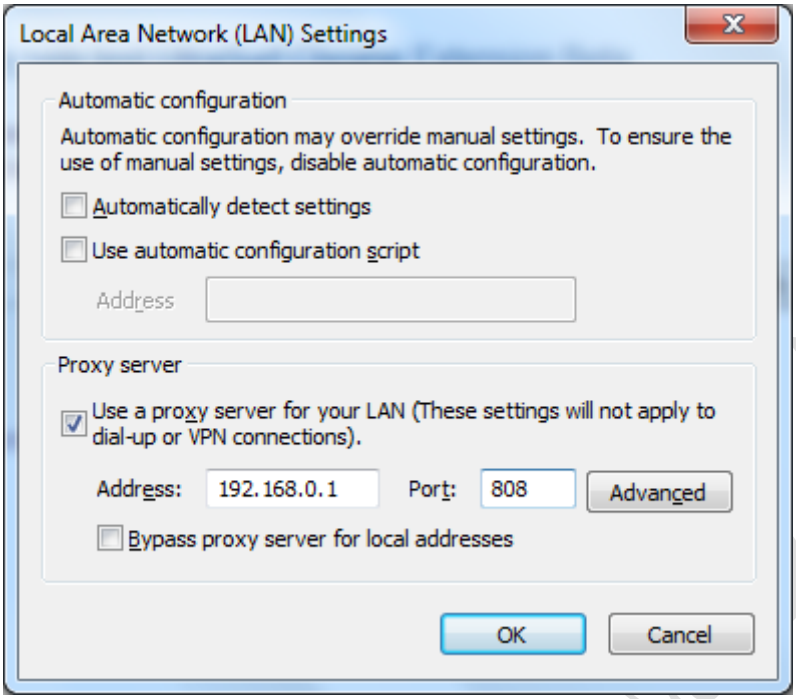
2- إضافة حسابات للزبائن، فمثلاً يوضح الشكل التالي أنه يوجد حساب اسمه test



لانشاء حساب جديد نختار "New" ونضبط بارامتراته وخصائصه كما في الشكل



3- ضبط إعدادات المتصفح لدى الزبون وذلك من متصفح Internet Explorer افتح تبويبة "خيارات" (Tools) ثم "خيارات الانترنت" (Internet Options) ثم "اتصالات" (Connections) ثم "إعدادات الشبكة المحلية" (LAN Settings) كما هو مبين في الشكل التالي حيث سيتم وضع عنوان CCProxy وهو في مثالنا 192.168.0.1 و المنفذ الافتراضي 808.



المهندس باسل دهيمش

Ultra Surf

تعريف: هو برنامج يستخدم لكسر وتجاوز ملقم مزود خدمة الانترنت (ISP Proxy) – الذي يقوم عادةً بتصفية وحجب بعض المواقع والخدمات – حيث يقوم هذا البرنامج بإنشاء ملقم محلي (Local Proxy)على حواسيب المستخدمين، وتوجيه طلباتهم إليه بدلاً من (ISP Proxy). يستخدم عادة وبشكل افتراضي المنفذ (Port) رقم 9666.

أنواع النسخ: يتواجد من هذا البرنامج نسختين:

1- نسخة مخدم (Server) موجودة على سيرفرات موصولة بالانترنت بشكل دائم.

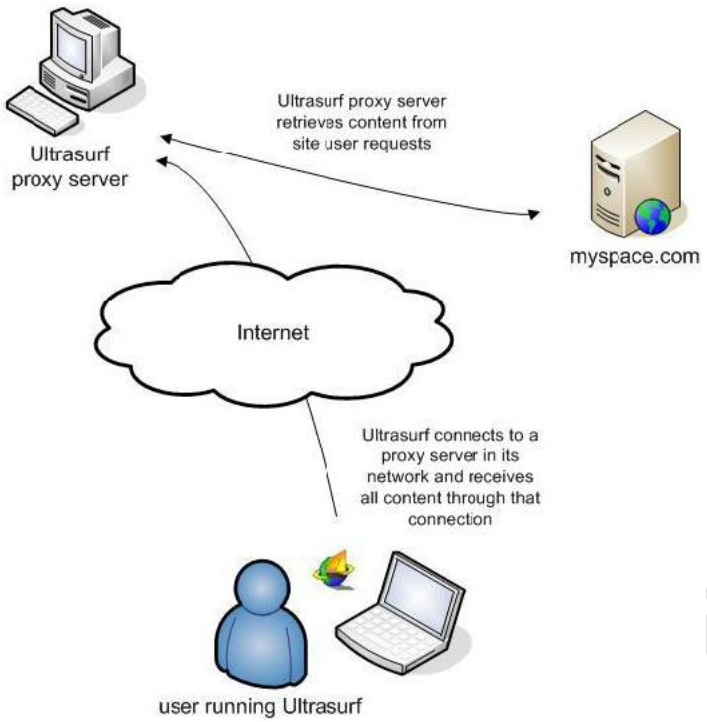
2- نسخة الزبون (Client) وهي عبارة عن ملف تنفيذي بالامتداد exe لبرنامج مكتوب بلغة ++C.

مبدأ العمل: يقوم المستخدم بتنفيذ نسخة الزبون بالنقر الثنائي على ملفها التنفيذي. سيحاول برنامج الزبون تأسيس اتصال مشفر مع برنامج المخدم.

يستخدم هذا الاتصال طريقة مصافحة غير تقليدية لعملية التوثيق وستكون الاتصال مشفراً باستخدام المنفذ رقم 443.

يحول برنامج الزبون حاسب المستخدم إلى (Local Proxy).

سيقوم المتصفح بتحويل البيانات إلى (Local Proxy) بدلاً من (ISP Proxy) بدليل ظهور العنوان 127.0.0.1 في خانة الملقم داخل إعدادات المتصفح. يوضح الشكل (1) مبدأ عمل البرنامج بنسختيه.



الشكل (1)

يقوم برنامج الزبون بطلب الصفحة من برنامج المخدم ثم يقوم برنامج المخدم بجلب الصفحة وإعادتها لبرنامج الزبون. وبذلك يضمن Ultra surf عدم مخاطبة المواقع المحظورة مباشرة.

طرق البحث عن مخدم (Server) برنامج Ultrasurf:

1- عن طريق ملفات الكاش (cache) الموجودة على حاسب المستخدم والتي تحفظ عناوين المواقع التي تمت زيارتها ومن ضمنها عناوين مخدمات Ultrasurf .
2- عن طريق استعلام DNS العالمي ، وهذه هي الطريقة التقليدية للحصول على IP المواقع والمخدمات.
3- عن طريق ملف مستند محفوظ مع مستندات Google، يحوي هذا المستند على عناوين مخدمات Ultrasurf الفعالة.
4- عن طريق قائمة ثابتة موجودة ومبنية بداخله.

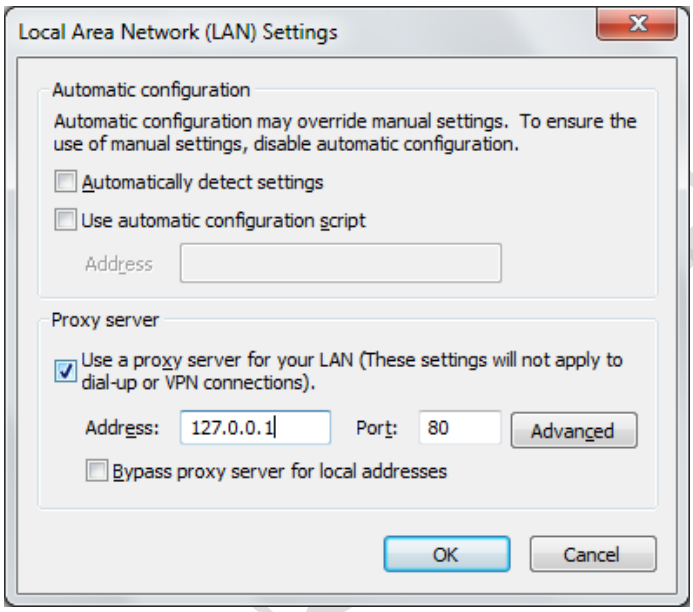
تدريب:

1- سجل عنوان Public IP الذي حصلت عليه من مزود الخدمة.
2- قم بزيارة أحد المواقع المحجوبة من قبل مزود خدمة الانترنت
3- شغّل برنامج Ultrasurf.
4- سجل عنوان Public IP الذي قد قام Ultrasurf بإسناده لك.

5- أعد زيارة أحد المواقع المحجوبة من قبل مزود خدمة الانترنت

6- من متصفح Internet Explorer افتح تبويبة "خيارات" (Tools) ثم "خيارات الانترنت" (Internet Options) ثم "اتصالات" (Connections) ثم "إعدادات الشبكة المحلية" (LAN Settings). ستلاحظ أن حاسوبك قد تحول إلى Local Proxy عبر وضع العنوان 127.0.0.1 في خانة "الملقم الوكيل" (Proxy Server).

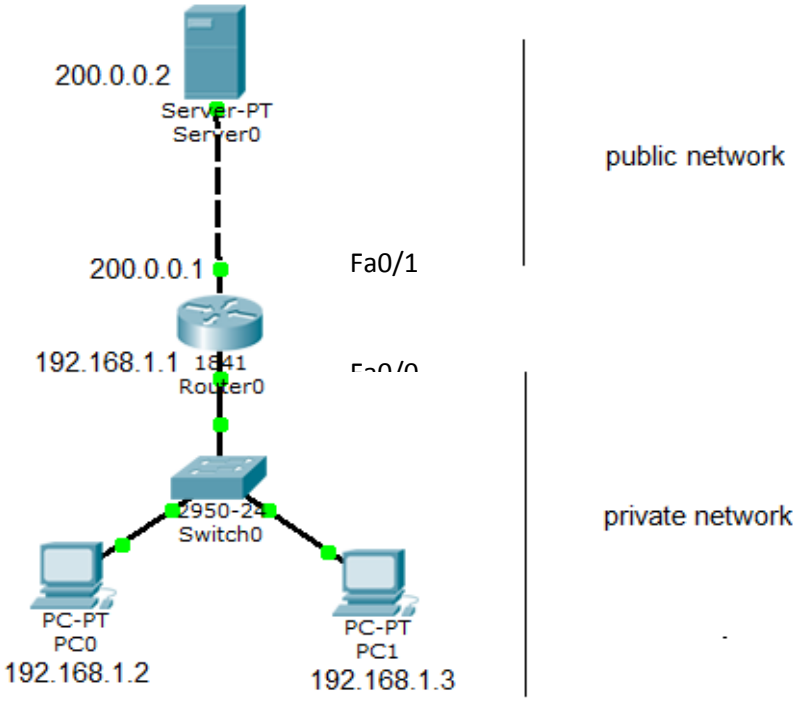
انظر الشكل (2)



الشكل (2)

ترجمة عنوان الشبكة (Network address translation: NAT)

ضبط إعدادات Nat : نقوم بالبداية بتوصيل و ضبط إعدادات الشبكة ووضع عناوين ip كما في الشكل التالي:



لمحاكاة عمل مزودات خدمة الانترنت سنقوم بحجب عناوين الشبكة الخاصة 192.168.1.0 من الخروج إلى الشبكة العامة عبر تعليمات قوائم التحكم بالوصول (Access Control List: ACL)

من نمط الإعدادات (configure terminal) نكتب الأمر التالي الذي يقوم بمنع خروج أي ip من private network إلى public network:

Access-list 1 deny 192.168.1.0 0.0.0.255

مع الأمر التالي الذي يسمح لباقي عناوين IP من الشبكات الأخرى بالخروج من private إلى public

Access-list 1 permit any

سيكون شكل الأمرين السابقين في الاعدادات هو:

```
Router(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Router(config)#acc
Router(config)#access-list 1 permit any
Router(config)#
```

نقوم بالانتقال إلى interface fastethernet الخاص بالمنفذ (0/1)

ونكتب الأمر:

ip access-group 1 out

لتطبيق access list 1 على هذا المنفذ لمنع خروج ip إلى public network

```
Router(config)#int fa 0/1
Router(config-if)#ip access-
Router(config-if)#ip access-group 1 out
```

نلاحظ الآن فشل الاتصال من الشبكة الخاصة إلى العامة وبإمكاننا تنفيذ ping للتأكد من ذلك.

I- إعداد nat الساكن : ويتم وفق ثلاث مراحل:

1- نقوم بتحديد الشبكة الداخلية

في interface fastethernet 0/0 نكتب التعليمة :

ip nat inside

سيكون شكل الأمرين السابقين في الاعدادات هو:

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
```

2- نقوم بتحديد الشبكة الخارجية

في interface fastethernet 0/1 نكتب التعليمة :

ip nat outside

سيكون شكل الأمرين السابقين في الإعدادات هو:

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat ou
Router(config-if)#ip nat outside
```

3- نقوم بكتابة التعليمة التالية في وضع الإعدادات التي تقوم بالربط الدائم بين العنوان الخاص والعام :

ip nat inside source static 192.168.1.2 200.0.0.1

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router(config)#ip nat inside source static 192.168.1.2 200.0.0.1
```

حيث يتم ربط ip الداخلي مع الخارجي للخروج بالعنوان الخارجي .

حيث 192.168.1.2 يمثل inside local

و 200.0.0.1 يمثل inside global

ولعرض الإحصائيات و التراسلات نستخدم التعليمة:

Show ip nat statistics

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/1
Inside Interfaces: FastEthernet0/0
Hits: 0  Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 10 pool basil refCount 0
 pool basil: netmask 255.255.255.0
       start 200.0.0.1 end 200.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
Router#
```

ولعرض محتويات جدول NAT نستخدم التعليمة

Show ip nat translations

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router#sh ip nat tr
Router#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  200.0.0.1         192.168.1.2        ---                ---
```

والذي يوضح عملية ربط دائم بين العنوان العام والخاص.

لإلغاء الربط حتى نتمكن من تنفيذ أنوع NAT الأخرى نكتب التعليمة :

no ip nat inside source static 192.168.1.2 200.0.0.1

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router(config)#no ip nat inside source static 192.168.1.2 200.0.0.1
```

II- إعداد nat المتغير : ويتم وفق خمسة مراحل:

نقوم بتحديد inside nat و outside nat كما في الخطوتين 1 و 2 في NAT الساكن

3- نقوم بتعريف pool

وهو حوض يحوي مجموعة ip تحجزها الأجهزة للخروج إلى الشبكة الخارجية.

يتم تعريفه بالتعليمة :

ip nat pool basil 200.0.0.1 200.0.0.255 netmask 255.255.255.0

```
Router(config)#ip nat pool basil 200.0.0.1 200.0.0.255 netmask 255.255.255.0
Router(config)#
```

الحوض السابق اسمه basil ويحوي 255 عنوان ip ، أي يسمح لـ 255 حاسوب بالاتصال المتزامن بالانترنت.

ملاحظة: يمكن حل التمرين باستخدام عنوان مسجل واحد في الحوض وسيكون شكل التعليمة هو التالي:

ip nat pool basil 200.0.0.1 200.0.0.1 netmask 255.255.255.0

4- ثم نعرف access list لتضم الشبكات المسموح لها بالاتصال الخارجي .

Access-list 10 permit 192.168.1.0 0.0.0.255

```
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#
```

5- ثم نقوم بالربط بين عناوين access list الداخلية و المسموح لها بالاتصال مع عناوين الحوض pool الخارجية.

ip nat inside source list 10 pool basil

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router(config)#ip nat inside source list 10 pool basil
Router(config)#
```

III- إعداد PAT : ويتم وفق خمسة مراحل:

تتشابه الخطوات 1 و 2 و 3 و 4 بين NAT المتغير مع PAT

يوجد اختلاف وحيد بينهما هو:

أن الربط في الخطوة 5 هنا يتم على أساس رقم المنفذ وليس على أساس ip، وبالتالي ستكون الخطوة الخامسة هي:

5- نقوم بالربط بين عناوين access list الداخلية و المسموح لها بالاتصال مع عناوين الحوض pool الخارجية مع استخدام الكلمة المحجوزة overload لتشير إلى تحميل ip خارجي واحد لعدة ips داخلية باستخدام تقنية ترجمة عنوان المنافذ.

ip nat inside source list 10 pool basil overload

سيكون شكل الأمر السابق في الإعدادات هو:

```
Router(config)#ip nat inside source list 10 pool basil overload
```

أمان المنفذ (Port Security)

تعتمد فكرة أمان المنفذ في المبدلات على مايلي:

1- تعريف العدد الأعظمي لعناوين MAC المصدر المسموح لها بإرسال أطر إلى منفذ معين
2- مراقبة حركة كل الأطر عبر هذا المنفذ
3- عند وصول أطر لها عنوان MAC مصدر غير مسموح، سيتم انتهاك أمان المنفذ ، وعلى إثره سيقوم المبدل باتخاذ حدث (Action) لحماية المنفذ. الحدث الافتراضي هو (Shutdown).

علينا الدخول إلى المنفذ المراد إعداد الأمان عليه ثم تنفيذ الخطوات التالية:

الخطوة الأولى: تحديد نمط عمل المنفذ إما Access أو Trunk بالتعليمة التالية:

switchport mode access

أو

switchport mode trunk

الخطوة الثانية: تفعيل أمان المنفذ بالتعليمة التالية:

switchport port-security

الخطوة الثالثة: تحديد عدد عناوين MAC الأعظمي المسموح لهم الاتصال بالمنفذ وذلك بالتعليمة التالية:

switchport port-security maximum عدد العناوين الأعظمي

بحال عدم ضبط هذه التعليمة فسيتكون عدد عناوين MAC الأعظمي الإفتراضي هو 1.

الخطوة الرابعة: تحديد الحدث المتخذ بحال انتهاك المنفذ وذلك بالتعليمة التالية:

switchport portsecurity violation protect

أو

switchport portsecurity violation restrict

أو

switchport portsecurity violation shutdown

بحال عدم ضبط هذه التعليمة فسيكون الحدث المتخذ الافتراضي بحال انتهاك المنفذ هو Shutdown

الفرق بين الأحداث المتخذة بحال حدوث انتهالك المنفذ:

الفروقات بين الأحداث	محمي (protect)	مقيد (restrict)	مغلق (shutdown)
رفض البيانات الغريبة	نعم	نعم	نعم
إرسال رسالة إعلام لمدير الشبكة عند الانتهاك	لا	نعم	نعم
قفل المنفذ ورفض كل أنواع البيانات	لا	لا	نعم

الخطوة الخامسة: تحديد العناوين المسموح اتصالها بالمنفذ وذلك وفق التعليمة التالية:

switchport port-security mac-addressالعنوان

ملاحظة: نقوم بتكرار هذه التعليمة لكل عنوان MAC مسموح له بالاتصال بالمنفذ. أي نكرر هذه التعليمة حسب عدد عناوين MAC المحددة بالخطوة الثالثة.

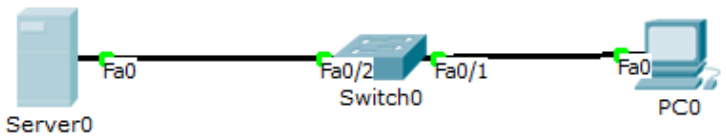
الخطوة السادسة: هذه الخطوة هي بديلة عن الخطوة الخامسة حيث يقوم المبدل بتعلم عنوان MAC الملتصق بالمنفذ واعتباره هو العنوان المسموح له بالاتصال بالمنفذ وفق التعليمة التالية:

switchport port-security mac-address sticky

ملاحظة: لا يجب تكرار هذه التعليمة حسب عدد عناوين MAC المحددة بالخطوة الثالثة. فمثلا: لو كان العدد الأعظمي المسموح هو 4، فعبر هذه التعليمة سيقوم المبدل بتعلم 4 عناوين MAC ملتصقة به ويعتبرها مسموحة المرور خلاله، وبحال محاولة عبور عنوان خامس فسيقوم بانتهاك المنفذ.

التطبيق العملي

ليكن لدينا الشبكة التالية والتي سنقوم بضبط إعدادات أمان المنفذ بالمبدل بحيث سنسمح فقط للحاسوب PC0 ذو عنوان MAC هو E0.A397.78BD بالاتصال بالمنفذ Fa0/1



Switch(config)#interface fa0/1

switchport mode access Switch(config-if)#

switchport port-security Switch(config-if)#

Switchport port-security maximum 1 (هذه تعليمة افتراضية يمكن الاستغناء عنها)

Switchport portsecurity violation shutdown (هذه تعليمة افتراضية يمكن الاستغناء عنها)

Switch(config-if)# switchport port-security mac-address 00E0.A397.78BD

المهندس باسل دهيمش