بعد ان تم تناول العديد من المواضيع التي تخص سيرفرات و راوترات المايكروتك في الجزء الاول من هذا الكتاب نعود اليكم اليوم مع تكملة باقي اجزاء الدورة المتكاملة لإدارة الشبكات بأجهزة المايكروتك وسيضم الجزء الثاني من الكتاب الفقرات التالية:

١- كيفية محاكاة اجهزة المايكروتك في محاكي الشبكات الشهير (GNS3).
٢- الشبكات الخاصة الافتراضية (VPN) في المايكروتك.
٣- حجب مواقع معينة عن مستخدمي المايكروتك بعدة طرق.
٤- تقييد الدخول الى المايكروتك بمدير الشبكة فقط.
٥- استخدام اجهزة المايكروتك كبديل لأجهزة ال (TP-Link) في الشبكات المنزلية.
٦- بروتوكول التحكم بالجسور في المايكروتك.
٧- ادارة المستخدمين بواسطة مدير المستخدمين في المايكروتك.

اتمنى ان ينال الكتاب رضاكم ويلبي طموحاتكم وتوقعاتكم حول محتوياته وفائدتها وللمزيد من الدروس والشروحات حول المايكروتك وكل ما يخص الشبكات خصوصاً وعلم الحاسوب عموماً ستجدون الكثير في مدونتي على الانترنت على العنوان التالي:

www.mustafasadiq0.wordpress.com

ولا يفوتني الاشارة الى ان الكثير من هذه الدروس متوفرة ايضاً في مدونة الشبكات الاقوى والاروع في العالم العربي (مجموعة الشبكات) على الرابط التالي:

www.networkset.net

اترككم الان مع محتويات الكتاب واسألكم الدعاء لي ولوالدي ولكم الحرية المطلقة في نسخ كل او جزء من الكتاب ونشره مع ذكر او بدون ذكر المصدر فالهدف ليس الشهرة بين الناس وانما نشر العلم طاعة لله تعالى وامتثالاً لأوامره في نشر العلم بين مستحقيه.

شكراً لكم

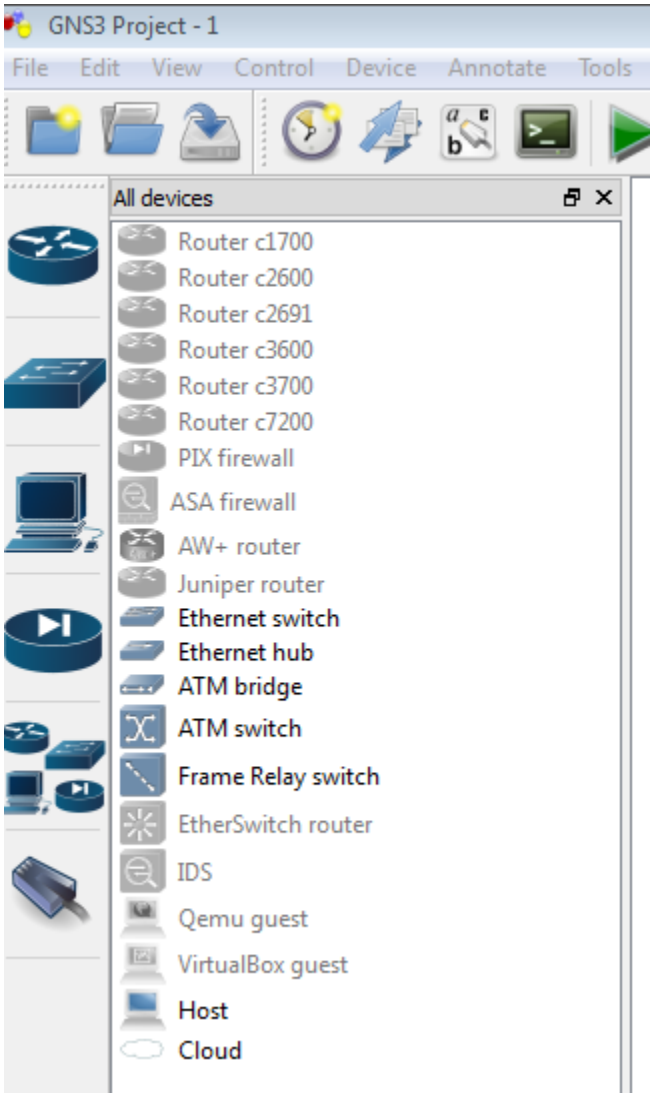
اخوكم مصطفى صادق لطيف – العراق

المايكروتك يتحدى المصاعب

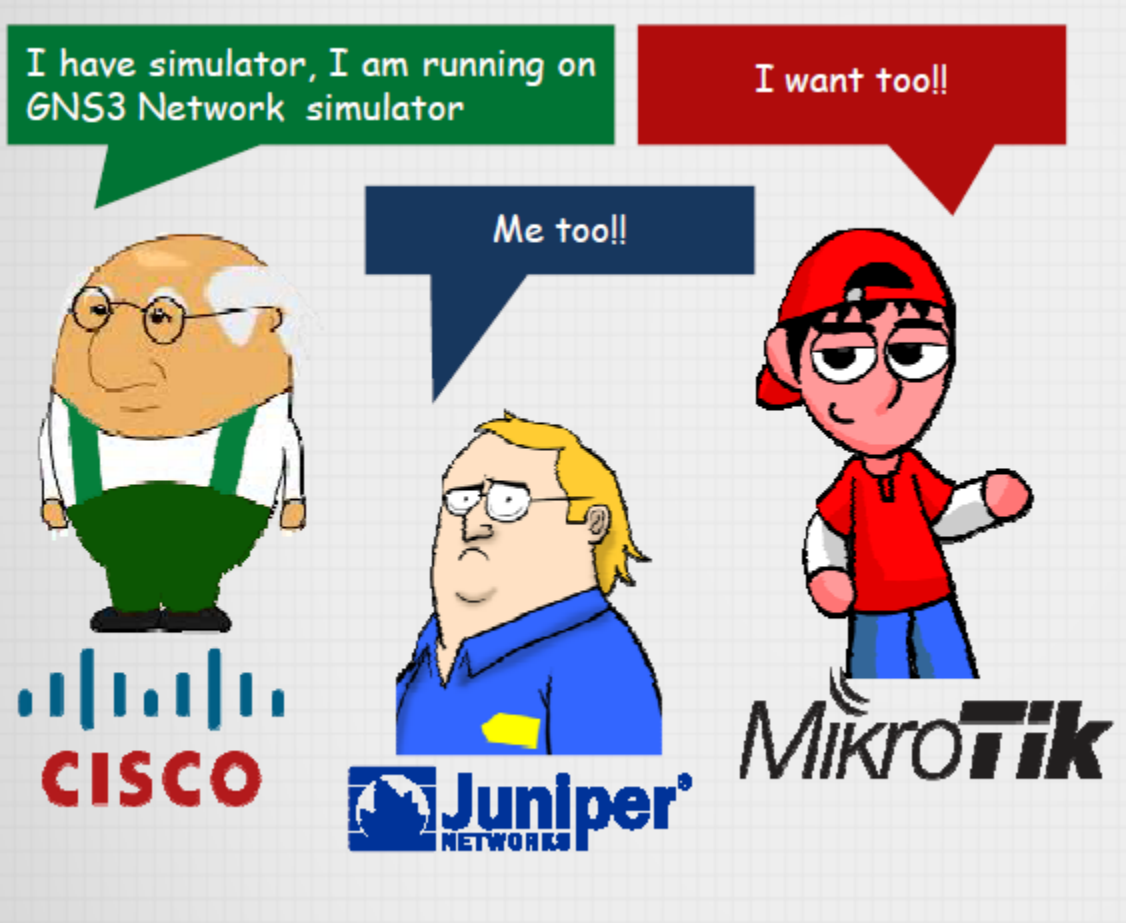
نعم انه يتحدى المصاعب ورغم صغر سنه وحداثة عهده وتكوينه مقارنة بشركات الشبكات الكبرى الاخرى مثل سيسكو وجونيبر الا انه يأبى الا ان يناطح الكبار وينافس في الصغيرة والكبيرة ويتقدم بخطى ثابتة الى الامام معطياً فكرة واضحة المعالم عن غدٍ اسهل لإدارة الشبكات بدون تعقيد اسطر الاوامر وبدون الحاجة الى حفظ الالاف من الايعازات في نظم تشغيل JUNOS و IOS لكل من اجهزة جونيبر وسيسكو وغيرهما وعلى الرغم من تشكيك الكثيرين بقدرة المايكروتك على الصمود في زمن الحوسبة السحابية (cloud computing) والعوالم الافتراضية (virtualization) والجيل الجديد من عناوين الانترنت (IPV6 next generation) الا ان الاصدارات الحديثة تتوالى من اجهزة هذا العملاق الصغير مثل سلسلة اجهزة (CCR1009 Mikrotik cloud core router) والاعلان بكل ثقة عن ان منتجات المايكروتك لا تتأثر بالفيروس الجديد القلب الدامي (Heart Bleed) كلها امور تجعلنا نعيد النظر في امكانية منافسة المايكروتك لبقية الشركات في التطبيقات الصغيرة والمتوسطة وبكلفة اقل واعدادات اسهل وامكانيات متقاربة وهو ما يبحث عنه أي مهندس شبكات في شركة محدودة ومتوسطة الدخل والدعم والصرف وكثيرة هي الشركات من هذا النوع.

والان ما سبب قولنا انه يتحدى المصاعب؟

وللجواب على ذلك نأخذ مثال يوضح المقصود فألى حد قريب كانت شركة سيسكو تمتلك محاكيها الاجمل والافضل (Cisco Packet Tracer) والذي استخدم بشكل كبير في تعليم وتصميم ومحاكاة الكثير من منتجات شركة سيسكو من راوترات وسويتشات وكذلك تشاركت كل من سيسكو وجونيبر وعدة شركات اخرى العمل والمحاكاة في محاكي الشبكات الرسومي الاوسع انتشاراً عالمياً (GNS3 Graphical Network Simulator) كما في الصورة التالية:



ولم يكن للمايكروتك من وسيلة لمحاكاة شبكاته وعمل اجهزته الا من خلال الماكنة الافتراضية في الحواسيب الشخصية (Virtual Machine) حيث يتم تنصيب نظام تشغيل المايكروتك في الماكنة الافتراضية والعمل على الجهاز من خلال الويندوز في الجهاز الاصلي الحقيقي ولما كانت هذه الطريقة غير كافية لاختبار اداء شبكة كاملة ولا تحقق امكانية تصميم واختبار شبكة متنوعة ومتكاملة لمنتجات عدة شركات في نفس الوقت فقد قام خبراء الشبكات والمحاكيات بخطوة كبيرة الى الامام بالاستعانة بعدة برامج لإدخال المايكروتك في فريق العمل بداخل ال (GNS3) ولسان حالهم في الصورة التالية:



والغاية من ذلك كما ذكرنا تسهيل محاكاة عمل الشبكات المتكونة من اجهزة مايكروتك حيث ان انشاء شبكة تتكون من ٨ روترات مايكروتك مكلف للغاية عملياً ولكن بالشرح الذي سنشرحه ستكون العملية اكثر سهولة واقل كلفة واضمن نتيجة ان شاء الله.

لماذا نحتاج الى المحاكاة وبرامج المحاكيات؟

بأختصار وبعد كل ما قيل: اختبار الوظائف الجديدة وتصميم شبكات تجريبية قبل الاضطرار الى شراء اجهزتها فعلياً وللأغراض التعليمية.

ادوات التجربة (احتياجات العمل):

١- برنامج المحاكي (GNS3) ويمكن تنزيله من رابط الشركة التالي: www.gns3.net

٢- برنامج (QEMU): ويسمى ايضاً المحاكي السريع (Quick Emulator) ويستخدم عادة لمحاكاة جهاز كامل او جهاز حاسوب بشكل ادق ويمكن تنزيله من رابط الشركة التالي: www.qemu.org.

٣- ملف ايزو لنظام المايكروتك (Mikrotik ISO file) وهو الملف التنصيبي الذي يمكن تنزيله من موقع الشركة ويكون جاهز للتنصيب على أي جهاز حاسوب (فيزيائي او افتراضي) وتتوافر العديد من المستويات له على حسب الامكانيات المتاحة لها وعلى حسب المبلغ المدفوع لقائها وتتدرج من المستوى صفر الى المستوى ٦ ويمكن تنزيلها من رابط الشركة المعروف www.mikrotik.com/download.

جدير بالذكر ان المايكروتك يمكن محاكاة عمله كما ذكرنا سابقاً بأستخدام الماكنة الافتراضية وبرنامج ال (Winbox) او بأستخدام الطريقة التي سنشرحها والتي تعتبر الافضل والاكفأ كما سنرى.

اضافة المايكروتك الى ال (GNS3)

نقوم بخلق ملف جديد في القرص سي ونسميه (mikrotik) ونضع بداخله ملف ال (qemu) الذي قمنا بتنزيله وفك ضغطه وكذلك نضع بداخله نسخة الايزو للمايكروتك (mikrotik.iso) ثم نقوم بفتح سطر الايعازات في الويندوز (command prompt) ونكتب الايعازات التالية:

```
C:\ cd mikrotik
C:\mikrotik>Qemu-img.exe create mikrotik.img –f qcow2 256M
```

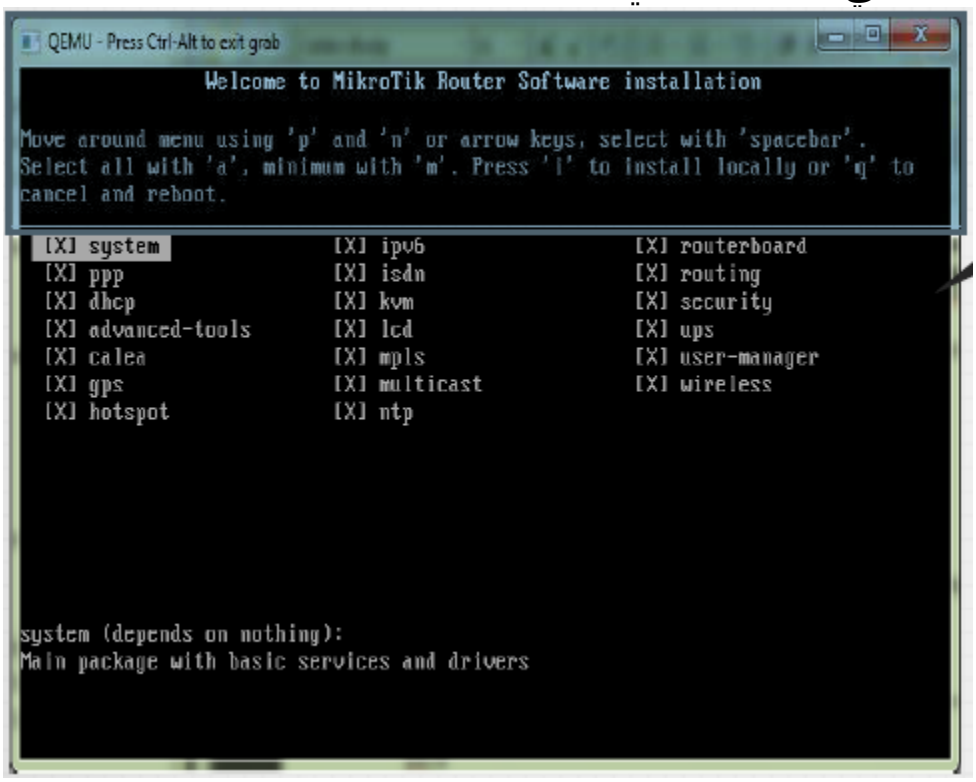
فيتم انشاء صورة افتراضية للمايكروتك في داخل المجلد الذي قمنا بأنشائه وتظهر رسالة نجاح ذلك كالاتي:

```
Formatting 'mikrotik.img', fmt=qcow2 size=268435456 encryption=off cluster_size=0
```

والان نكتب الايعاز التالي:

```
C:\mikrotik>qemu.exe mikrotik.img –boot d –cdrom "mikrotik-6.12.iso"
```

حيث ان (mikrotik-6.12) هو اسم ملف الايزو الذي قمنا بتنزيله لنظام تشغيل المايكروتك والان سيقوم ال(Qemu) بتنصيب المايكروتك وبنفس الطريقة التقليدية كما في النافذة التالية:

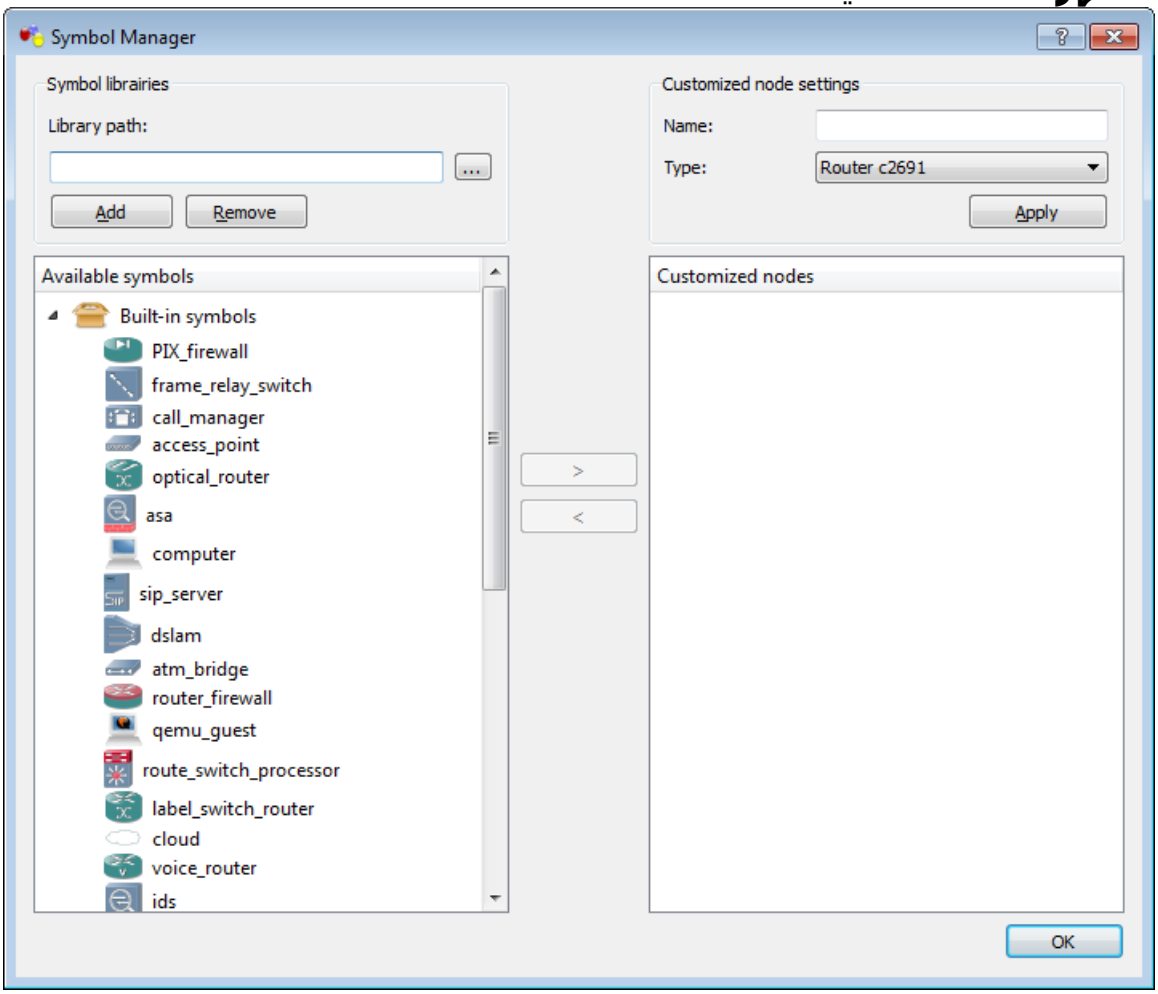


وبعد اكتمال التنصيب نغلق نافذة (qemu) ونعود الى نافذة الدوز ونكتب:

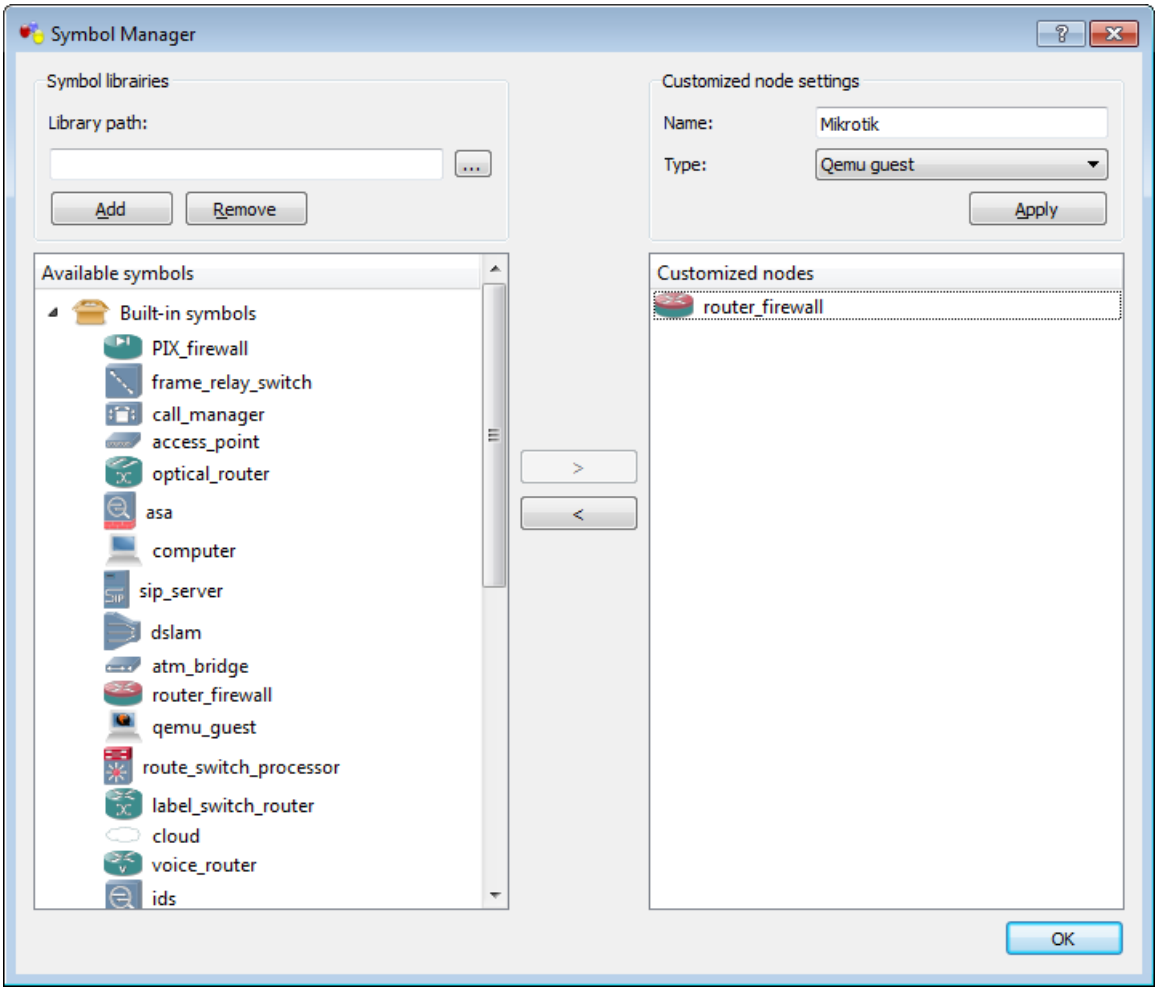
```
C:\mikrotik>qemu.exe mikrotik.img –boot c
```

لتظهر نافذة بدء عمل المايكروتك فنقوم بأدخال الايعاز التالي (System shutdown) ثم (yes) ونقوم بأغلاق نافذة ال(qemu).

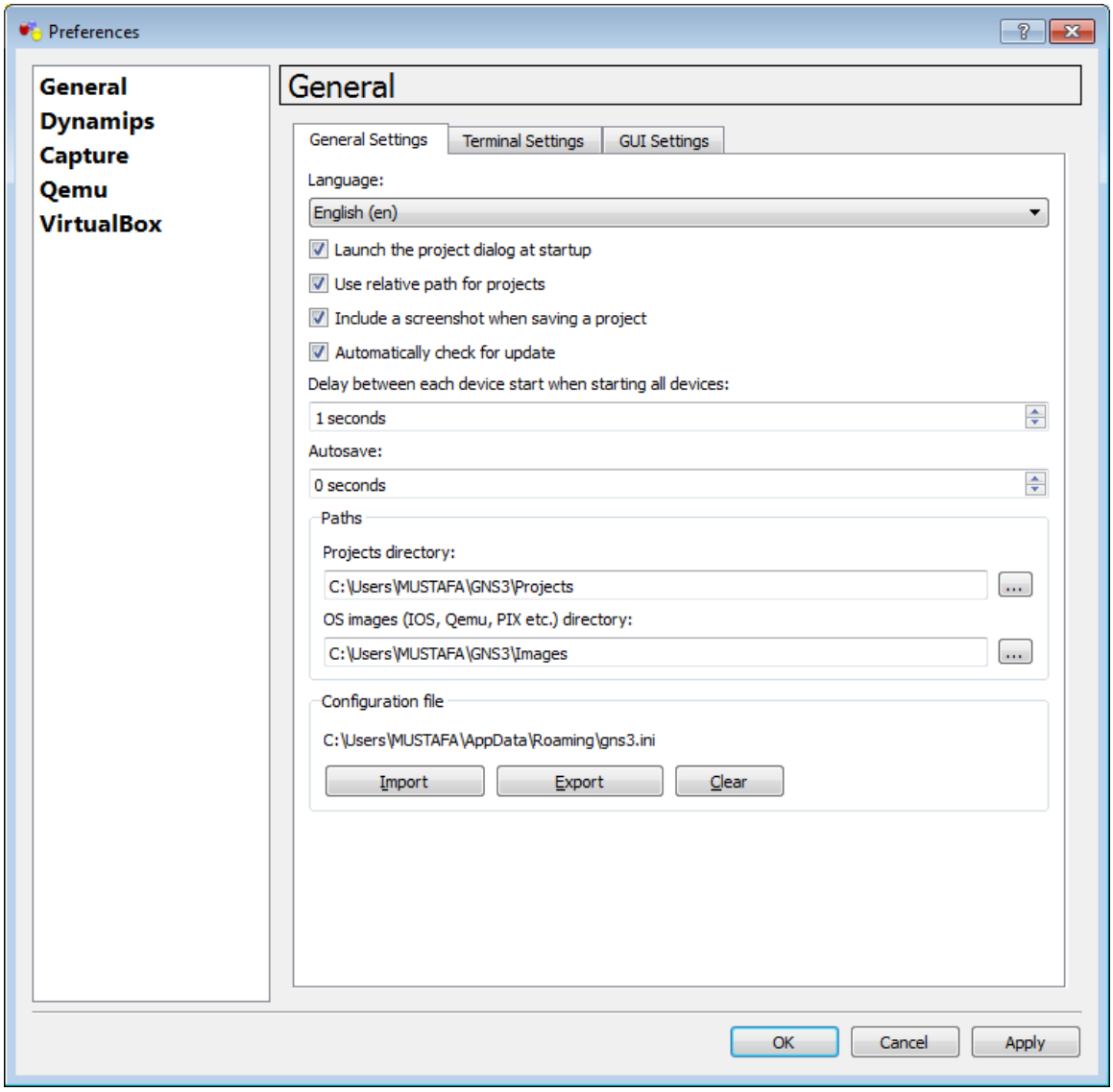
والان نقوم بفتح برنامج ال (GNS3) ونذهب الى قائمة (edit) ثم (symbol manager) لتظهر النافذة التالية:



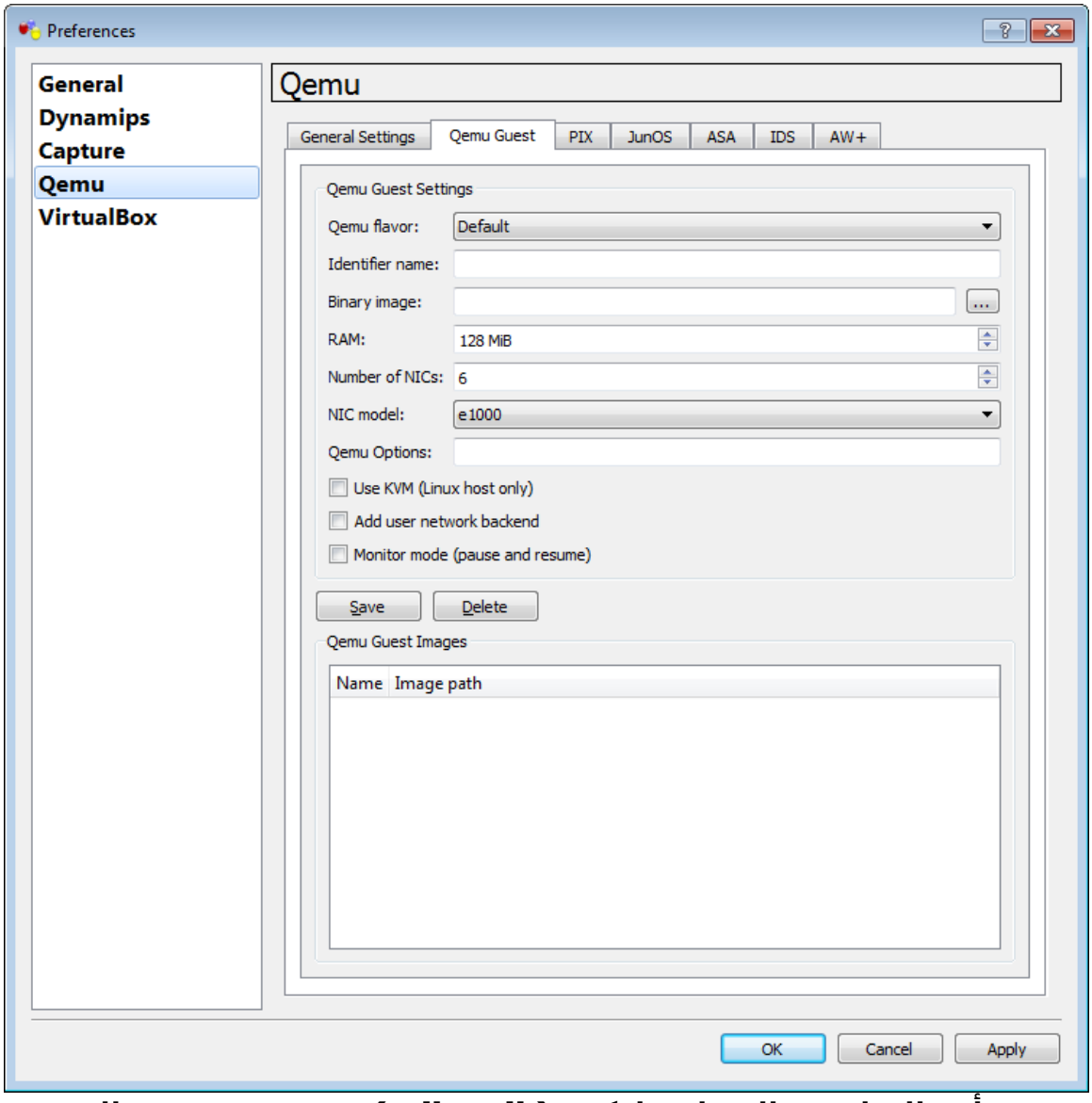
نختار اي من الاجهزة قليلة الاستخدام وليكن (router firewall) وننقر على السهم في منتصف النافذة لأضافته الى الجانب الايمن



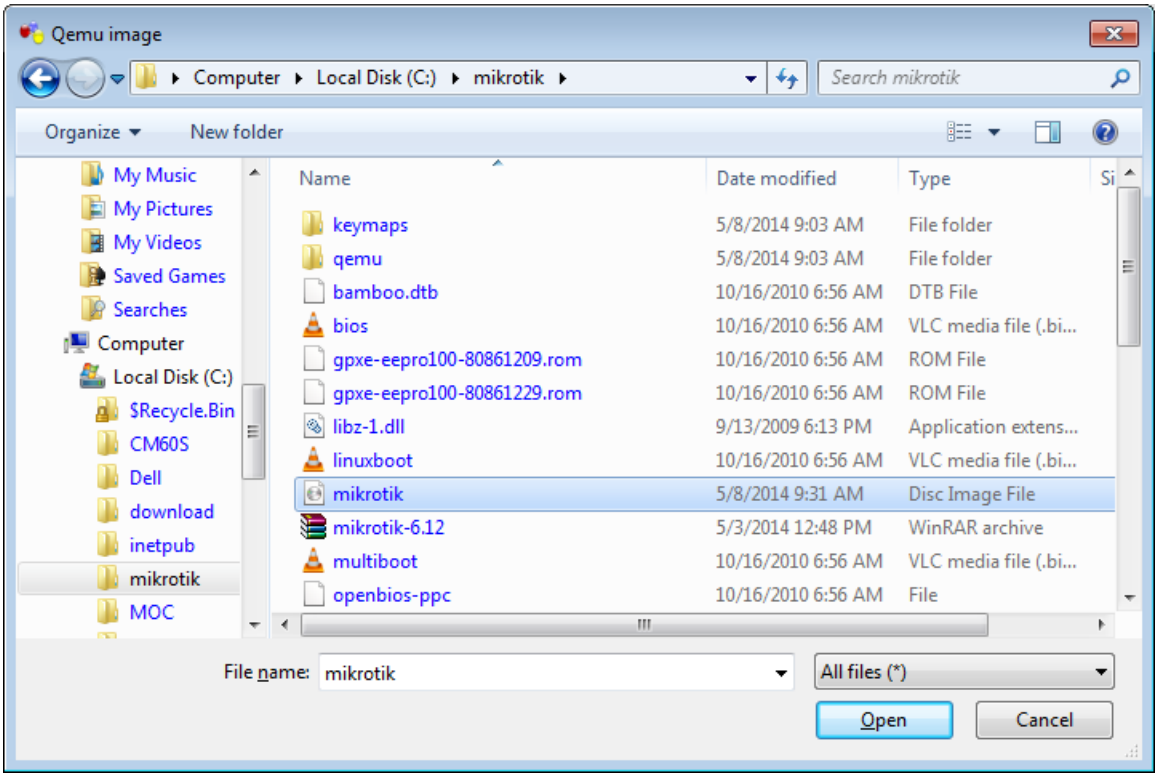
ونعطيه اسم وليكن (mikrotik) ونحدد نوعه (qemu guest) ثم (Apply) ثم (ok).
والان نذهب الى قائمة (edit) ونختار (preferences) لتظهر النافذة التالية:



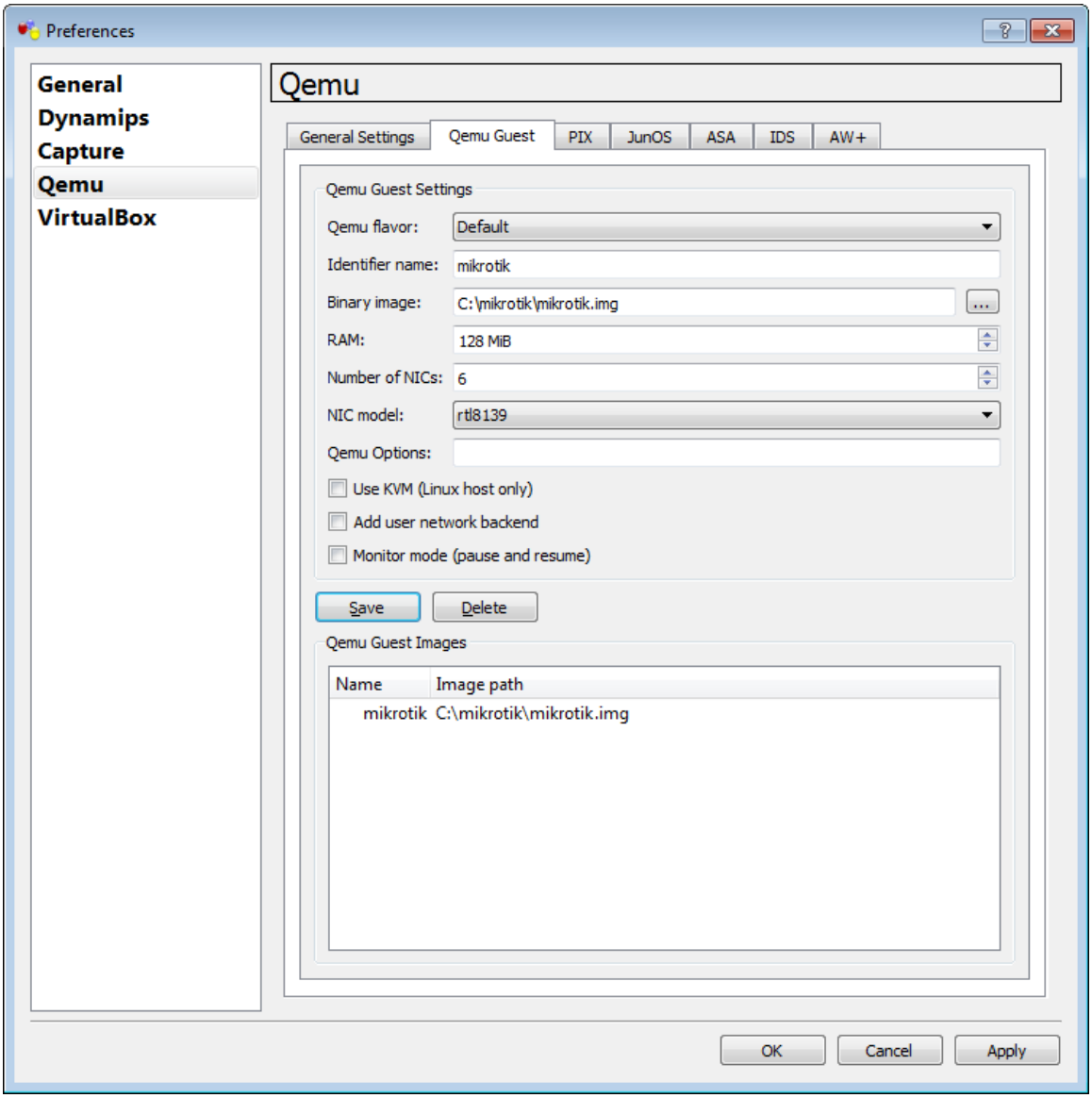
نذهب الى (qemu) ثم (qemu guest) لتظهر النافذة التالية:



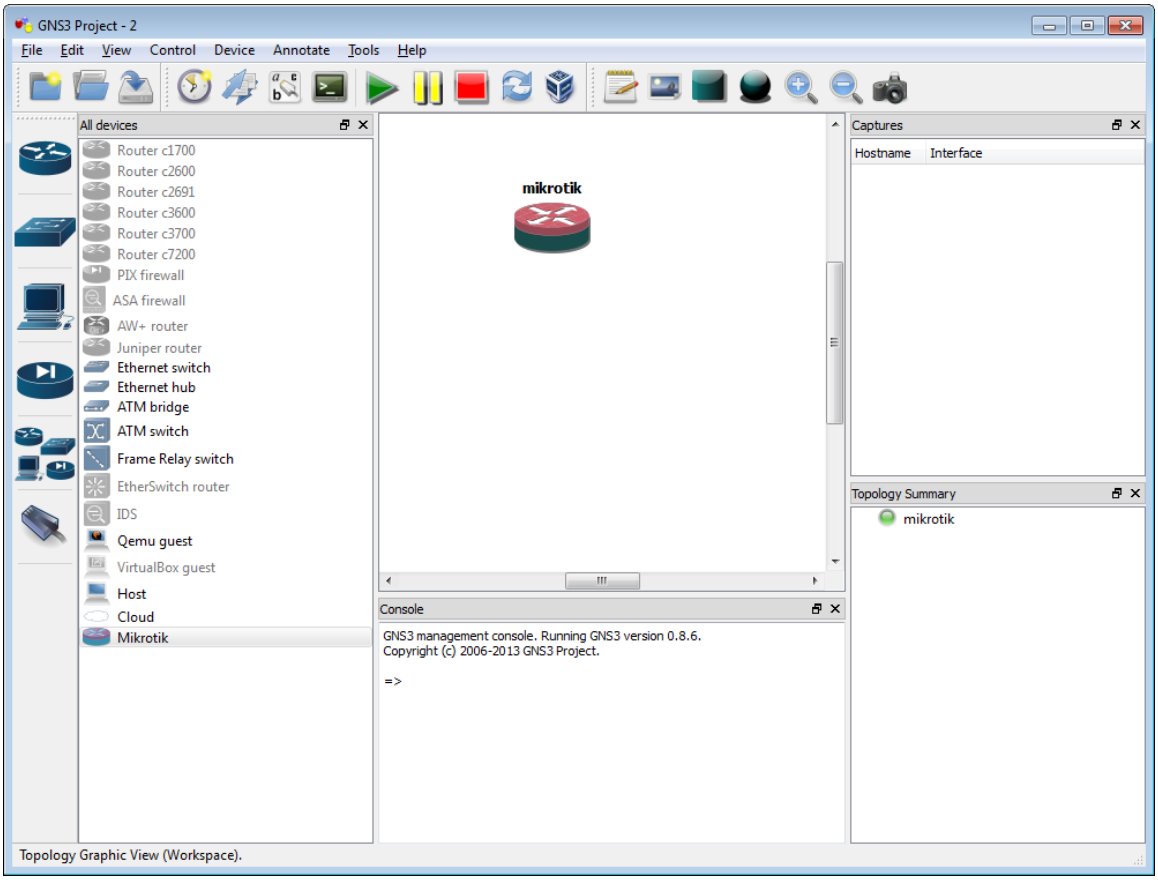
نقوم بأدخال اسم الجهاز وليكن (mikrotik) ونقوم بتحديد الصورة الثناية (binary image) كما في النافذة التالية:



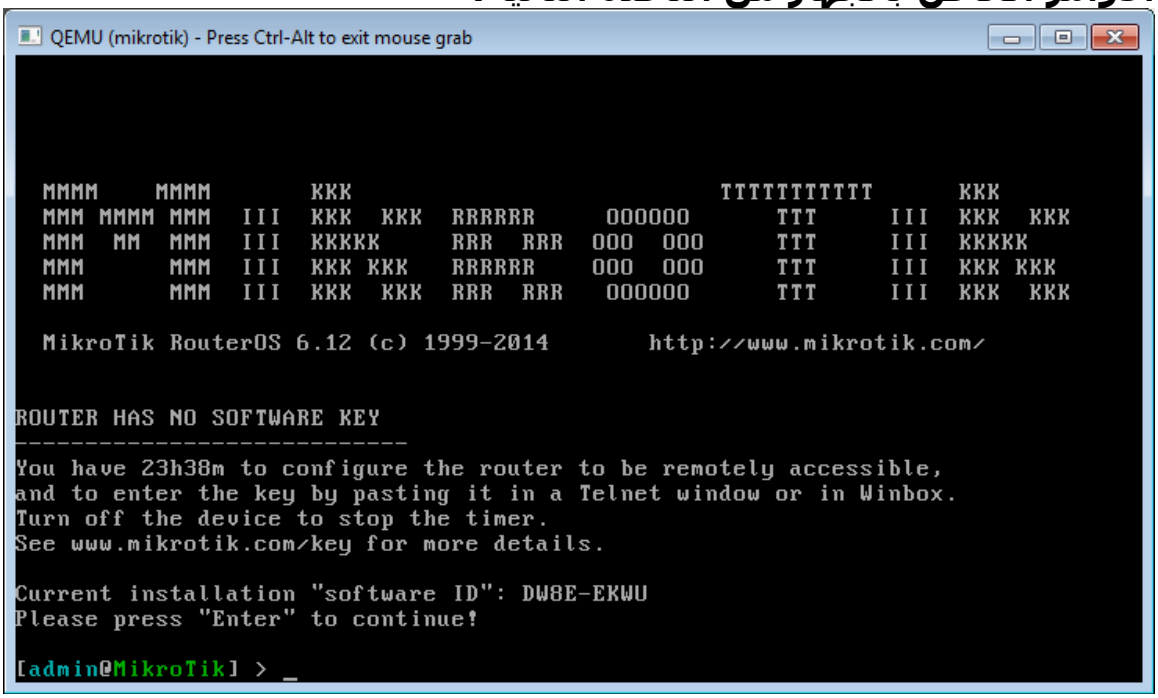
ونحدد مقدار الذاكرة (RAM) وعدد المنافذ المقترحة للجهاز ونوع كرت الايثرنت وننقر على (save) ثم (Apply) وكما في النافذة التالية:



والان نجد ان المايكروتك كجهاز قد اضيف الى قائمة الاجهزة التي يمكن محاكاتها في ال (GNS3) فنختاره بالسحب والافلات الى نافذة المحاكاة وكما في النافذة التالية:



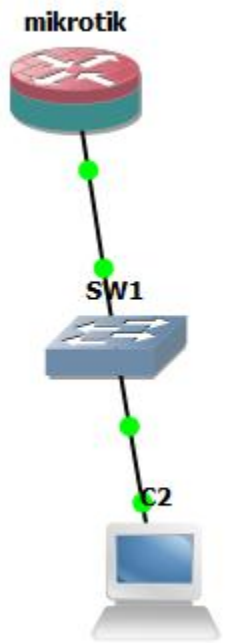
ولبدء عمله قبل او بعد ربطه ننقر على ايقونته نقرة يمين ونختار (Start) لتظهر نافذة (qemu) تطلب (user name and password) للجهاز فندخلها ونبدأ العمل على سطر الاوامر الخاص بالجهاز من النافذة التالية:



الى هنا ينتهي درس اليوم على امل اللقاء بكم في درس اخر لشرح كيفية ربط شبكة مايكروتك متكاملة في هذا المحاكي وضبط اعداداتها واختبار ادائها.

المايكروتك يتحدى المصاعب ٢

بعد ان توصلنا في الجزء الاول من هذا المقال الى كيفية محاكاة المايكروتك في المحاكي الشهير (GNS3) نأتي اليوم لنتحدث عن كيفية التعامل مع هذا الجهاز الذي ربطناه في شكل مشابه للتالي:



ولكن كما نعرف فأن المايكروتك لا يمكن التعامل معه بشكل مباشر الا عن طريق نافذة الاوامر (command terminal) والتي تتطلب من مدير الشبكة حفظ ومعرفة الكثير من الايعازات او الاستعانة بدليل مستخدم او كتاب مرجعي لإيعازات المايكروتك بشكل مشابه لما يحصل في انظمة تشغيل اجهزة سيسكو وجونيبر الامر الذي لا يفضله الكثير من مستخدمي المايكروتك الذين يبحثون عن البساطة في التعامل والادارة عن طريق الاداة الشهيرة (winbox) ولكن كيف نستطيع الدخول الى المايكروتك عن طريق هذه الاداة في بيئة محاطي الشبكات (GNS3)؟

هذا ما سنجيب عنه في درسنا اليوم:

كما قلنا سابقاً فأن محاكي الشبكات الذي نعمل عليه يتميز بمرونة كبيرة تسمح له ان يربط شبكة بداخله ويعبر حدوده ليربط شبكته بحاسوبنا الشخصي الذي نعمل عليه!

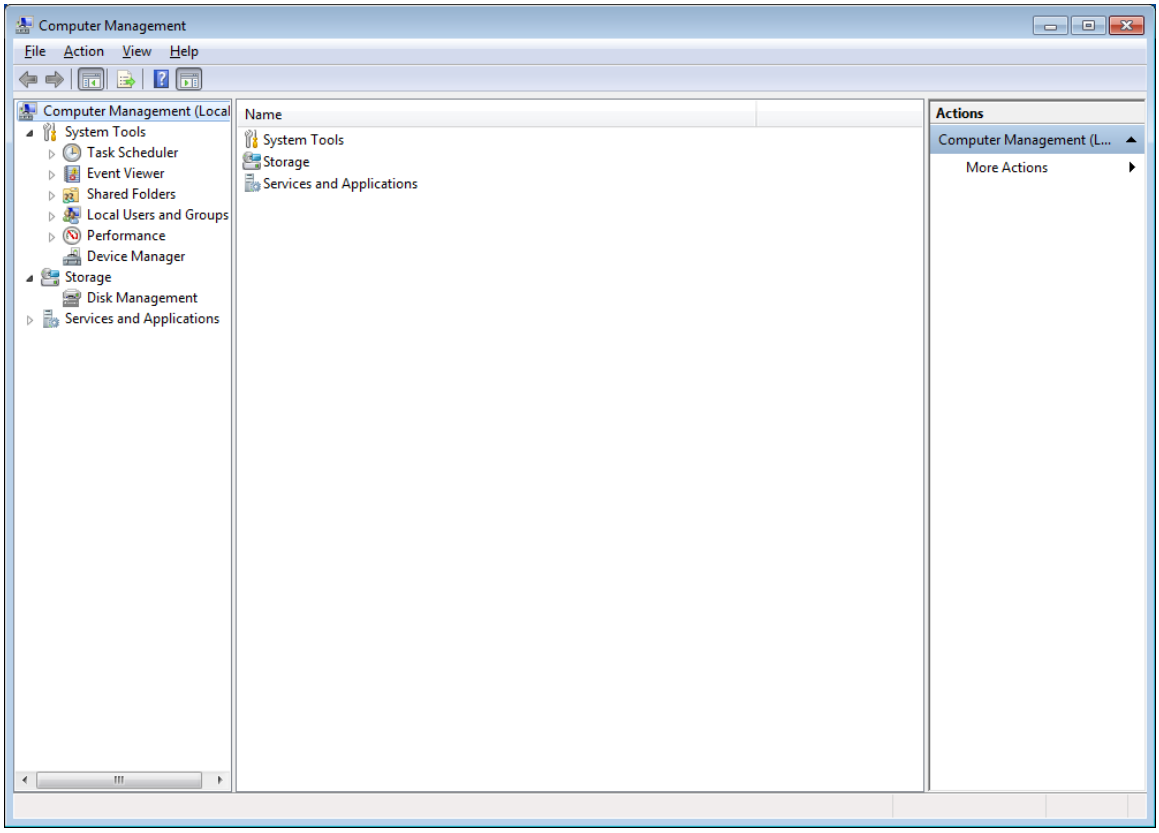
كيف هذا؟

نعم انه يربط شبكة افتراضية بداخل حاسوب ويعتبر هذا الحاسوب نفسه جزءاً من تلك الشبكة!

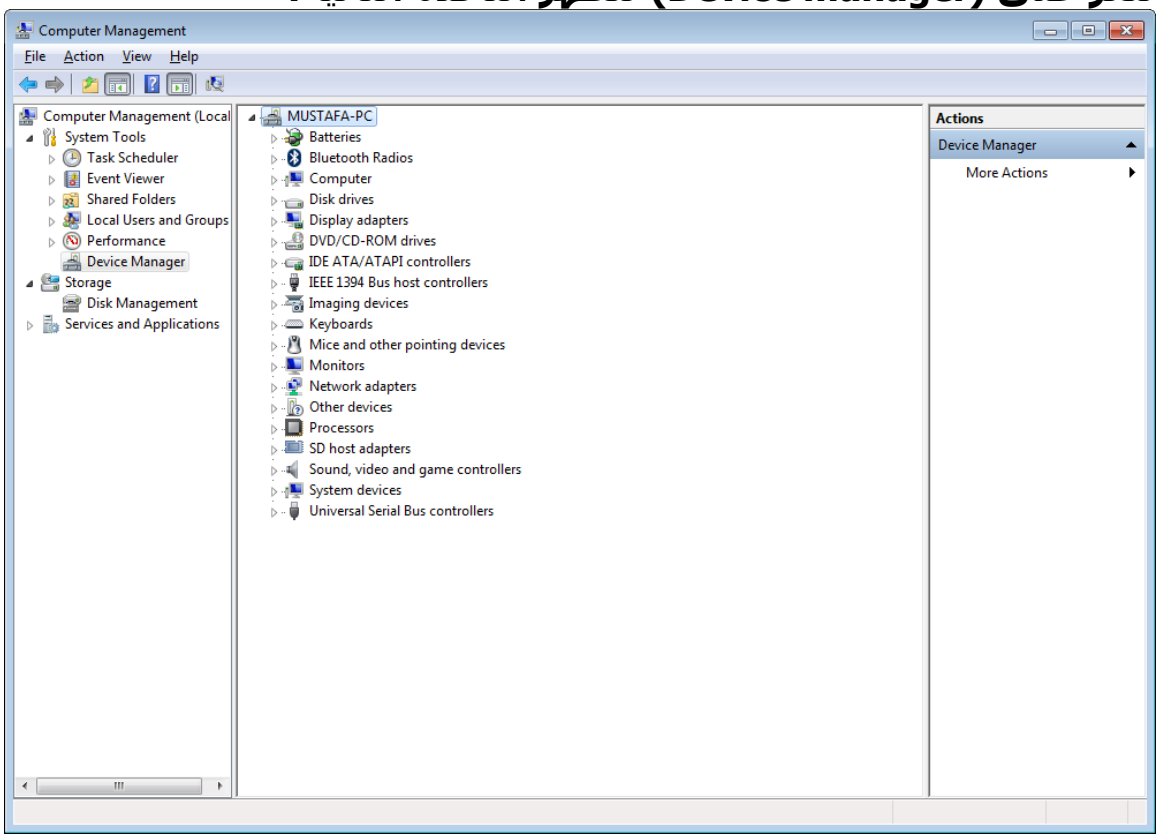
ولكن كيف يتم ذلك؟

عن طريق ما يسمى (loop back adapter) وهو كرت شبكة افتراضي نقوم بإضافته الى حاسوبنا الشخصي لكون حلقة الوصل بين الحاسوب والشبكة داخل الى (GNS3) وكما يلي:

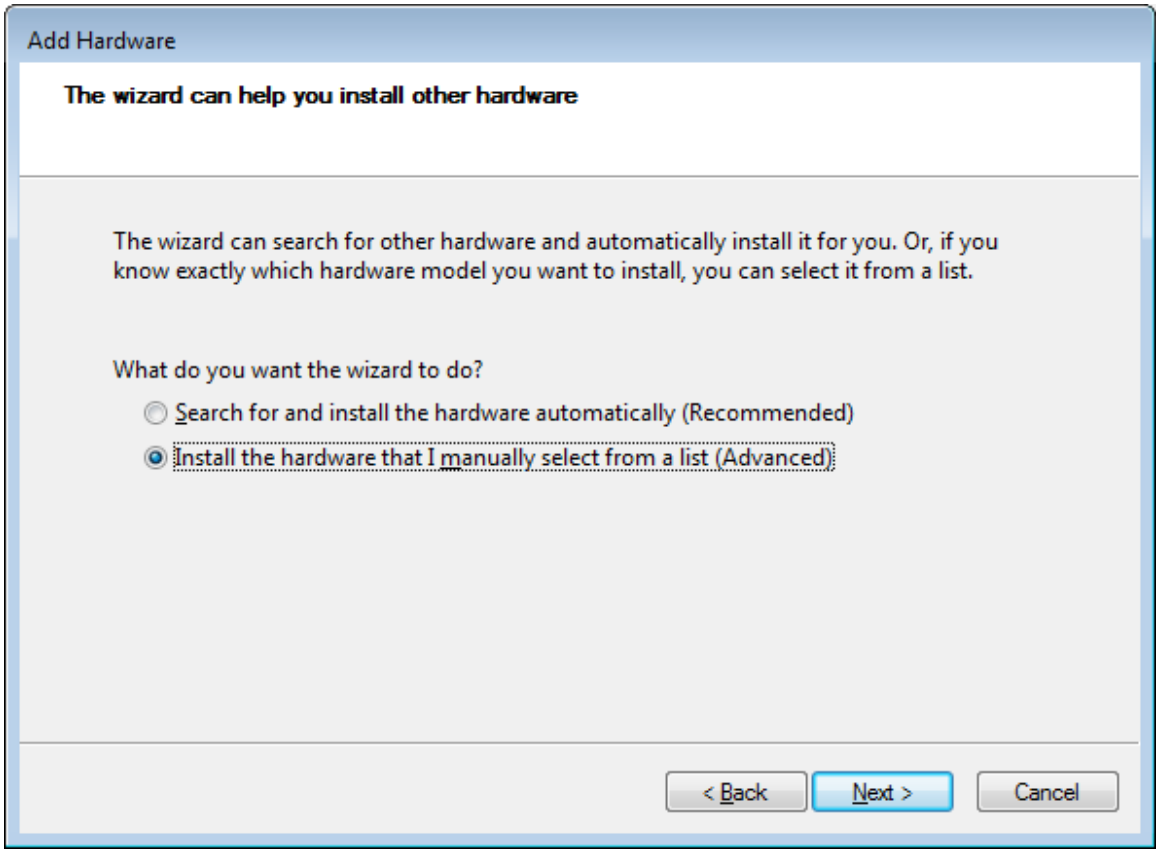
نقوم بفتح مدير الاجهزة (device manager) عن طريق النقر الايمن على ايقونة جهاز الكومبيوتر لتظهر نافذة مشابهة لما يلي:



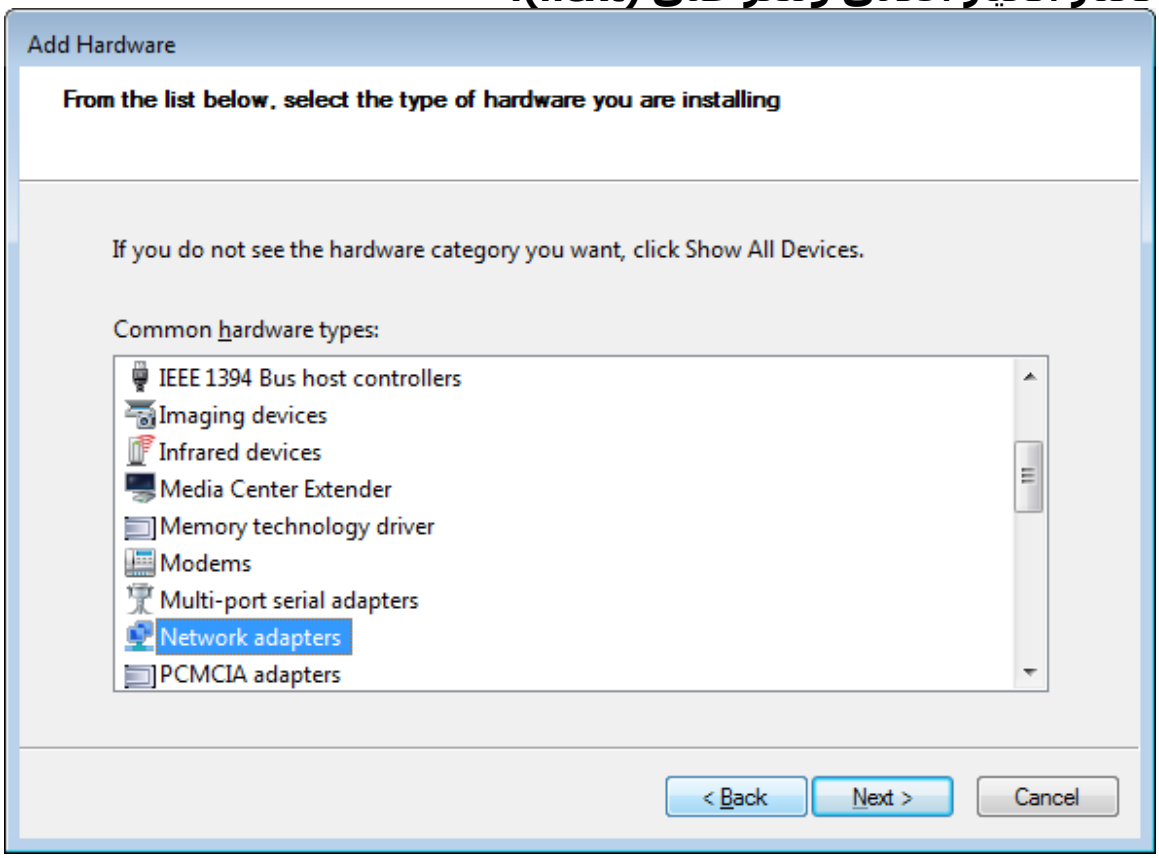
ننقر على (Device manager) لتظهر النافذة التالية:



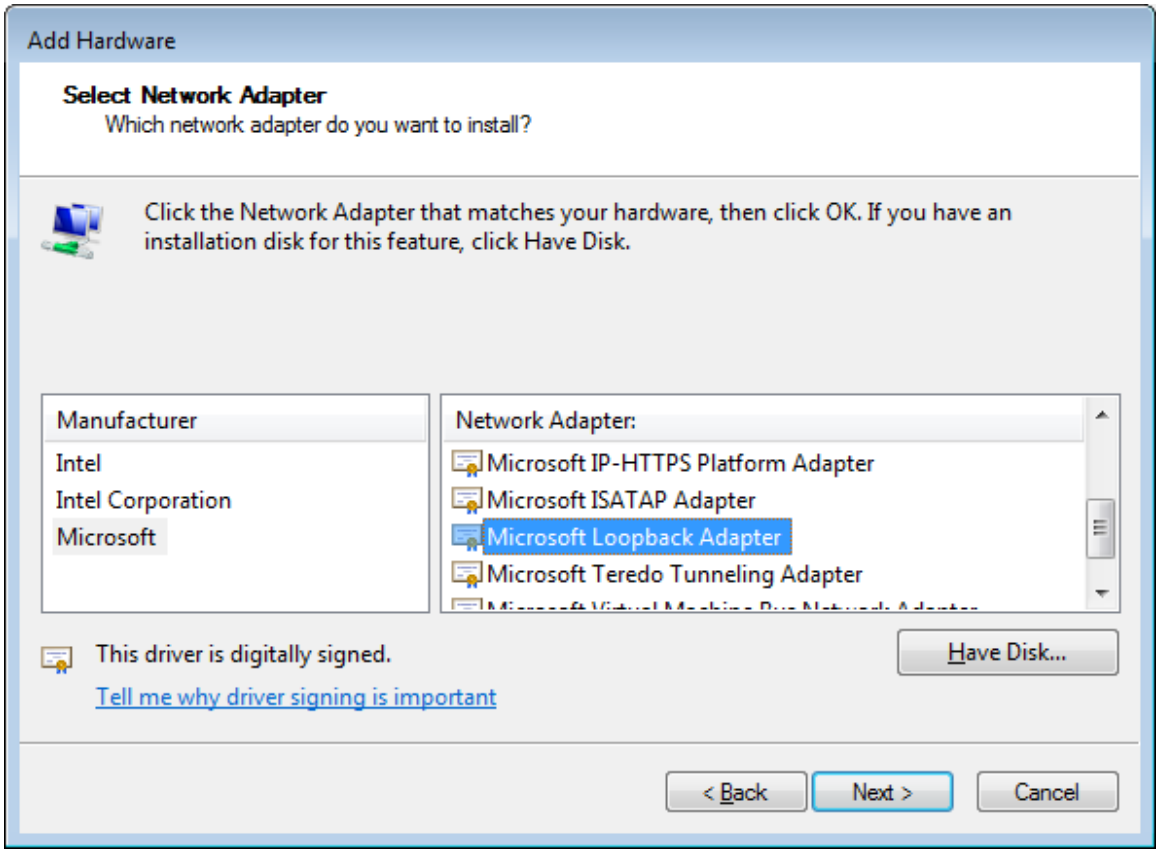
ننقر على اسم الكومبيوتر نقرة ماوس ايمن ونختار (Add legacy hardware) لتظهر نافذة اضافة جهاز جديد فننقر على (next) لتظهر النافذة التالية:



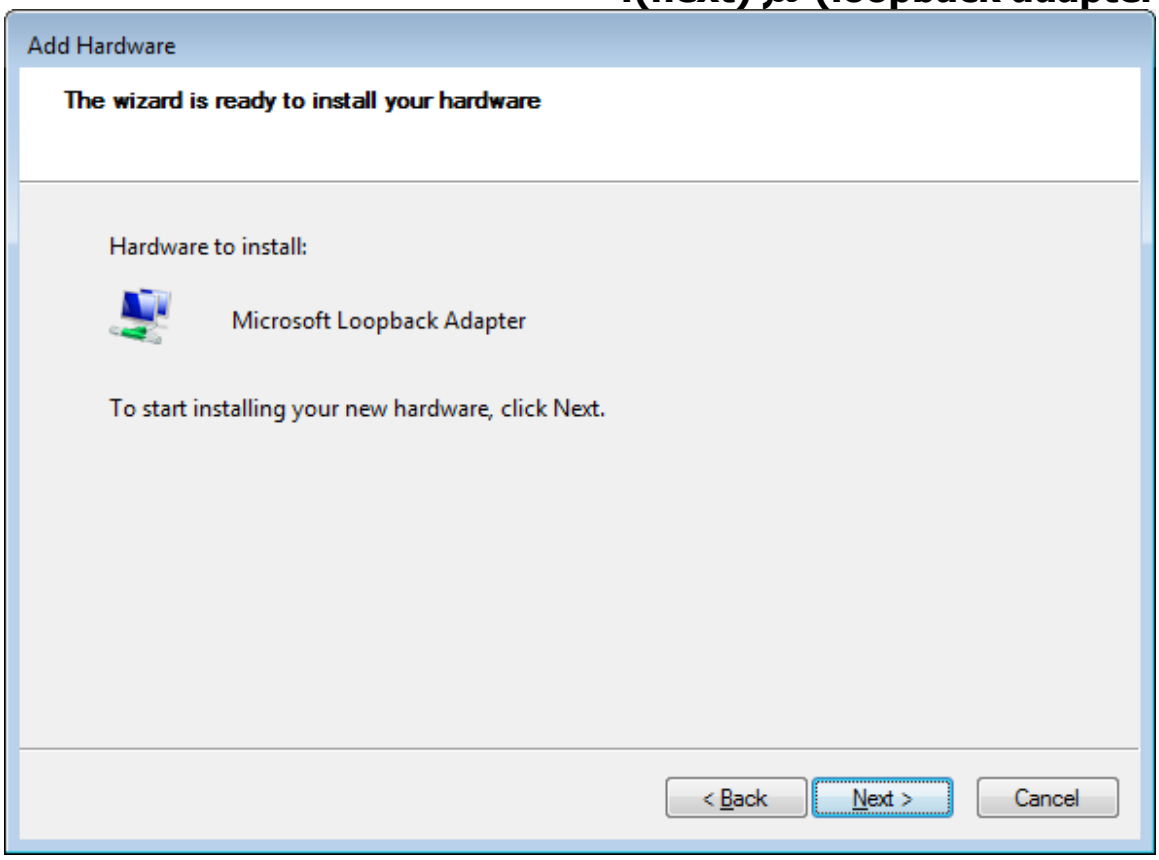
نختار الخيار الادنى وننقر على (next):



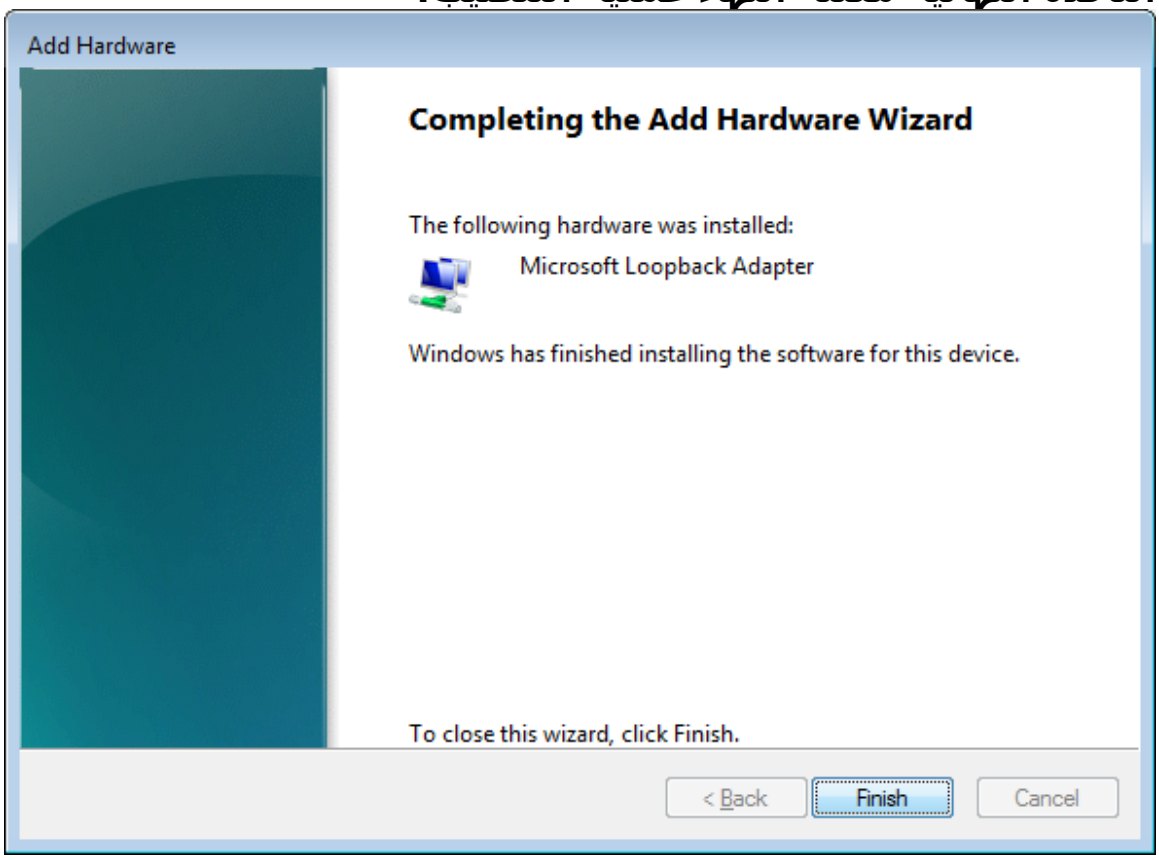
تظهر النافذة اعلاه فننقر نقرة مزدوجة على (network adapters) لتظهر النافذة التالية:



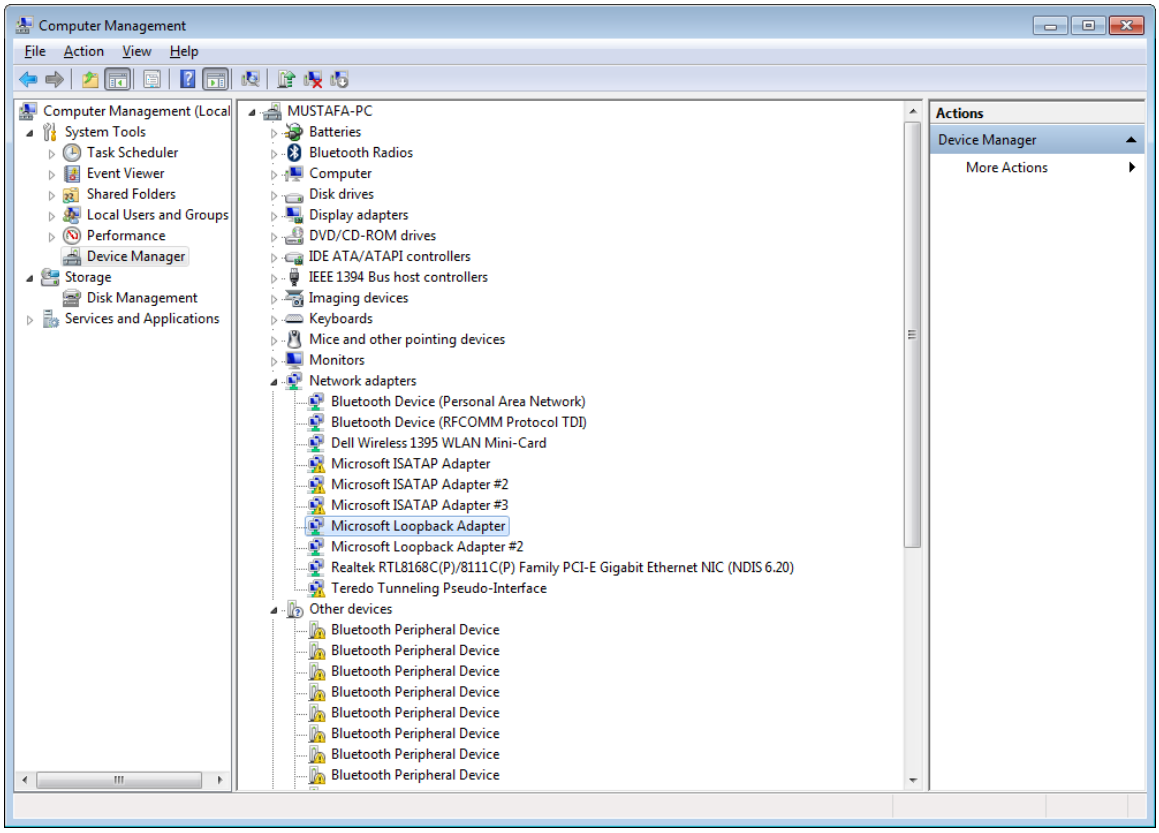
نختار من النافذة اعلاه المصمم (Microsoft) وكرت الشبكة من نوع (Microsoft loopback adapter) ثم (next):



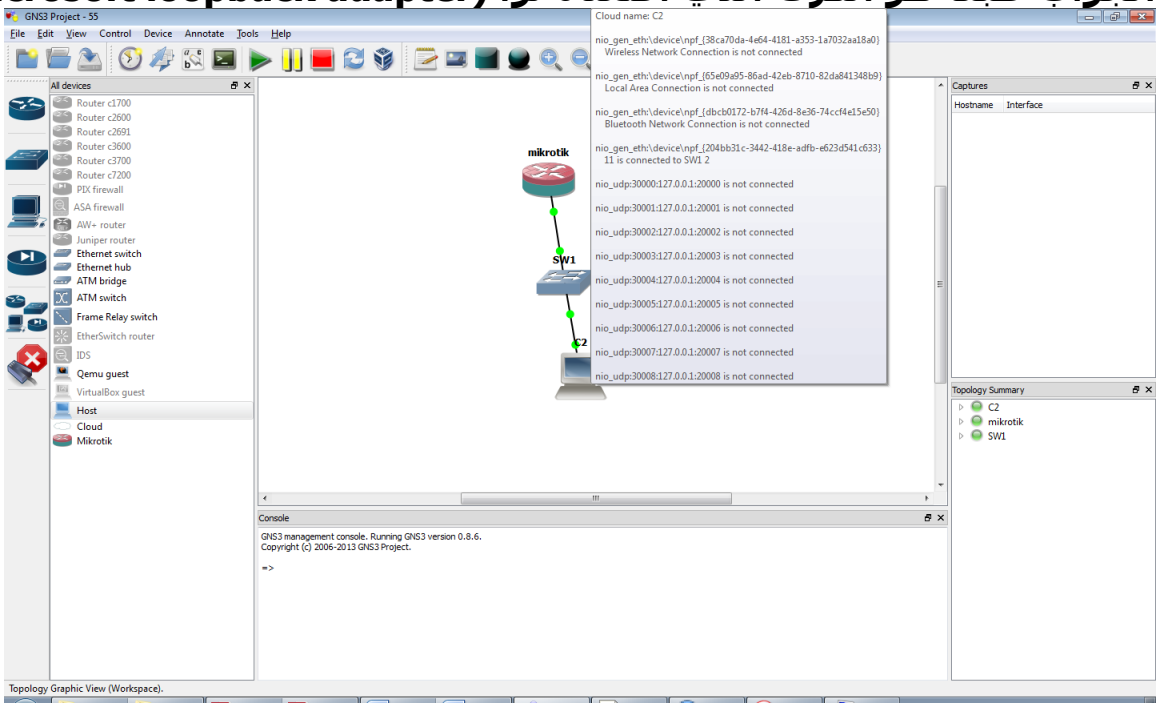
تظهر النافذة اعلاه لتعلن قرب تنصيب الكرت المطلوب وكلما علينا فعله هو النقر على (next):
تبدأ عملية التنصيب التي لا تحتاج أي مكونات او اقراص اضافية فكل ما تقوم به هو تفعيل احد مكونات الويندوز الموجودة مسبقاً والتي لا تعمل الا بهذه الطريقة لتظهر النافذة النهائية معلنة انتهاء عملية التنصيب:



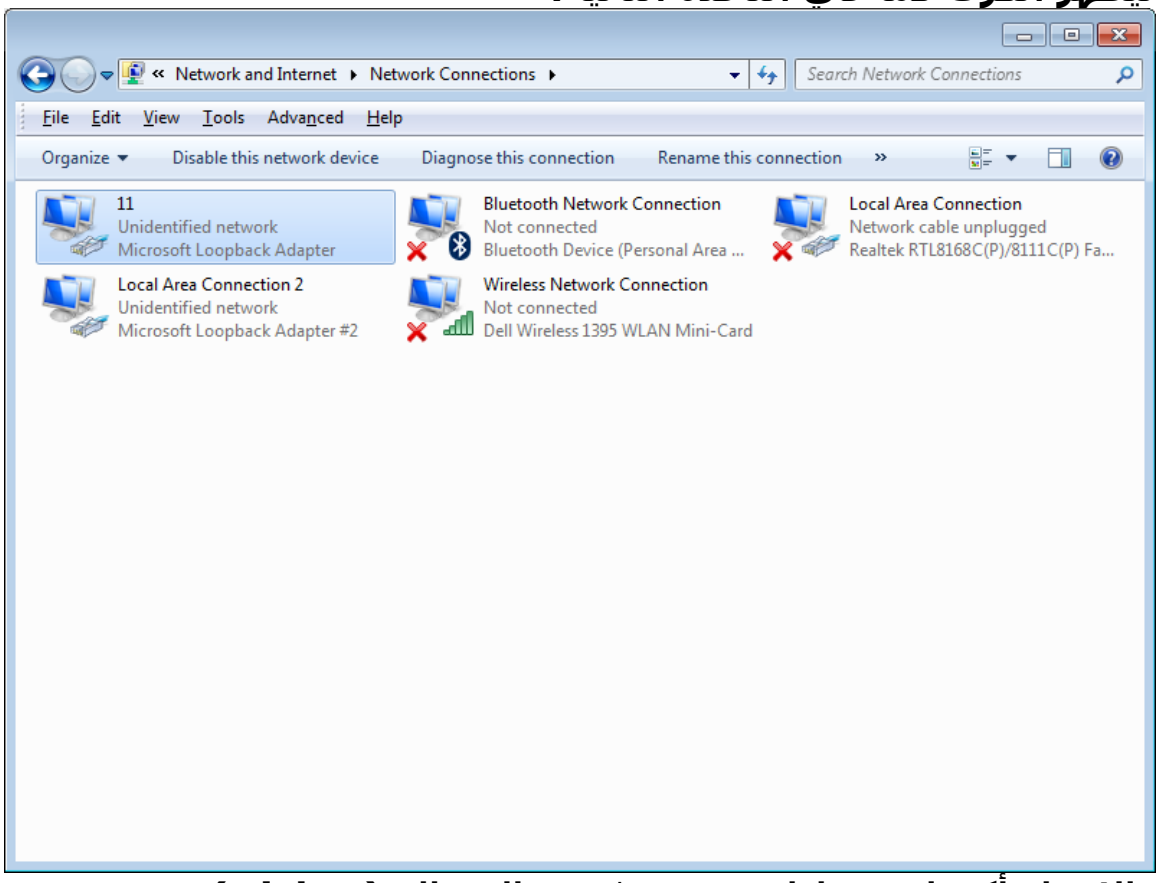
والان نذهب الى نافذة مدير الاجهزة لنجد ان كرتنا قد تمت اضافته وكما يلي:



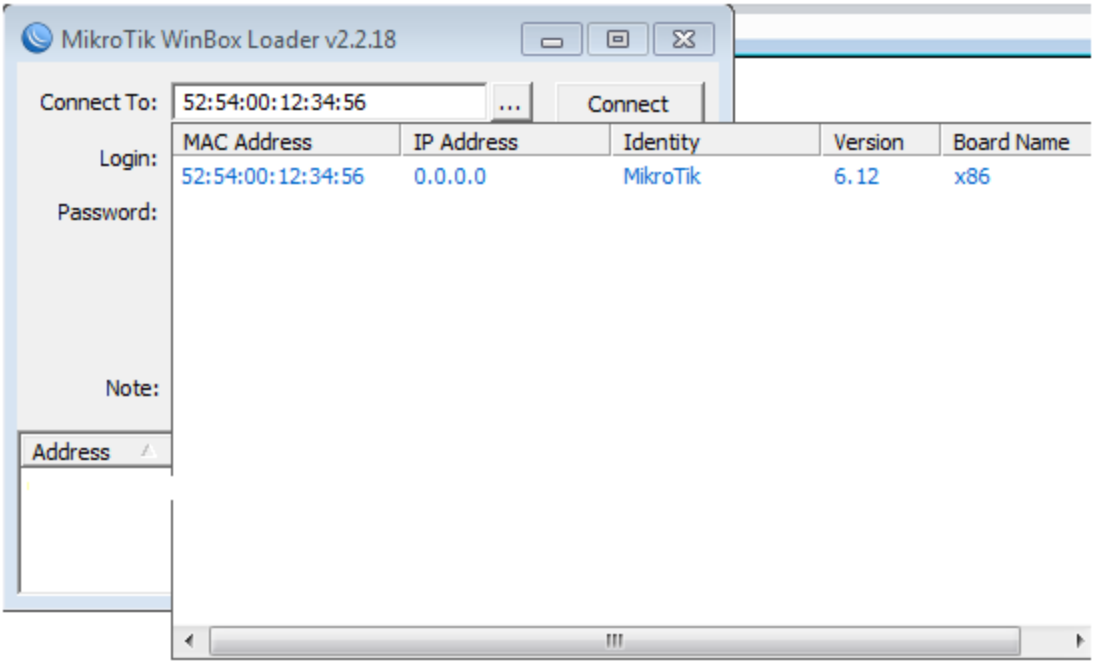
والان نذهب الى ال (GNS3) ونربط الشبكة المبينة في اول صورة في الدرس وننقر على المثلث الاخضر لبدء تشغيل الشبكة فتظهر نافذة ال (QEMU) الخاصة بالمايكروتك وتظهر الاوامر التي تطلب ادخال اسم المستخدم وكلمة المرور والتي تكون تلقائياً وقبل التغيير (UN: admin) وكلمة المرور فارغة وهنا تبرز النقطة المهمة وهي أي من كروت الحاسوب (Host) هي التي نربطها الى السويتش؟
الجواب طبعاً هو الكرت الذي اضفناه تواً (Microsoft loopback adapter) وكما يلي:



فنلاحظ هنا اننا ربطنا الكرت (١١) الى السويتش ولكن ما هو الكرت (١١)؟
انه كرت اللوب باك الذي اضفناه قبل قليل بعد ان اعدت تسميته في حاسوبي الى الاسم (١١) ولكن كيف عرفته؟
من خلال الذهاب الى صفحة ادارة كروت الشبكة في الحاسوب بأتباع الخطوات:
Start→ network → network and sharing center → change adapter settings →
ليظهر الكرت كما في النافذة التالية:



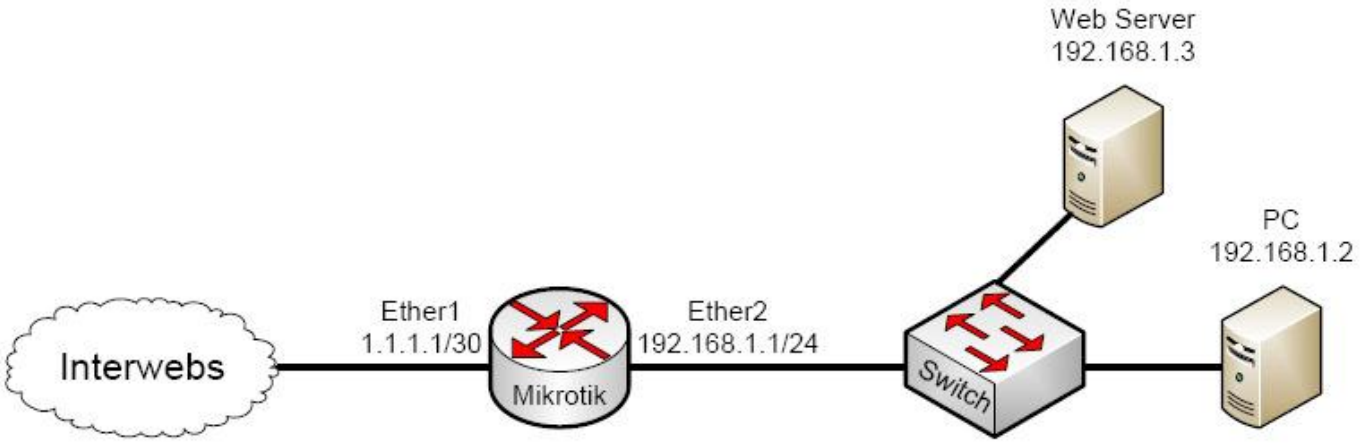
والان لنتأكد ان عملنا صحيح نذهب الى ال (winbox) ونفتحه ونقوم بالبحث على اجهزة مايكروتك في شبكتنا (حاسوبنا الشخصي) فيظهر لنا الجهاز المربوط في الشبكة الافتراضية داخل برنامج المحاكاة كما في ادناه:



فنكتب اسم المستخدم (admin) وكلمة المرور فارغة وندخل الى ال (Winbox) لنقوم بأي شيء نريده لإدارة الشبكة.

الشبكة الخاصة الافتراضية في المايكروتك (VPN in Mikrotik)

سبق ان قمنا بشرح مفهوم الشبكة الافتراضية وكيف انها تستخدم لتأمين الاتصال عبر بيئة مفتوحة سلكية او لا سلكية بين نهايتين متباعدتين بشكل امن ومستقل بعيداً عن التجسس ومحاولات الاختراق والاطلاع على البيانات وتستخدم هذه الشبكات مفهوم الاتصال النفقي (Tunnel Communication) والذي تم شرحه ايضاً في درس سابق وسيكون تركيزنا اليوم على كيفية تطبيق تلك المفاهيم النظرية على شبكة تستخدم منتجات المايكروتك وللنموذج الافتراضي المبين في الصورة التالية: علماً ان هذا النموذج يمكن توسيعه الى شبكة اكبر وبنفس الاعدادات:

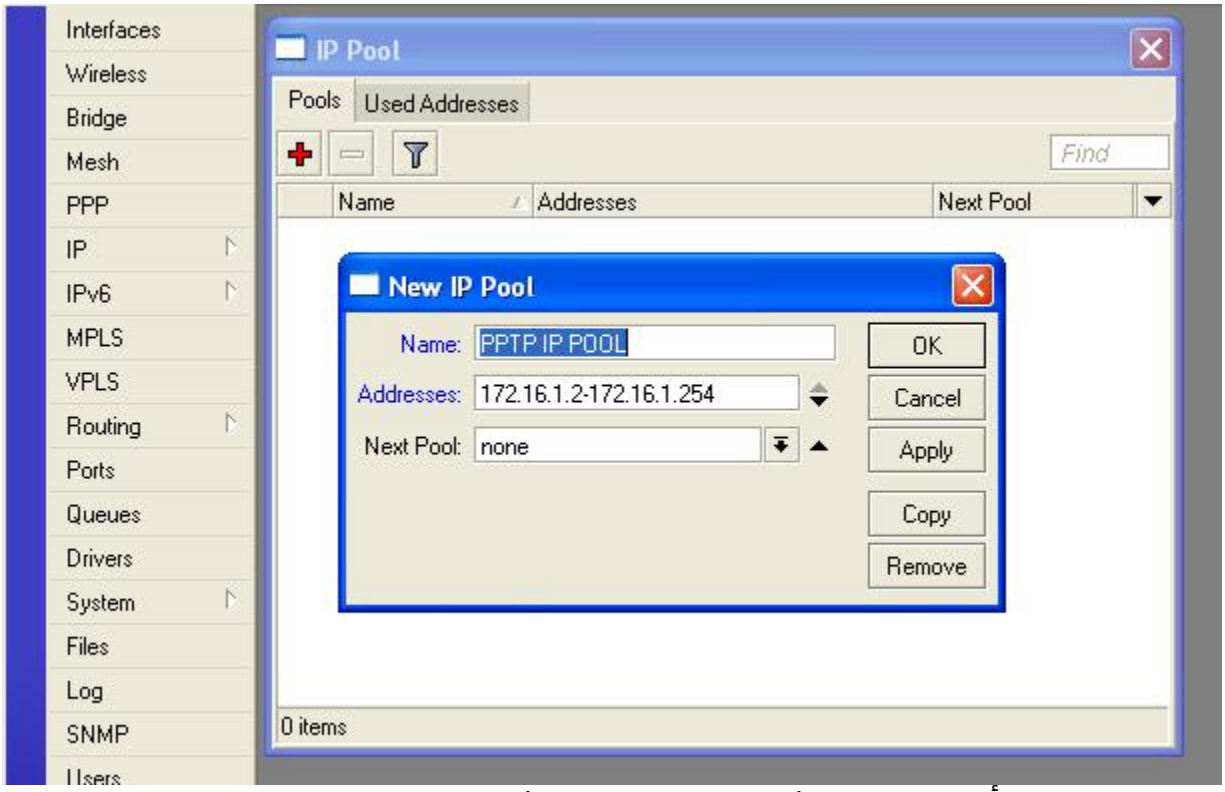


لما كانت الاتصالات النفقية متعددة التطبيقات وقد شرحنا سابقاً احد امثلتها وهي (PPPOE client and server) سيرتكز شرحنا اليوم على النوع الاخر الاكثر شيوعاً وهو (Point to Point Tunnel Protocol PPTP) والذي لا يسمح بخيار تجزئة النفق اي انه سيحدد مصدر واحد (جهاز مرسل واحد) وهدف واحد (جهاز مستلم واحد) ويمنع البقية من الاستلام للترافك الموجه الى حاسبة معينة. من مميزات هذا النوع سهولة ضبط اعداداته فتقريباً كل انظمة الويندوز الحديثة تضبط حاسباتها لتكون (PPTP client) تلقائياً.

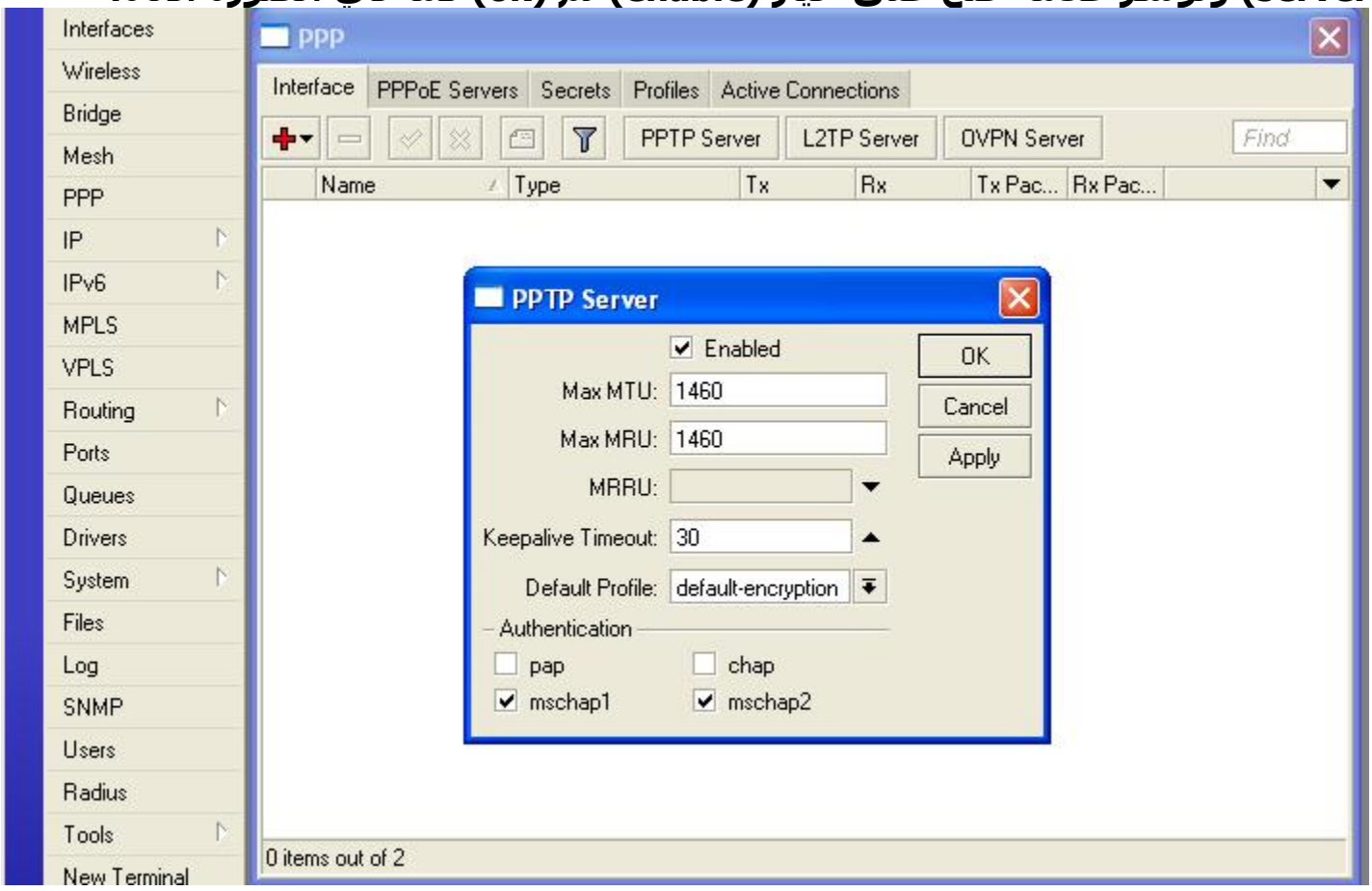
يمكن استخدام ال(PPTP) بخيارين احدهما بلا امنية وتشفير والاخر هو الاتصال الامن عبر قناة مشفرة وذلك بأستخدم بروتوكول التشفير (MSCHAP V2) ولتمكين الاتصال بواسطة هذا البروتوكول مع الجهاز البعيد (remote) نتبع الخطوات التالية:

اعدادات سيرفر ال (PPTP):

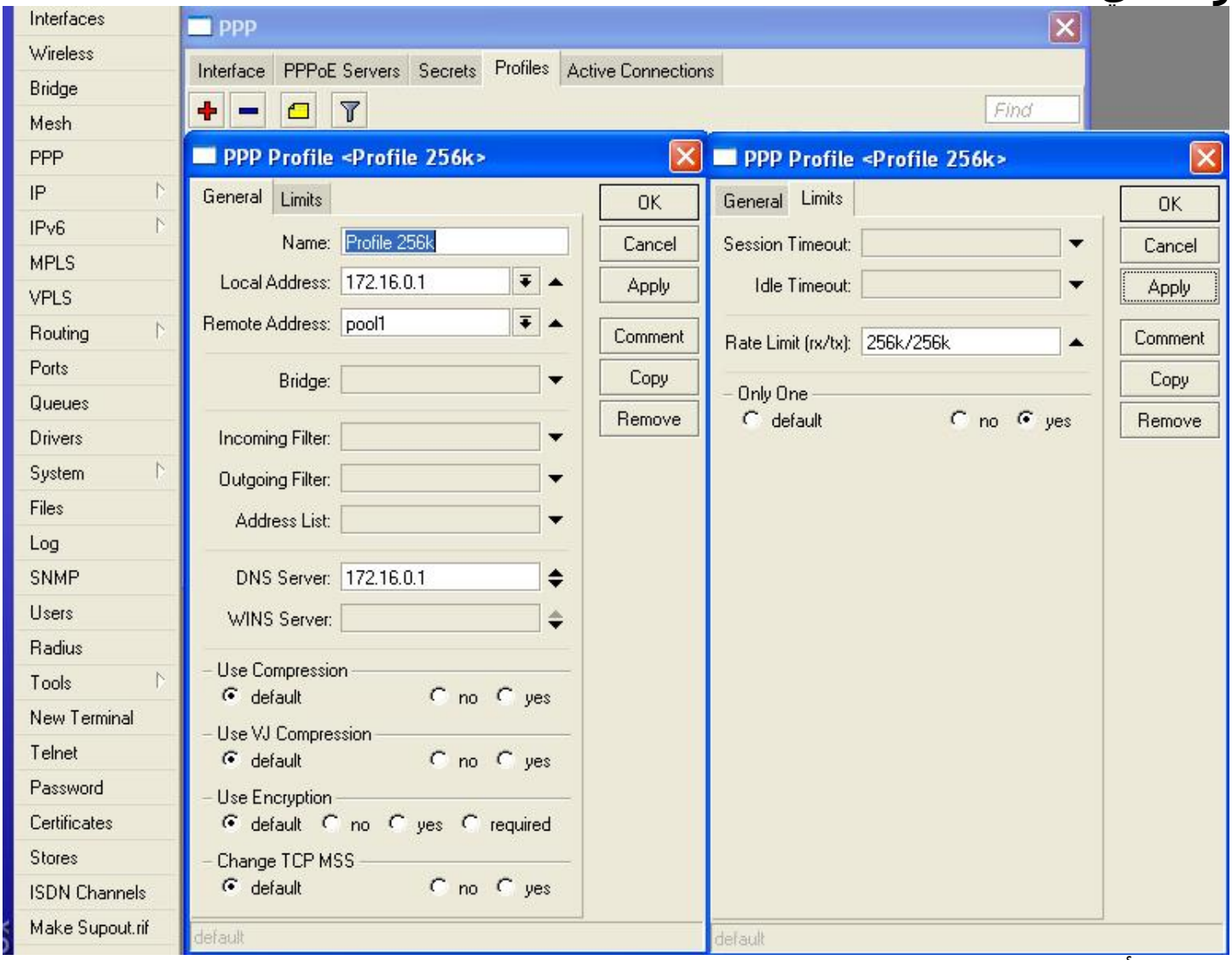
بعد ضبط اعدادات منافذ الجهاز ال (LAN and WAN) كما تم شرحه سابقاً نذهب الى تبويب (IP) ثم الى (POOL) وننقر على علامة الزائد (+) ثم نحدد اسم ومدى حوض العناوين وننقر على (ok) كما في ادناه:



والان نقوم بأنشاء سيرفر ال (PPTP) فنذهب الى تبويب (PPP) ثم الى (PPTP server) ونؤشر علامة صح على خيار (enable) ثم (ok) كما في الصورة ادناه:

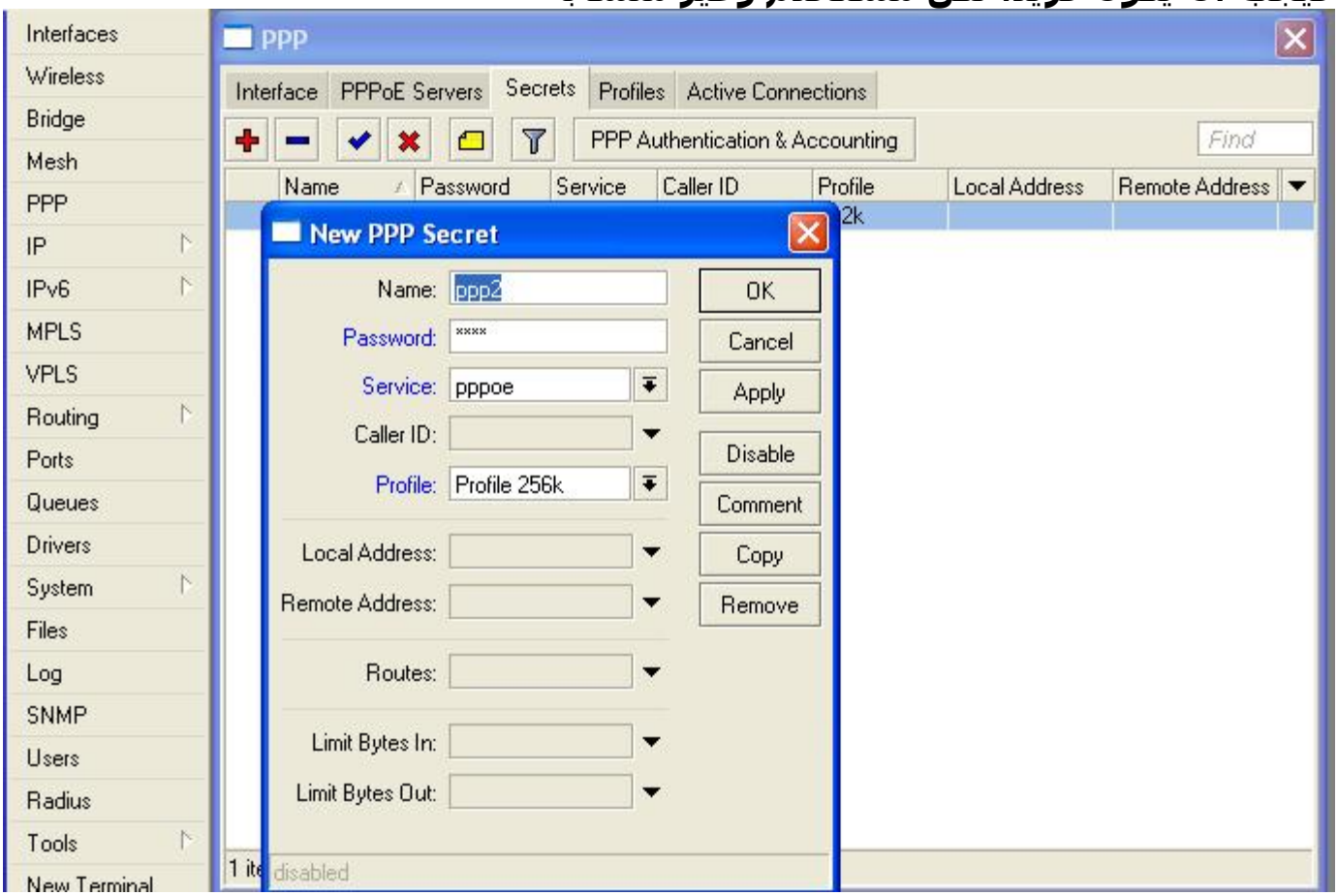


والان نقوم بخلق البروفايل الذي سيستخدم من قبل كل المستخدمين لهذا السيرفر وذلك بالنقر على تبويب(PPP) ثم الى تبويب (Profiles) وهنا سنجد بروفايلين موجودين مسبقاً فلا نتلاعب بهما وانما نقوم بأنشاء واحد جديد بالنقر على علامة (+) ونسميه بأي اسم نختاره وليكن (profile 256K) ونحدد عنوان السيرفر كعنوان محلي وبخصوص العنوان (remote) ننقر على السهم فيظهر لنا اسم الحوض الذي انشأناه قبل قليل ونختاره وان لم يظهر فنقوم بكتابة اسمه في حقل (remote address). في حقل ال (DNS server) نكتب عنوان السيرفر الذي كتبناه سابقاً في ال (local) وبعدها ننقر على تبويب (limits) لتحديد اقصى مقدار للأرسال والاستقبال المسموح لهذا المستخدم او للمستخدمين الذين يستخدمون هذا البروفايل ونحدد (256K/256K) ويختلف هذا المقدار حسب نوعية الخدمة المطلوب تقديمها للمستخدمين وبأختلاف اسعار الخدمة المقدمة وبعدها ننقر على (apply) ثم (ok) وكما في ادناه:

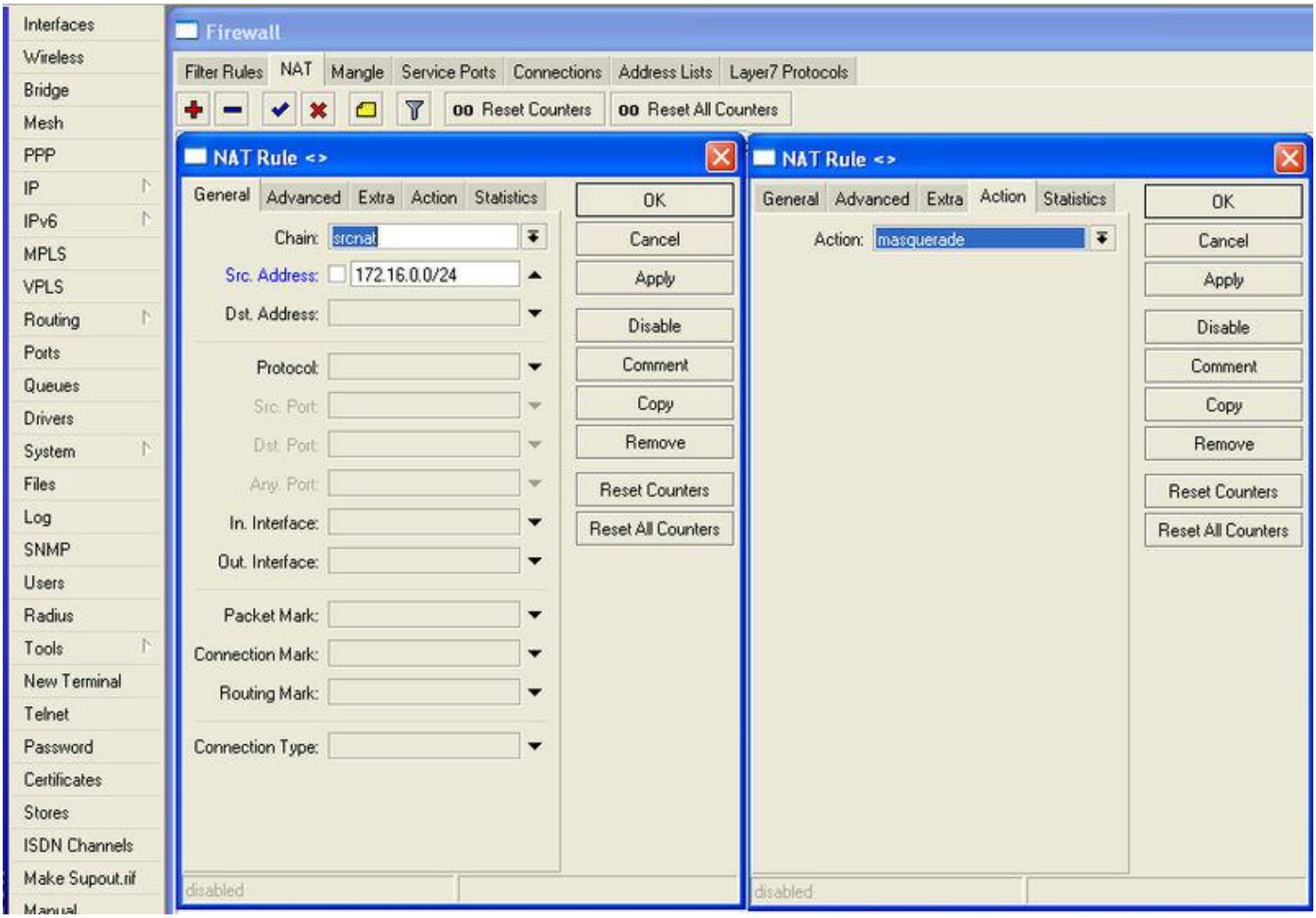


والان لأضافة مستخدم الى هذا الاتصال النفقي نذهب الى تبويب (Secrets) ثم نكتب اسم المستخدم وكلمة المرور التي سيستخدمها المستخدم للدخول الى النظام واكتساب القدرة على الاتصال. واما بخصوص العنوان المحلي (local address)

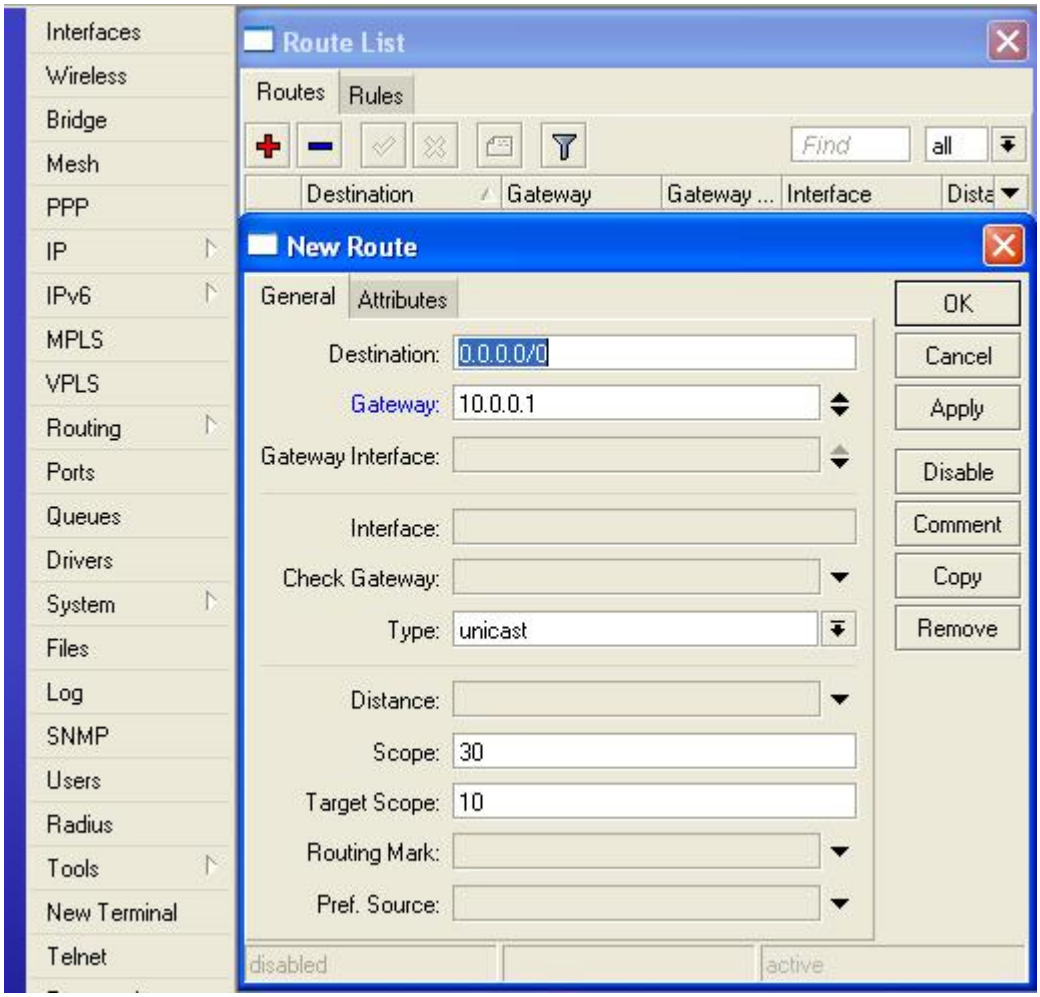
فيمكن ان يكون نفسه لكل المستخدمين واما العنوان البعيد (remote address) فيجب ان يكون فريداً لكل مستخدم وغير متشابه



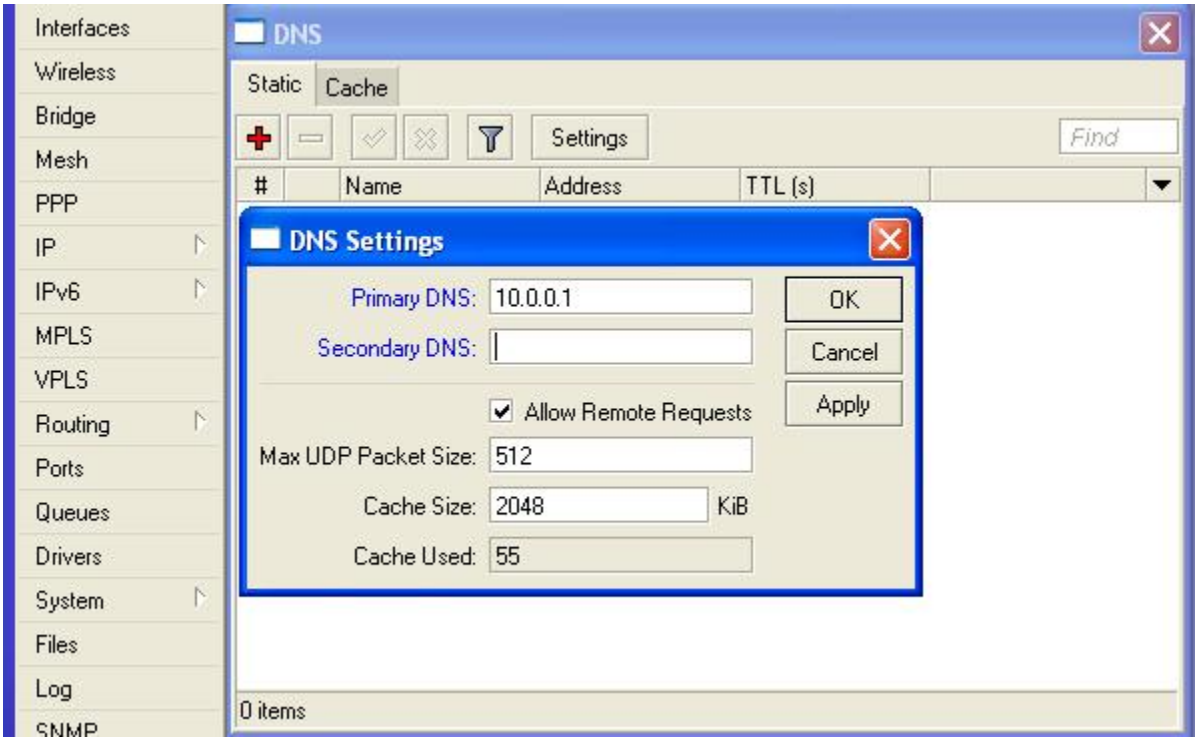
والى هنا تنتهي اعدادات سيرفر ال (PPTP)
والان لأكمال تأمين الشبكة نذهب الى تبويب (IP) ثم (Firewall) ونختار تبويب (NAT) ثم ننقر على علامة الزائد (+) لأضافة سلسلة جديدة (Chain=secret) ونضبط عنوان ال (Scr. Address) ليكون هو نفسه عنوان شبكة المنفذ المحلي للسيرفر ثم نذهب الى تبويب (Actions) في نفس النافذة ونختار (action= masquerade) لأضافة التنكر الى الشبكة ثم (apply) ثم (ok) وكما في ادناه:



والان نضبط المسار الافتراضي (default route) فنذهب الى تبويب (IP) ثم الى (routes) ونقوم بأضافة مسار ثابت (static route) بالنقر على زر (+) ونختار العناوين كما في النافذة ادناه ثم (Apply) ثم (ok):



والان ننتقل الى الخطوة الاخيرة وهي اضافة عناوين ال (DNS server) وذلك بالذهاب الى تبويب (IP) ثم (DNS) ثم ادخال العناوين التي يفترض ان يمنحك اياها مزود الخدمة (ISP) وتذكر ان تفعل (allow remote requests) والتي ستجعل جهازك يعمل ك (DNS server) وضبط حجم الكاش على ان لا يقل عن (2048) ثم (apply) و (ok) كما في ادناه:

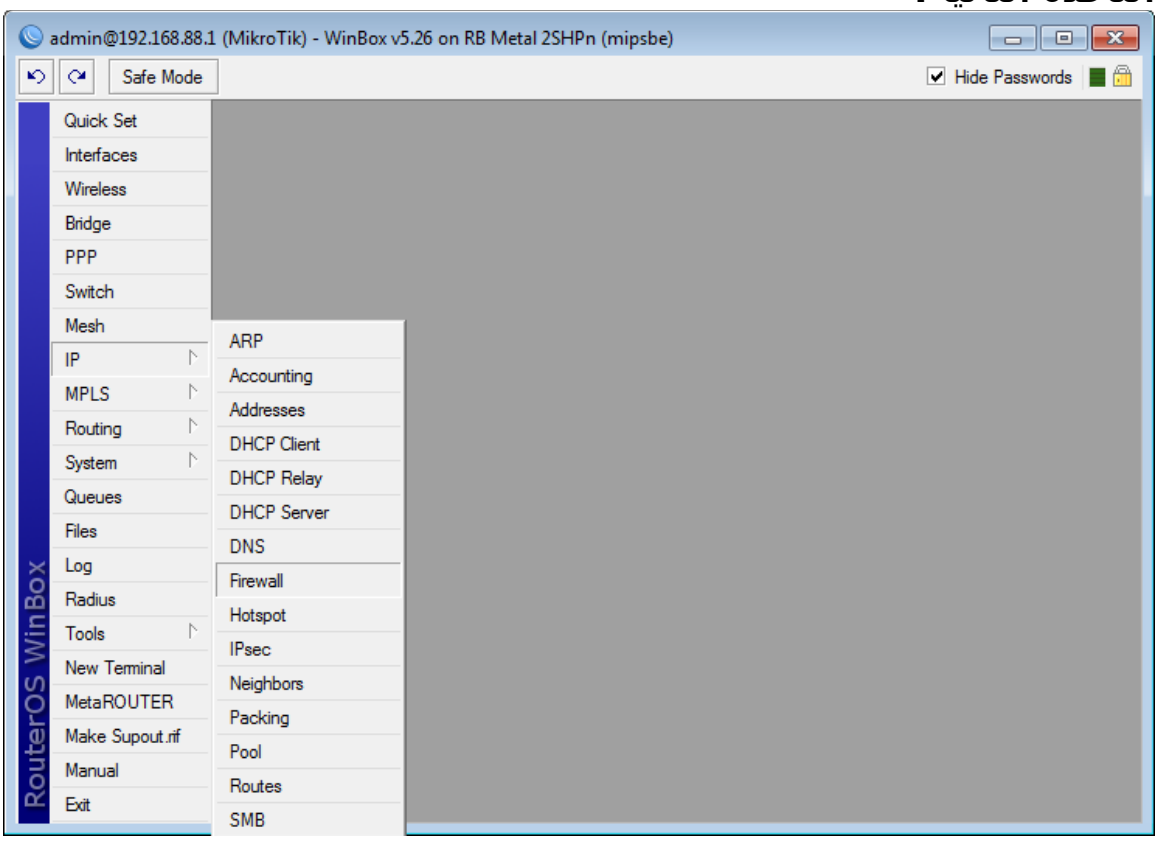


والى هنا تنتهي اعدادات سيرفر ال (PPTP) واما بخصوص الطرف الاخر الخاص بالمستخدم فيتلخص العمل بأنشاء (broad band connection) ونضع فيه اسم المستخدم وكلمة المرور التي اعطانا اياها مزود الخدمة (PPTP server).

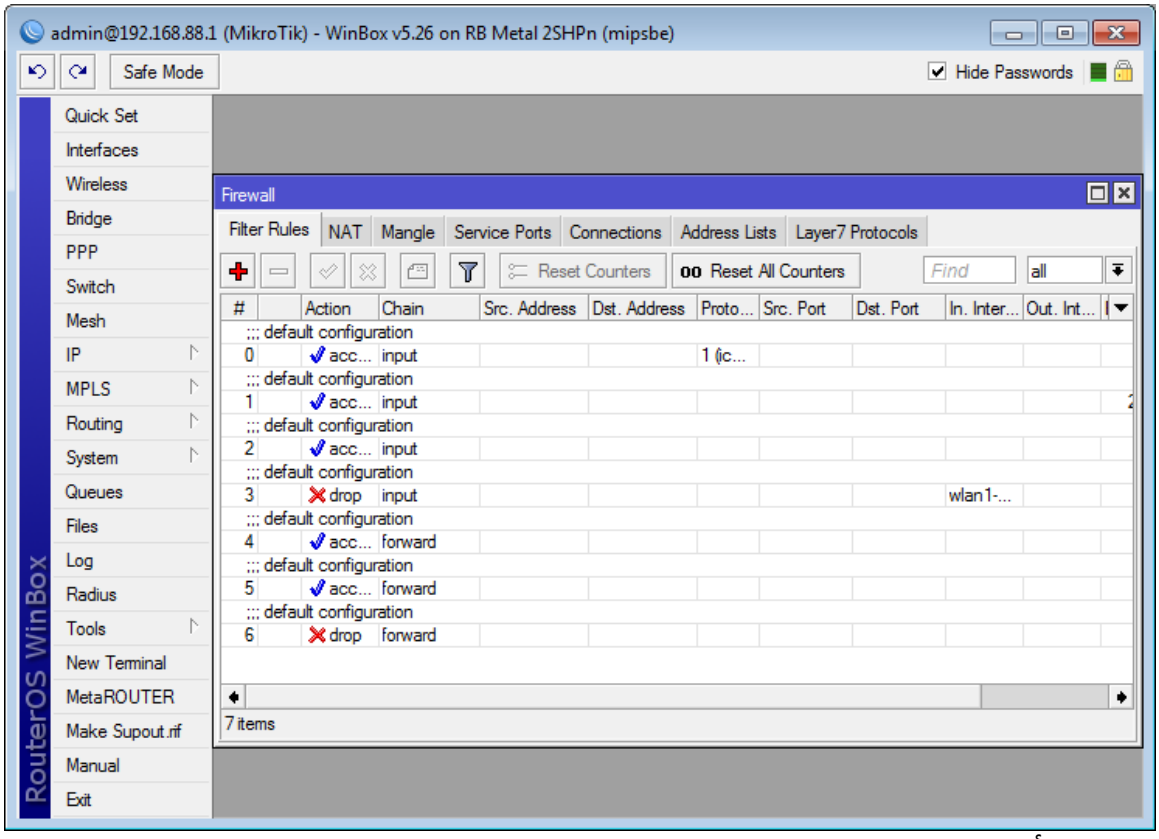
حجب مواقع معينة بأستخدام الجدار الناري للمايكروتك

من اهم وظائف مدير الشبكة قدرته على ترشيح وترشيد الدخول الى مواقع معينة من قبل المستخدمين في شبكته التي يديرها ومن اهم الادوات المستخدمة في حجب الوصول الى مواقع معينة في المايكروتك هو الجدار الناري (Firewall) والذي يمكننا من وضع ما يسمى بالسلاسل (chains) وتقييد العمل بداخلها بفعاليات معينة (actions) من سماح ومنع وقفز وتحويل وغيرها الكثير وسيكون مثالنا اليوم عن كيفية حجب الفيس بوك بأستخدام المايكروتك ويمكن تطبيق نفس الخطوات لأي موقع اخر مع تغيير عنوان الموقع (IP address) وكما يلي:

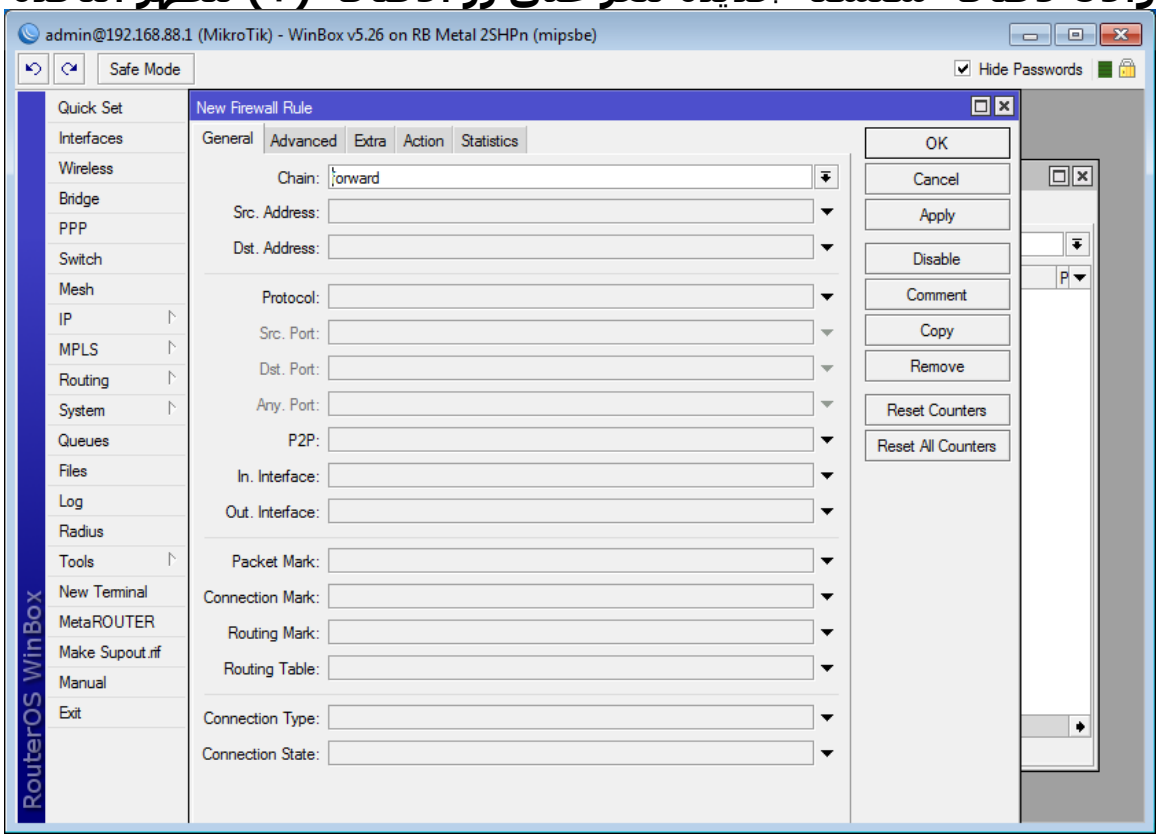
نبدأ بفتح ال(winbox) بالطريقة الاعتيادية ونذهب الى (IP) ثم (firewall) كما في النافذة التالية:



عندها تظهر نافذة جديدة مشابهة للنافذة ادناه:

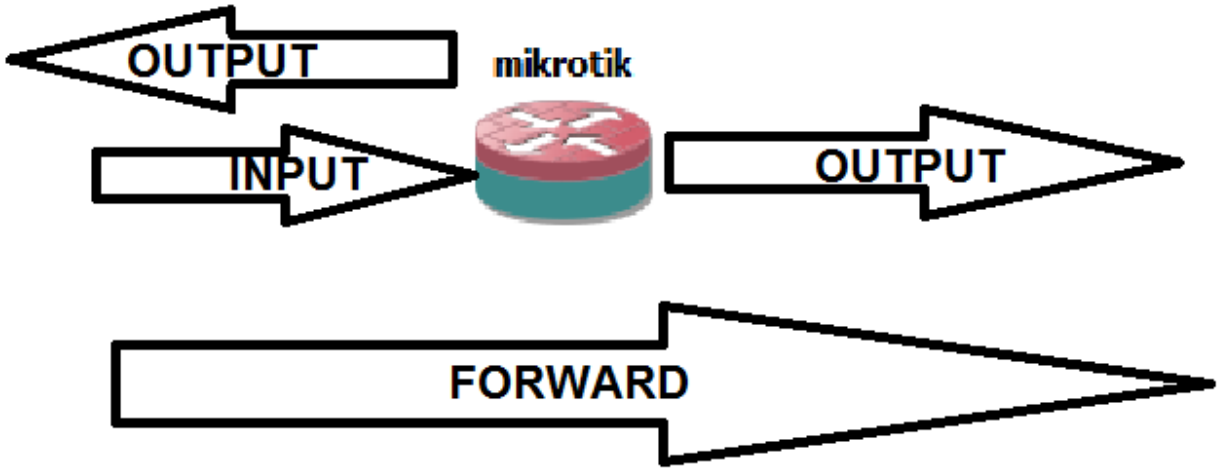


والان لأضافة سلسلة جديدة ننقر على زر الاضافة (+) لتظهر النافذة التالية:

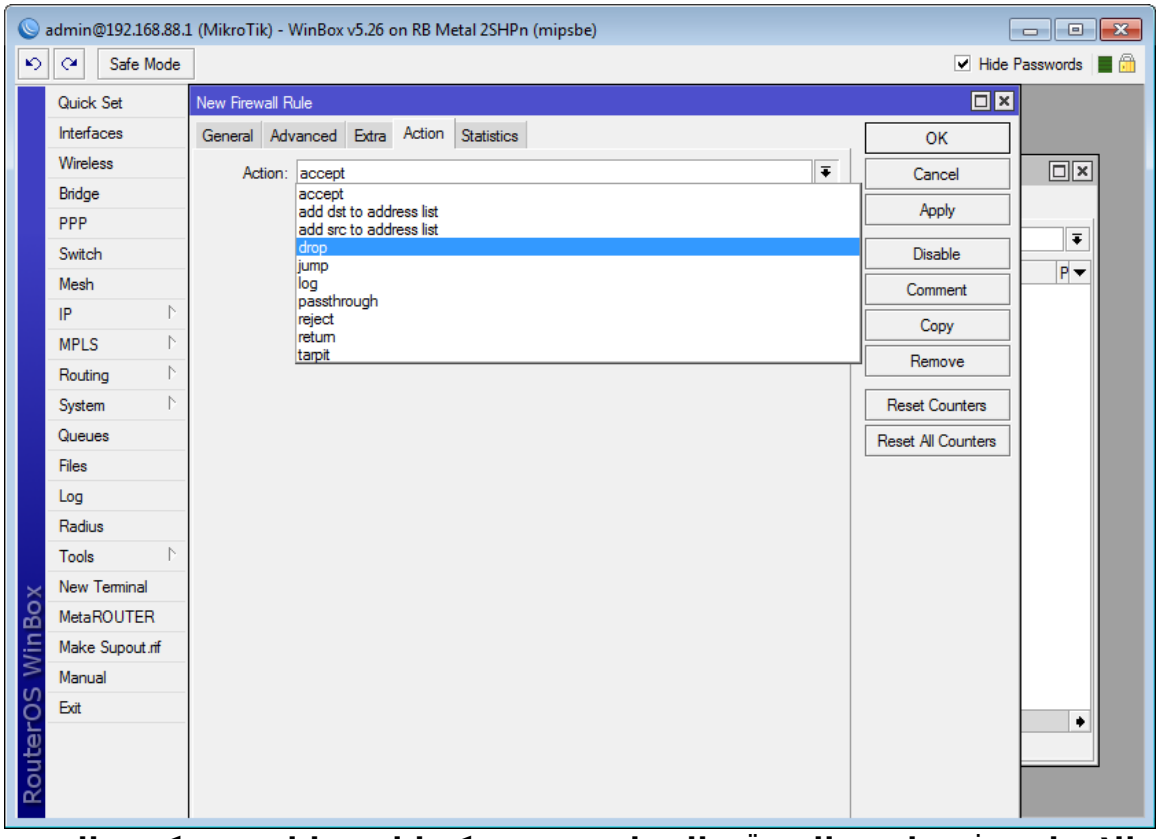


والان نصل الى كيفية اختيار السلسلة وهل هي (forward, input, output) وكما يلي:

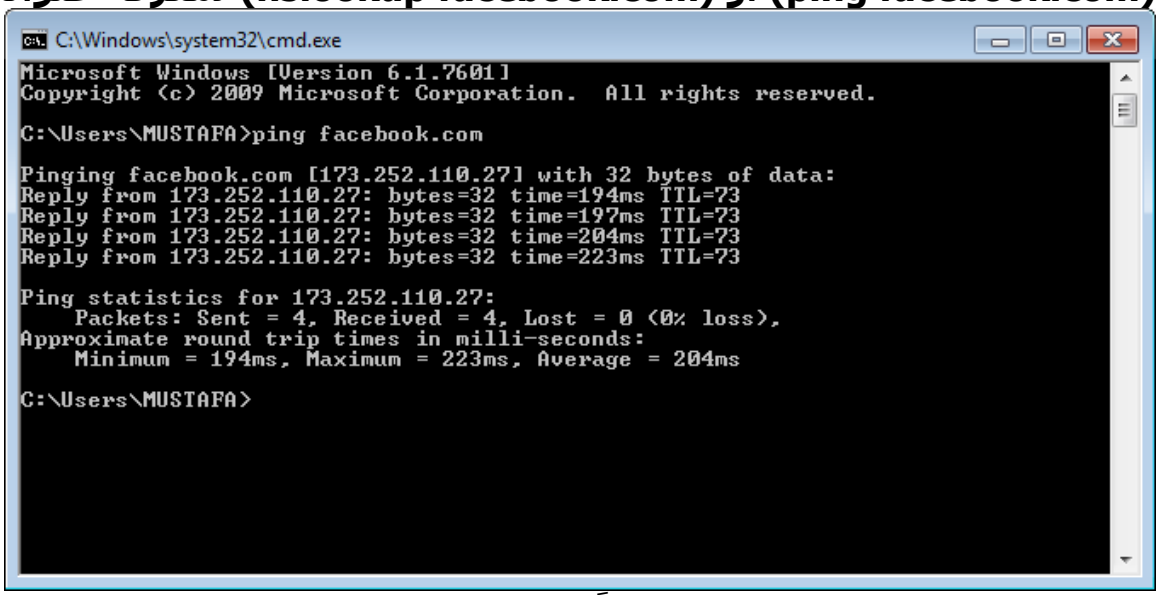
١- (Forward): لأي سلسلة تتحكم في طلبات المستخدم للمواقع في شبكة ال (WAN) وتكون وظيفة الراوتر (المايكروتك) فقط توجيه (forward) البيانات.
٢- (input): للأجراءات والسلاسل التي تحكم علاقة المستخدم بالمايكروتك.
٣- (output): للسلاسل التي يكون مصدر العمل فيها هو المايكروتك وتخرج منه البيانات الى المستخدم او الى شبكة (WAN) وكما في الرسم التوضيحي التالي:



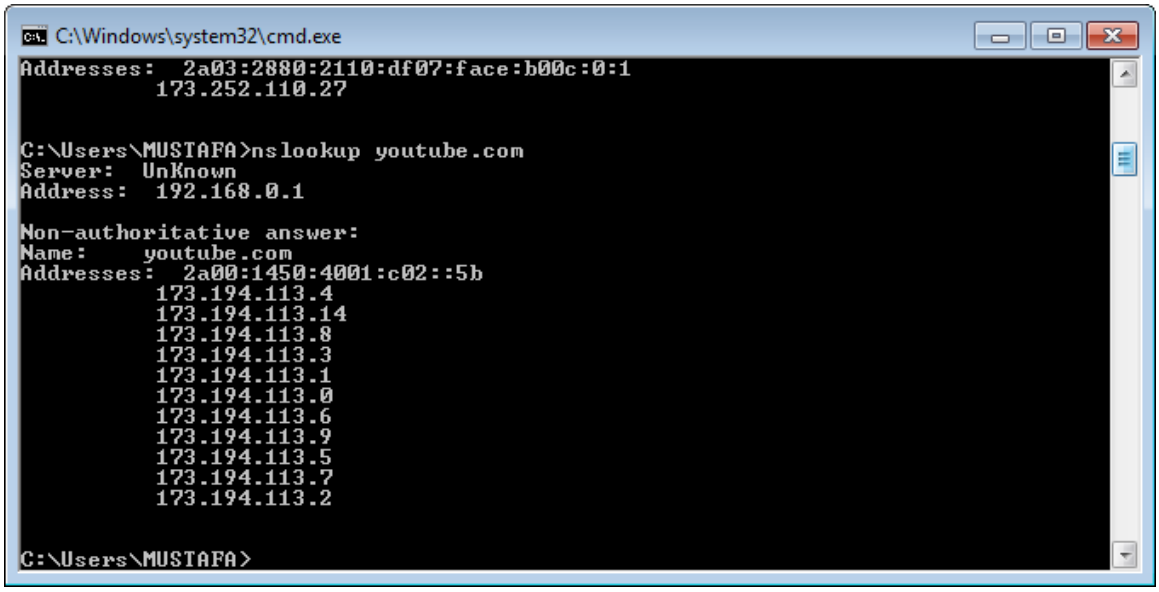
والان يفترض اننا عرفنا ان علاقة المستخدم بالشبكة الدولية تستلزم اختيار (forward) وبعدها ننقر على تبويب (action) ونختار (drop) والذي يعني ان كل طلب من المستخدم للموقع (الذي سنحدده لاحقاً) سيتم اهماله وعدم الاستجابة له وكما في النافذة ادناه:



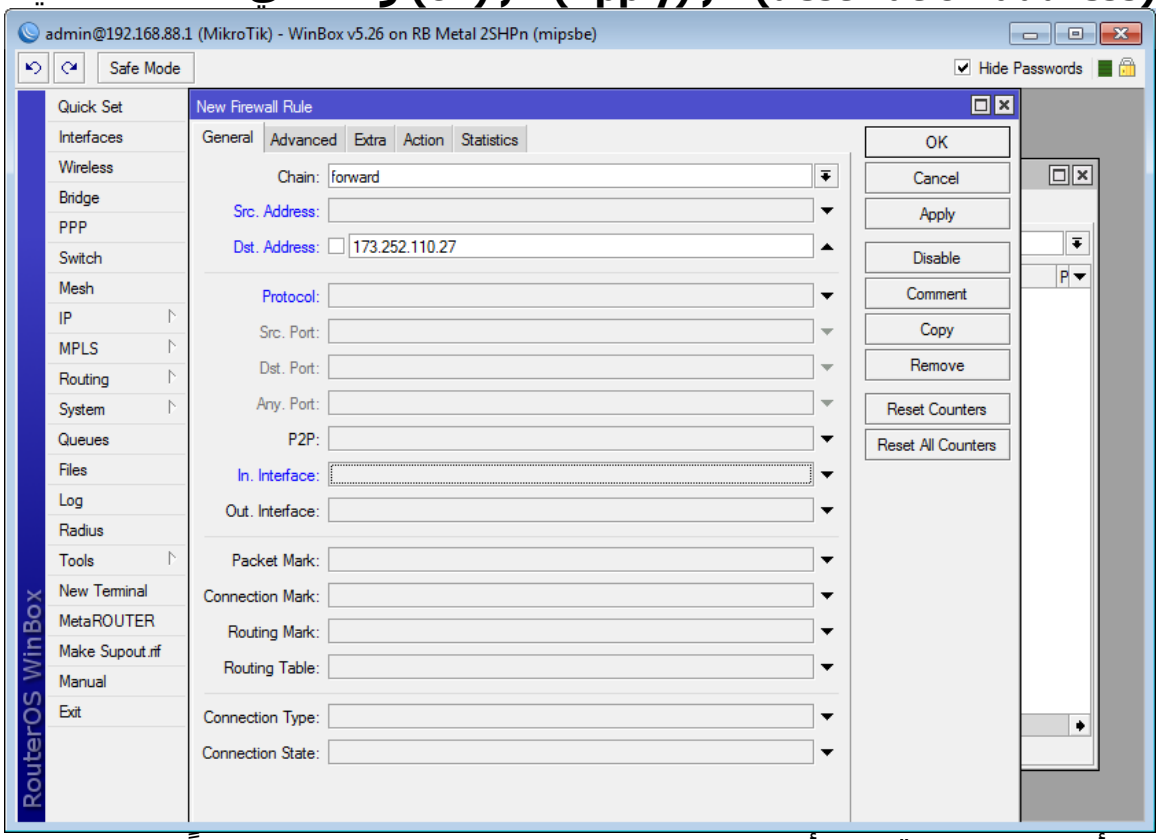
والان لنعرف ما هو الموقع المراد حجبه وكما اتفقنا انه سيكون الفيس بوك نقوم بعمل (ping facebook.com) او (nslookup facebook.com) لمعرفة عنوانه وكما يلي:



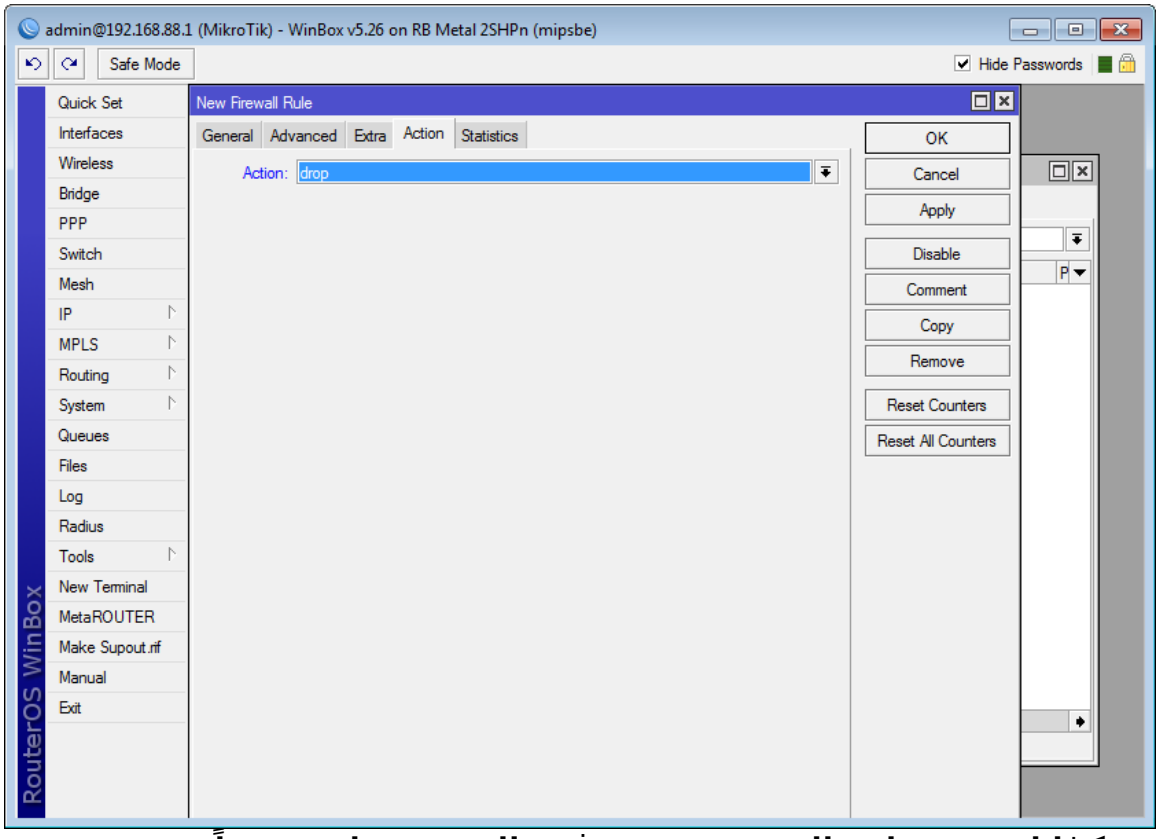
مع الانتباه الى فقرة مهمة جداً وهي ان بعض المواقع تحتوي عدة عناوين (IP address) مما يعني وجوب عمل عدة سلاسل وفعاليات (chain and action) لكل منها وكما في اليوتيوب الذي يمتلك (١١) عنوان وكما في النافذة التالية:



والان بعد ان عرفنا عنوان الموقع المراد حجبه فقط نقوم بإضافته الى ال (destination address) ثم (Apply) ثم (ok) وكما في النافذة التالية:

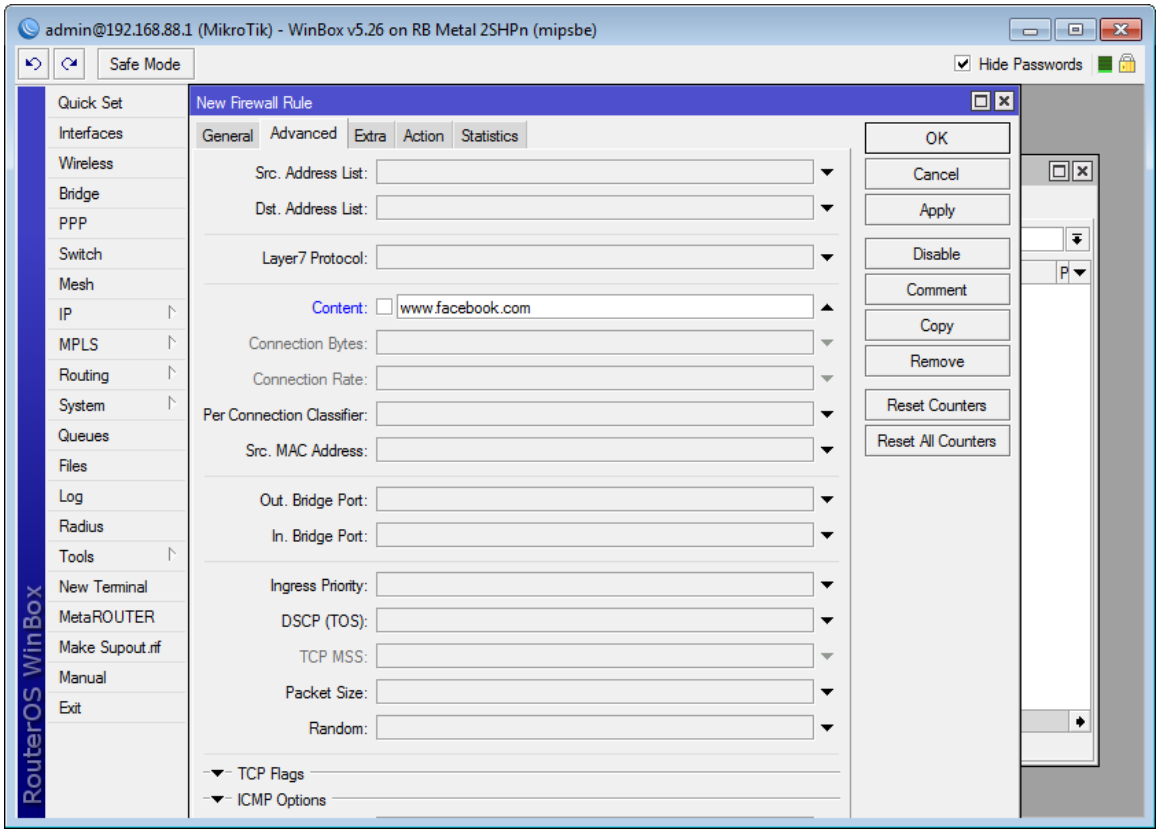


ونتأكد من اننا قمنا بأختيار (action: drop) كما بيننا سابقاً :



وهكذا لن يستطيع المستخدمون فتح الفيس بوك مجدداً.

هناك طريقة اخرى لعمل ذلك وبخطوات مشابهة حيث اننا بدل ان نحدد عنوان الموقع المستهدف في تبويب (general) نستطيع تحديده في تبويب (Advanced) في ال (Content) ونحدد ايضاً الاكشن ك (Drop) كما بينا سابقاً وكما في النافذة التالية:

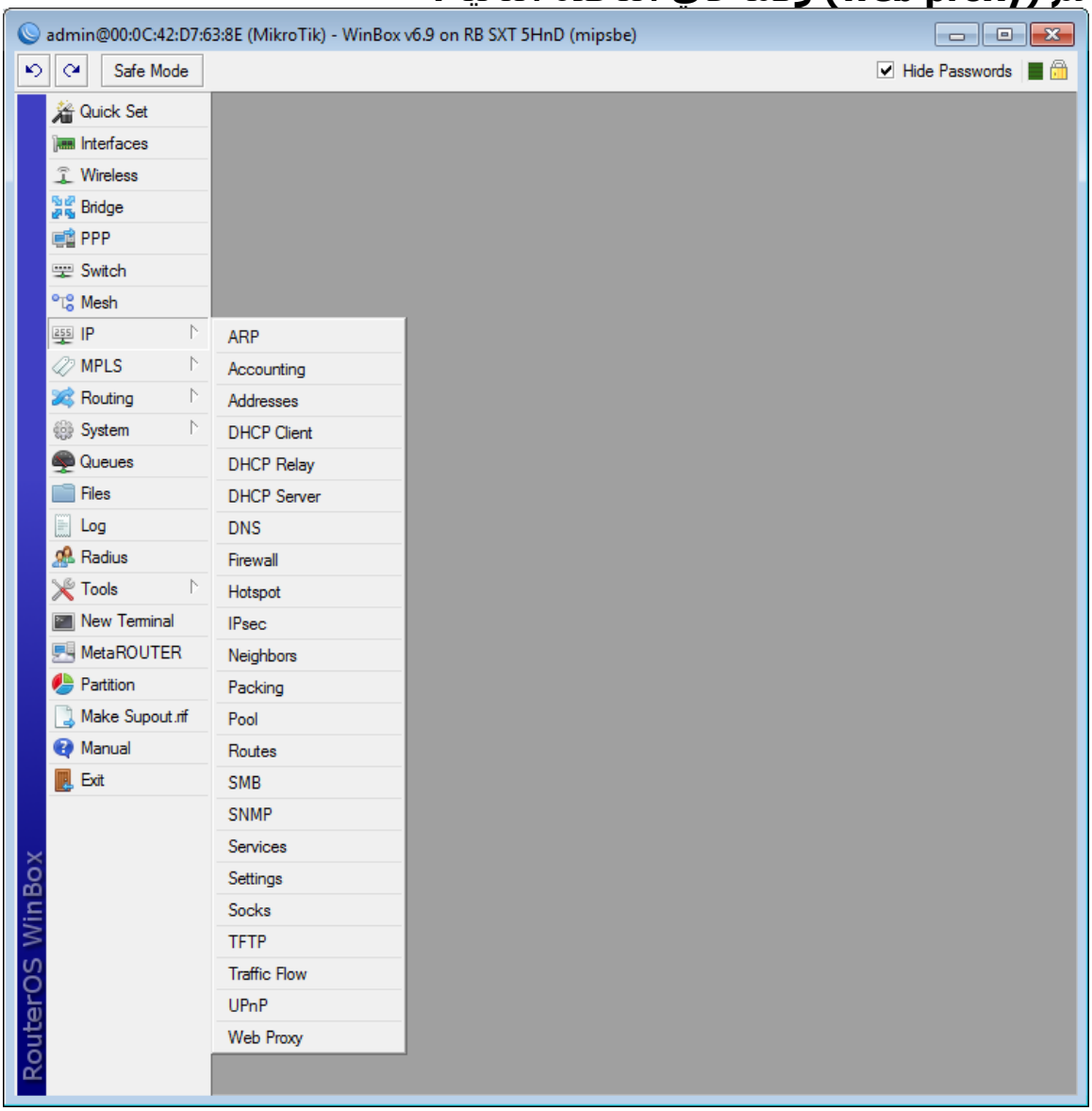


ملاحظة اخيرة تجدر الاشارة اليها هي ان هناك الكثير من الطرق الاخرى باستخدام ال (open dns) و (web proxy) والتي سنقوم بشرحها لاحقاً ان شاء الله.

حجب المواقع في اجهزة المايكروتك بأستخدام ال (web proxy)

بعد ان شرحنا طريقة حجب موقع معين باستخدام الجدار الناري في الدرس السابق نبدأ اليوم رحلتنا مع خاصية جديدة اكثر كفاءة من سابقتها في اجهزة المايكروتك لحجب مواقع معينة او عمل تحويل واعادة توجيه لها الى مواقع وعناوين اخرى نحن نحددها واليكم التفصيل:

يمكن استخدام الويب بروكسي لحجب مواقع نحدد عناوينها او جزء من اسمائها وذلك في اجهزة المايكروتك التي تحتوي رخصة (٤،٥،٦) ولا تعمل في الاجهزة التي تمتلك رخصة أدنى من ذلك ويتلخص الموضوع بالدخول على (Winbox) والذهاب الى (IP) ثم (web proxy) وكما في النافذة التالية:



والان تظهر نافذة مشابهة للنافذة التالية فنقوم بتمكين (enable) الويب بروكسي بالنقر في المربع بجانب كلمة التمكين و نترك عنوان المصدر (src. Address) فارغاً ونحدد المنفذ الذي سنتحكم في مروره وكما يعلم كل مختص شبكات فنحن لدينا (0-35535) منفذ يمكن استخدامها عدا المنافذ المستخدمة بشكل رسمي لبعض

البروتوكولات والتطبيقات مثل المنفذ (٨٠) لل (HTTP) واليكم ادناه قائمة بالمنافذ المستخدمة والتي لا يمكن استخدامها لمهام اخرى غير التي خصصت لها:

TCP/UDP Port Numbers

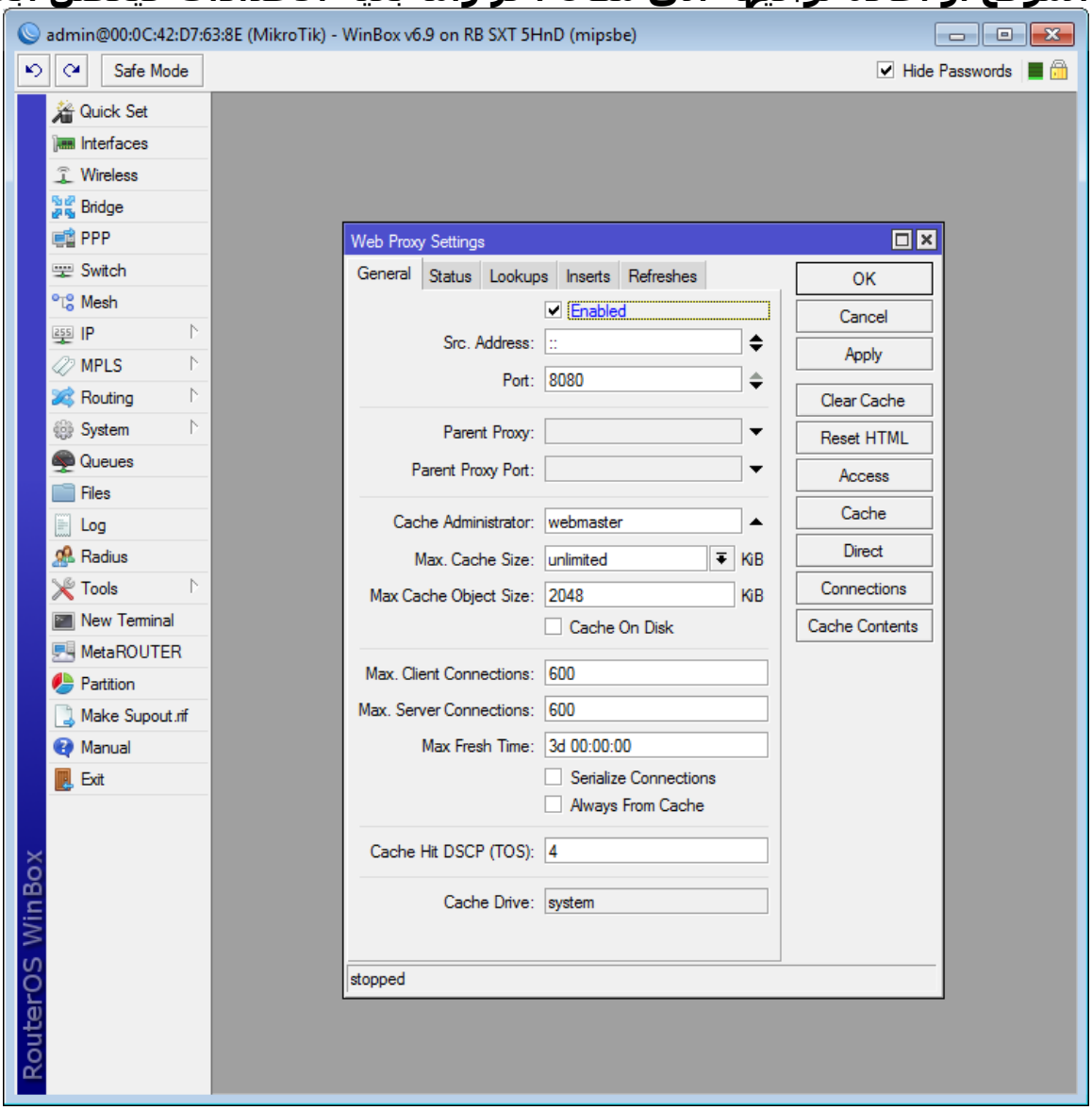
7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

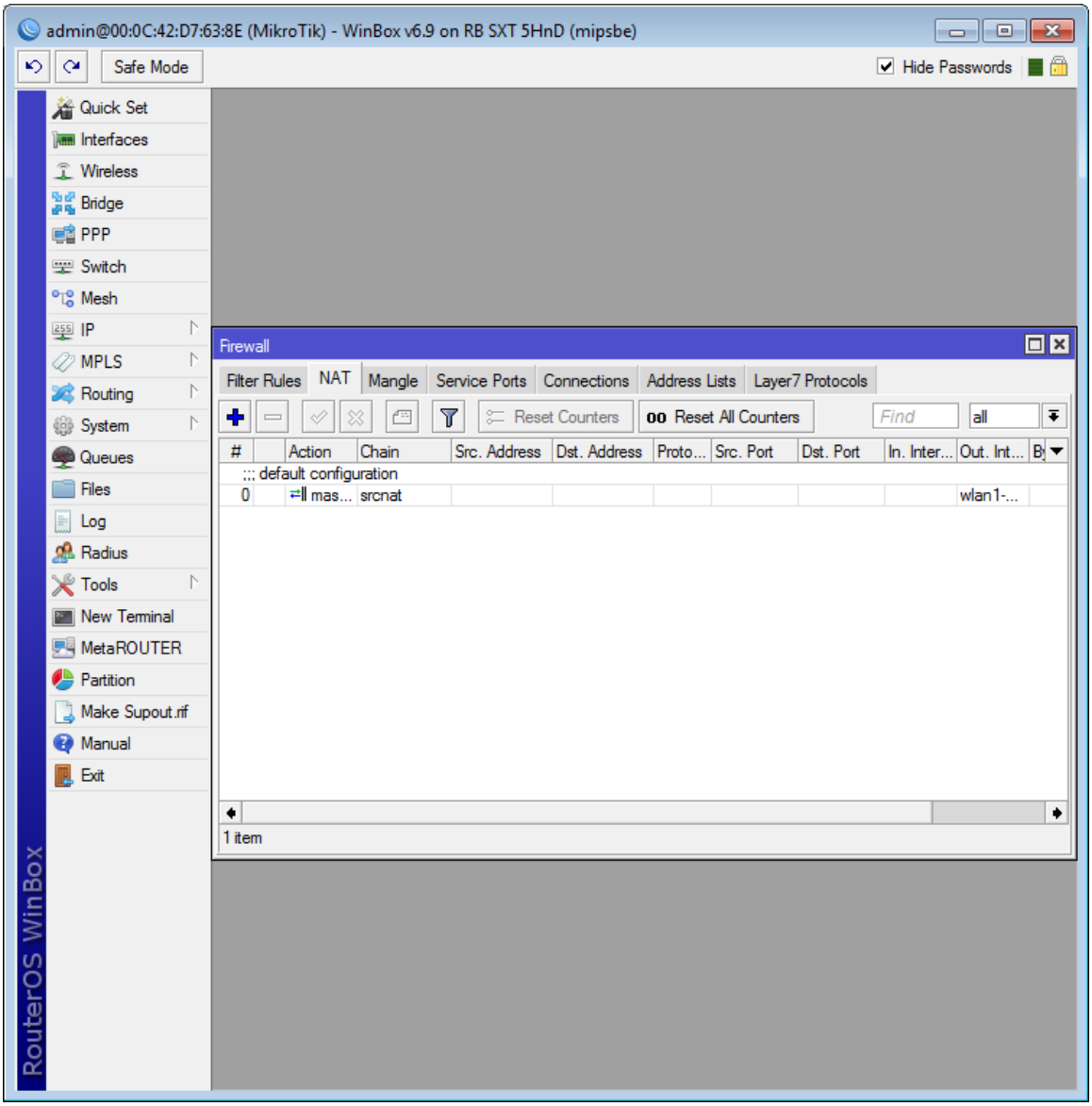
- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

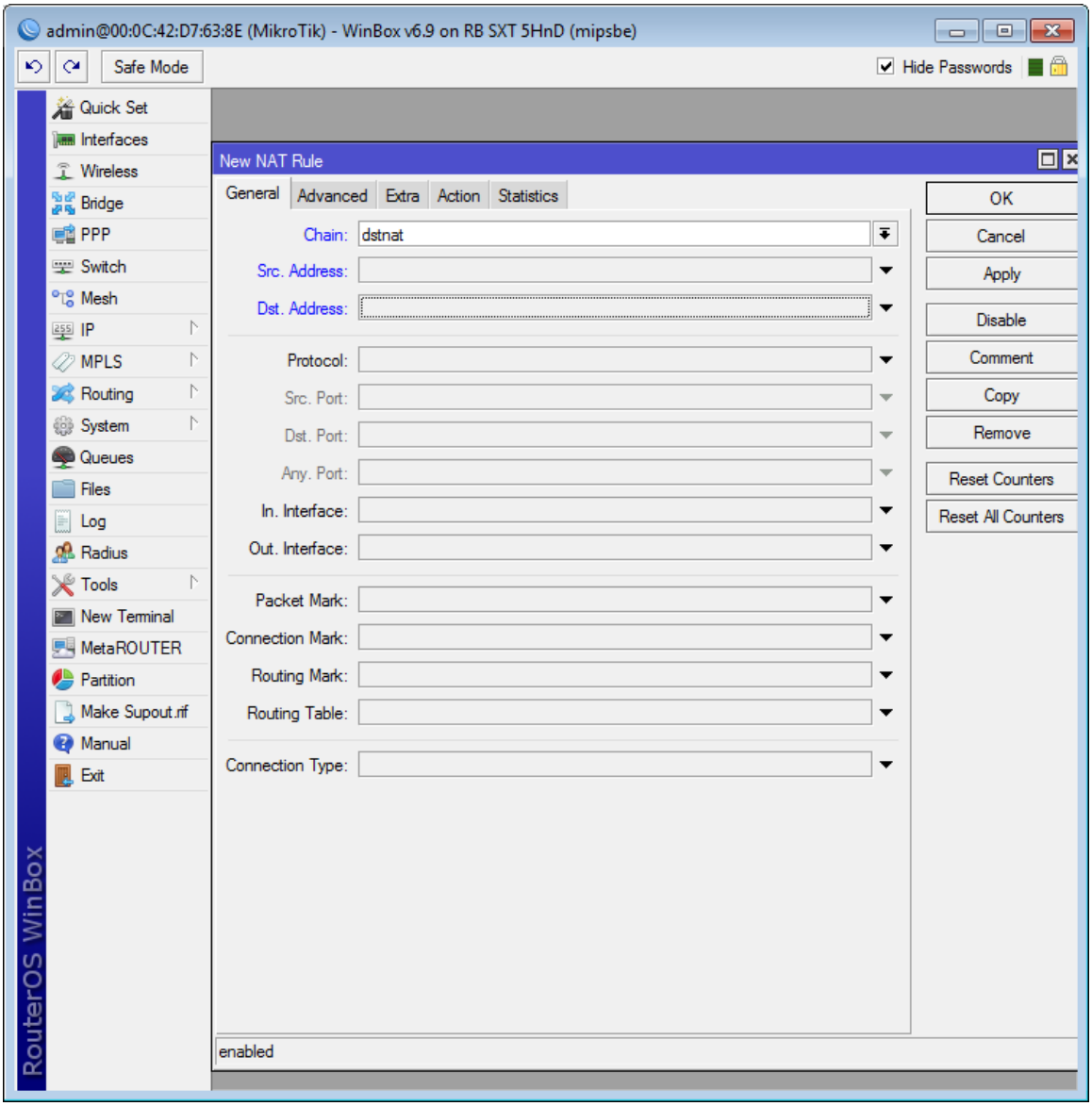
ونحن هنا اخترنا (٨٠٨٠) المحدد مسبقاً من قبل النظام والان في حقل الـ(cache administrator) نحدد اسم او عنوان يظهر للمستخدم للدلالة على من قام بحجب الموقع او اعادة توجيهه الى مكان اخر واما بقية الاعدادات فيفضل ابقائها كما هي:



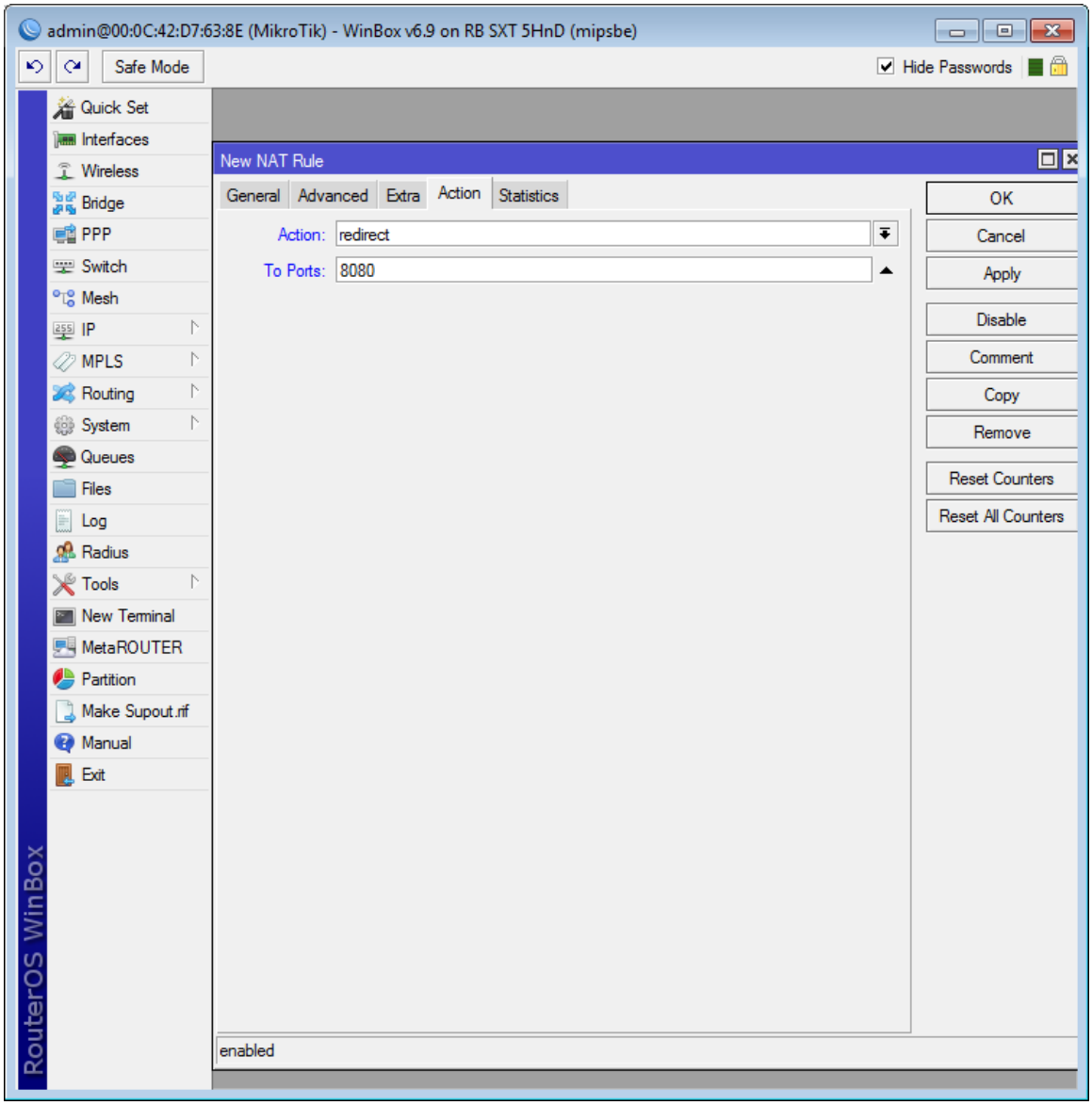
والان ننقر على (apply) ثم (ok) ونذهب الى (IP) ثم (firewall) ثم تبويب (NAT) لتظهر النافذة التالية:



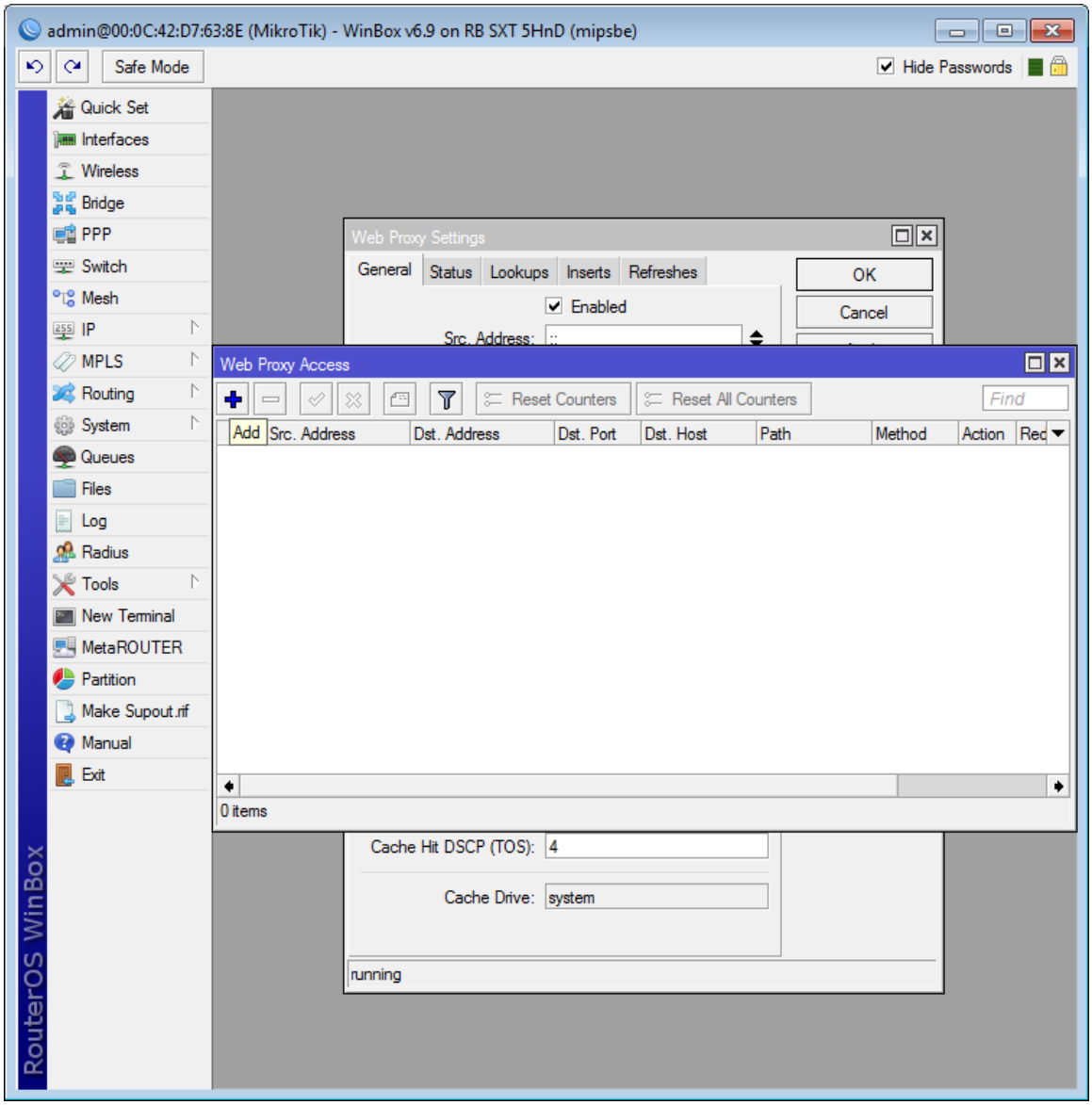
والان لتفعيل الكاش ننقر على اشارة الزائد لإضافة (rule) جديدة وكما في النافذة التالية:



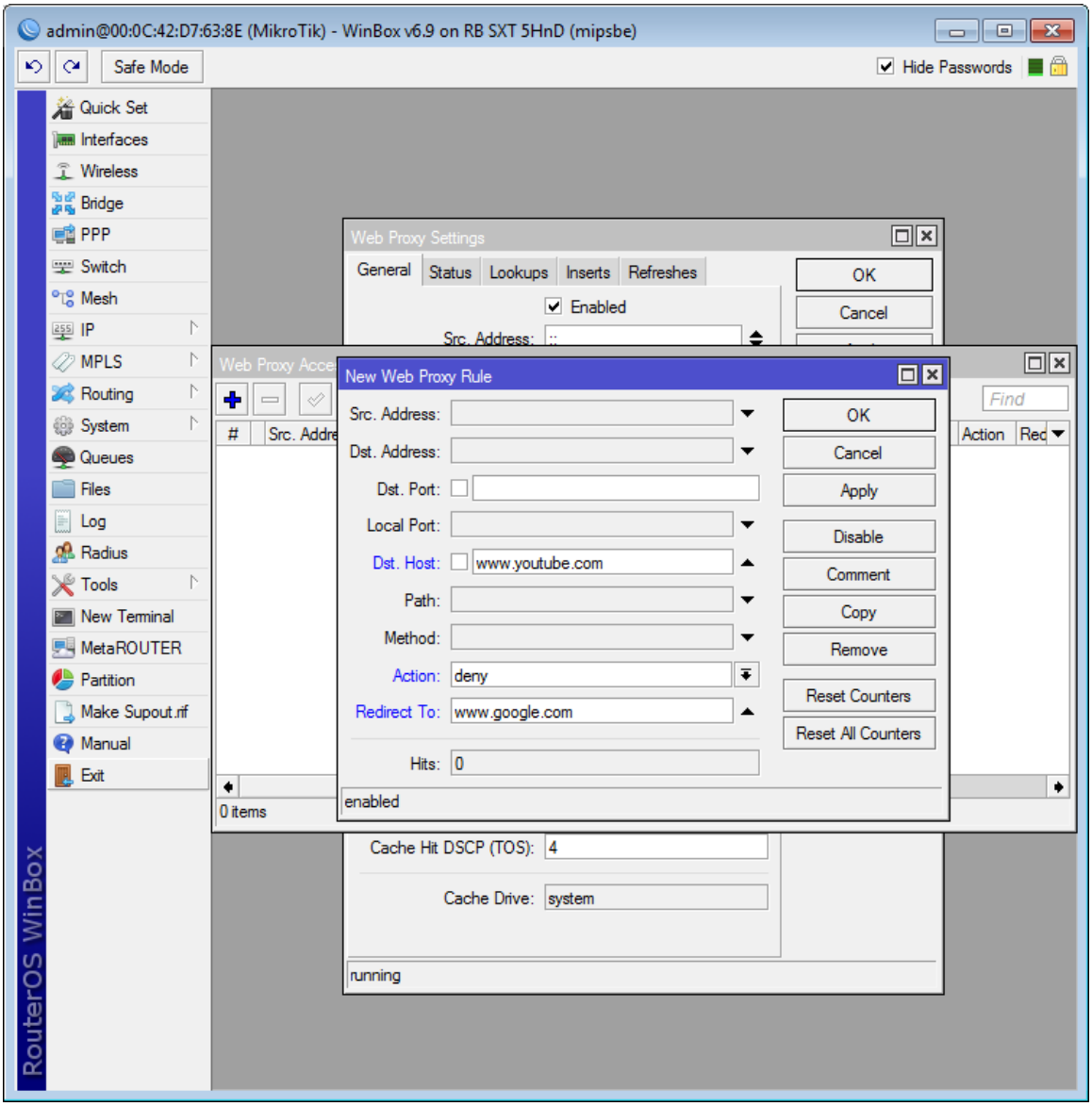
نغير ال (chain) الى (dstnat) ثم ننقر على تبويب (action) لتظهر النافذة التالية:



نغير ال(action) الى (redirect) والمنفذ الى رقم المنفذ الذي اخترناه مسبقاً (٨٠٨٠) ثم (apply) ثم (ok). والان نعود الى ال (web proxy) وننقر على زر (access) في جهة اليمين من نافذة ال (web proxy) لتظهر النافذة التالية:

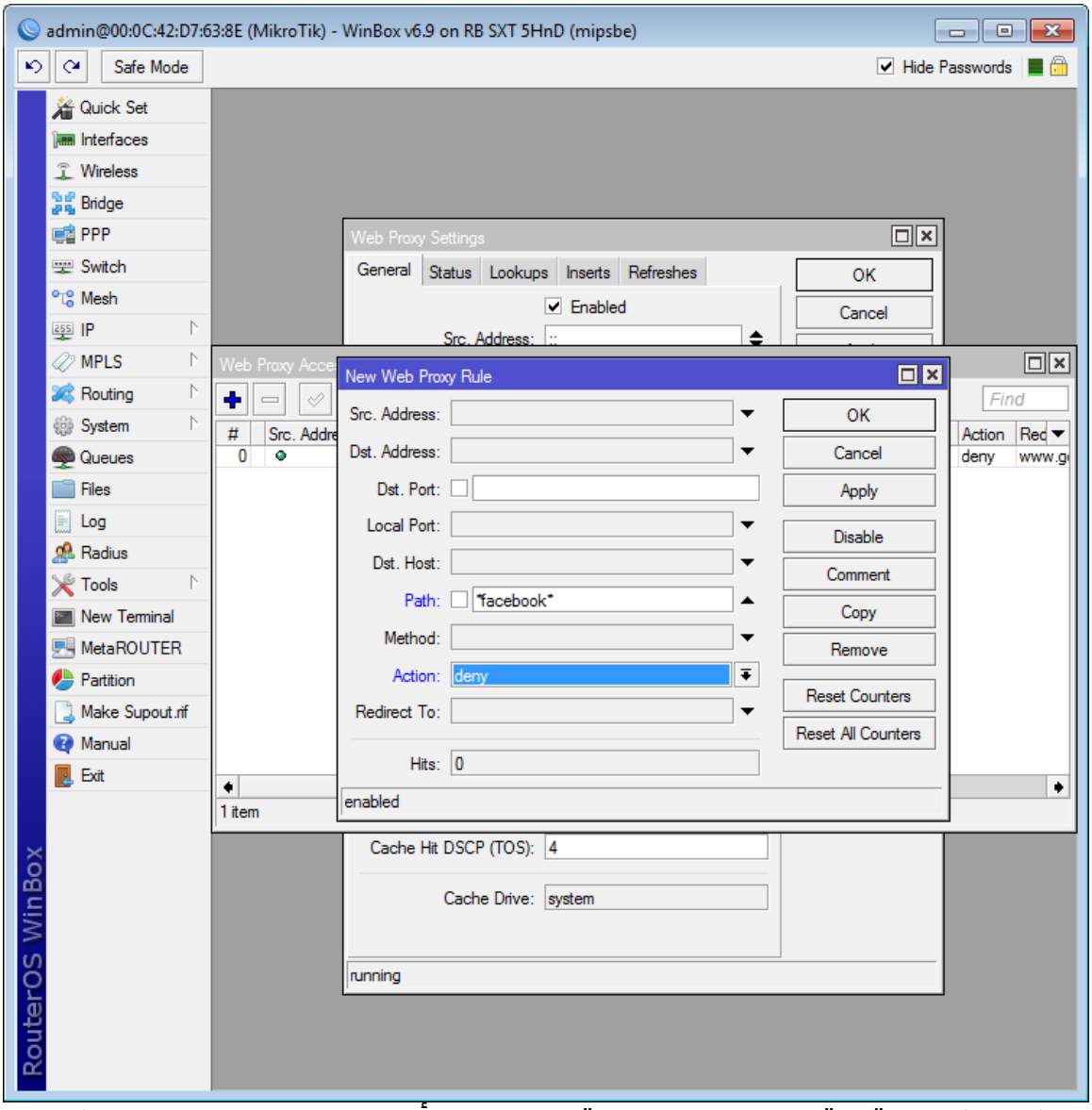


ننقر على زر الاضافة (+) لتظهر النافذة التالية:



نحدد من هنا عنوان المصدر او الهدف او موقع المصدر او الهدف والفعالية التي نريد تطبيقها عليه وهنا اخترنا الموقع المستهدف وهو (www.youtube.com) واخترنا الفعالية (Action) المراد تطبيقها عليه وهي المنع (deny) وكذلك يمكن بدل اختيار الحجب اختيار عملية اعادة توجيه المستخدم الى موقع اخر بأختيار (redirect to) ونكتب اسم الموقع الذي نريد للمستخدم ان يراه حين يطلب الموقع المراد حجبه وهو في حالتنا هذه (www.google.com) ثم ننقر على (apply) و (ok).

توجد طريقة اخرى نستطيع حجب المواقع بموجبها بأستخدام الويب بروكسي بأستخدام مسار الموقع او اسمه او جزء من اسمه والذي نعرفه فمثلاً لحجب اي موقع يحتوي اسمه على كلمة (facebook) نحصرها بين علامة نجمة وكما يلي (*facebook*) ويكون ذلك في قاعدة ويب بروكسي جديدة بالنقر على علامة (+) لتظهر نافذة نكتب فيها ما يلي:

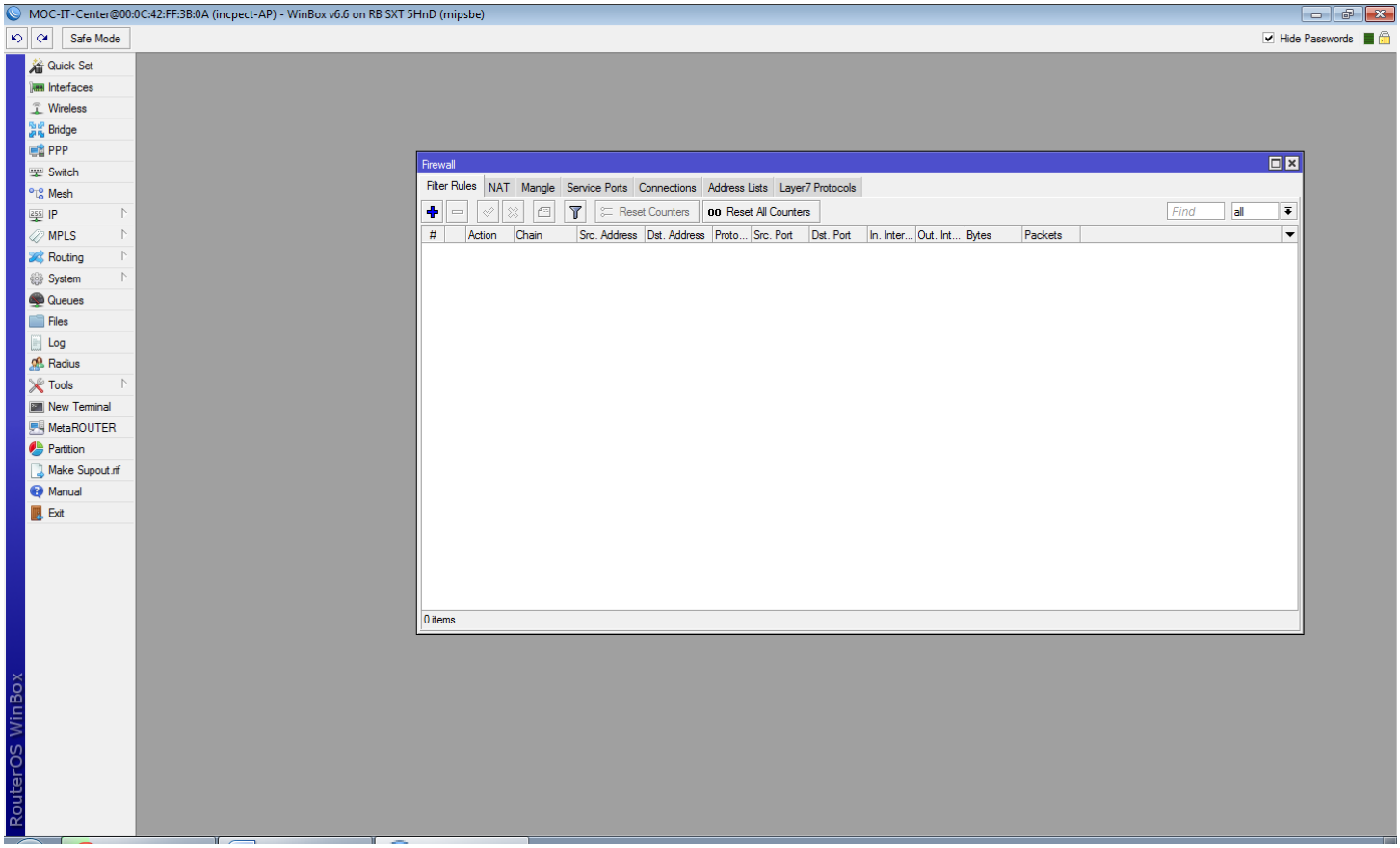


وهكذا نكون قد قمنا بحجب مواقع معينة بأستخدام روترات المايكروتك .

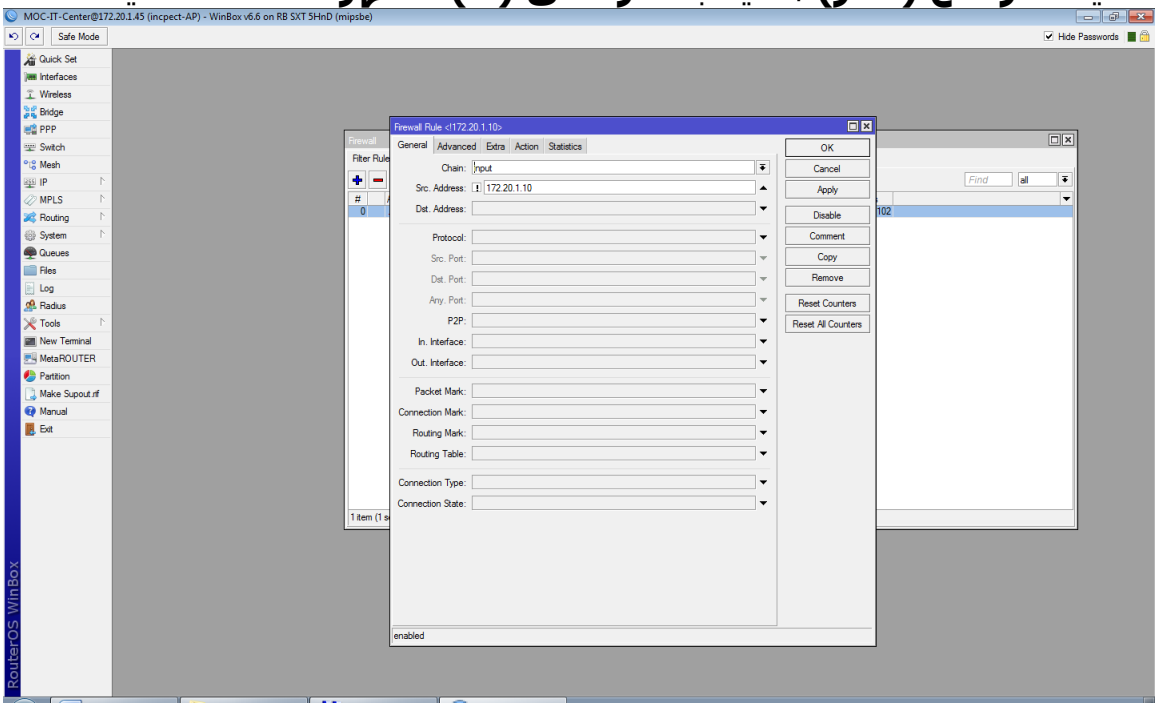
قفل المايكروتك لتحديد الدخول له من قبل المدير فقط

بعد ان عملنا في الدروس السابقة على ضبط اعدادات اجهزة المايكروتك في كل من طرفي الشبكة المحلية وهما السيرفر الذي يستلم الخدمة من ال (WAN) ويوزعها الى المستخدمين في الشبكة الداخلية (LAN) عن طريق الهوت سبوت او ال (point to point) او غيرها من الطرق المتعددة نصل اليوم الى مناقشة حقيقة مهمة وهي ان مدير الشبكة وبعد ان قام بنصب العشرات من الاجهزة في شبكته الداخلية لمؤسسة او حرم جامعة او شركة فهو بحاجة الى وضع اشارات على كل جهاز كأسم مميز للجهاز وللقسم او المكان الذي يخدمه ذلك الجهاز لتقليل زمن البحث عن الجهاز العاطل في حالة حصول خلل ما فبمجرد تبليغ قسم معين بوجود قطع في الخدمة لديهم سنذهب مباشرة الى الجهاز المسمى باسمهم والمسؤول عن ايصال الخدمة لهم ونقوم بعمل اعادة تشغيل له او (Reset) لإعدادات المصنع او اعادة ضبط اعداداته كما هو مطلوب وهكذا والامر الاخر المهم لكل مدير شبكة هو ان يمنع المستخدمين العاديين من الدخول الى اجهزة المايكروتك التي تزودهم بخدمة الانترنت لمنع التلاعب من قبلهم في البروفايلات وغيرها من الاعدادات التي يجب ان يعرفها ويشرف عليها مدير الشبكة فقط ويتم ذلك بمنع اي شخص من الدخول الى اجهزة المايكروتك عن طريق ال (winbox) عدا جهاز واحد فقط هو جهاز مدير الشبكة والذي يتحدد بعنوان (IP address) نحدده نحن ونسنده بشكل (static) فيما بعد الى اي جهاز نريد ان ندخل من خلاله الى الجهاز المراد ضبطه او اعادة ضبطه ويفضل ان يكون هذا العنوان سرياً لا يعرفه الا مدير الشبكة وان يكون موحداً لكل الاجهزة لمنع النسيان والاشتباه في حالة اختلاف عناوين الاجهزة المختلفة واليكم خطوات انجاز ذلك:

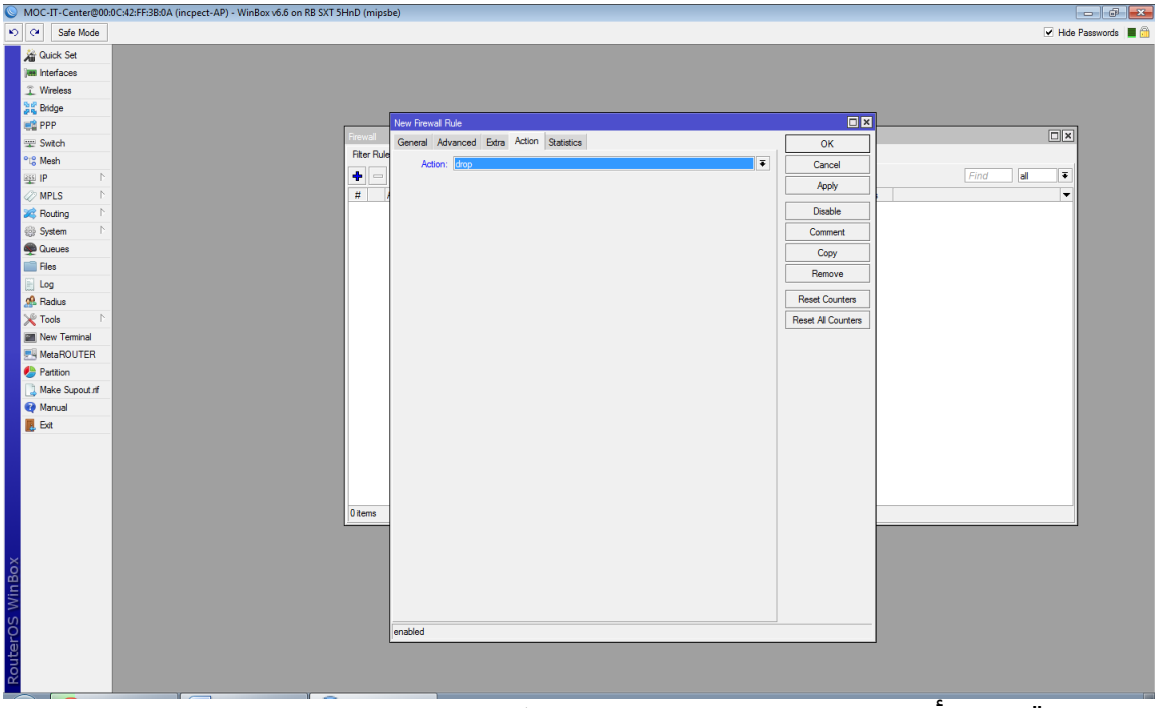
بعد اكمال ضبط اعدادات الجهاز عن طريق ال (Winbox) نقوم بالدخول الى قائمة (IP) ثم الى (firewall) لتظهر النافذة التالية:



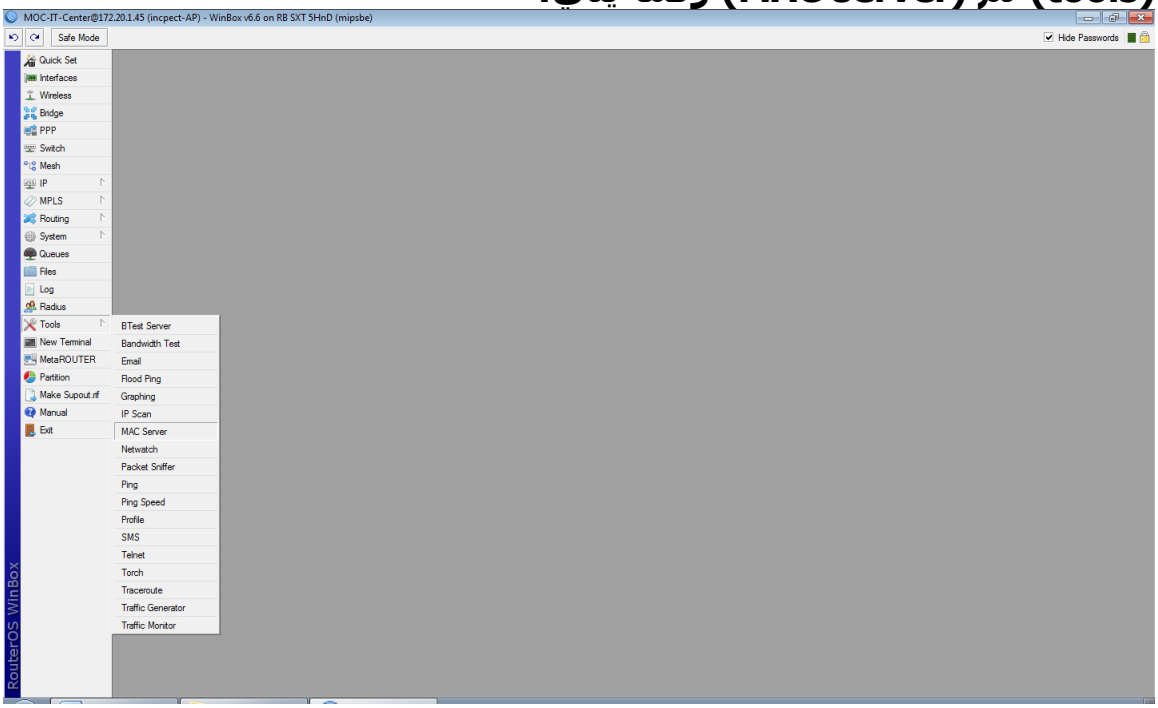
نضيف مرشح (فلتر) جديد بالنقر على (+) لتظهر النافذة التالية:



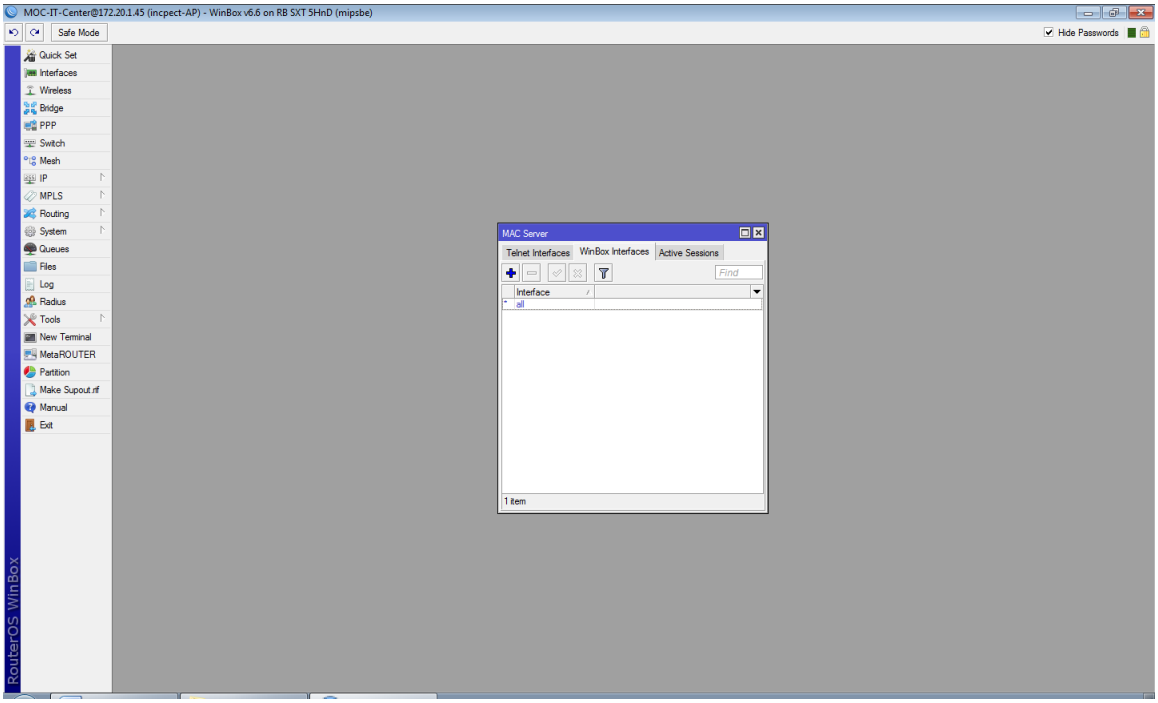
ونحدد نوع السلسلة ب(input) ونحدد عنوان ال(IP) الذي نريد ان يكون هو المنفذ الوحيد للدخول الى المايكروتك عن طريق ال (winbox) ثم نذهب الى تبويب (Action) ونحدد (drop) اي ان كل ادخال الى المايكروتك من اي عنوان عدا ال(IP address) الذي حددناه سيتم اهماله (drop it).



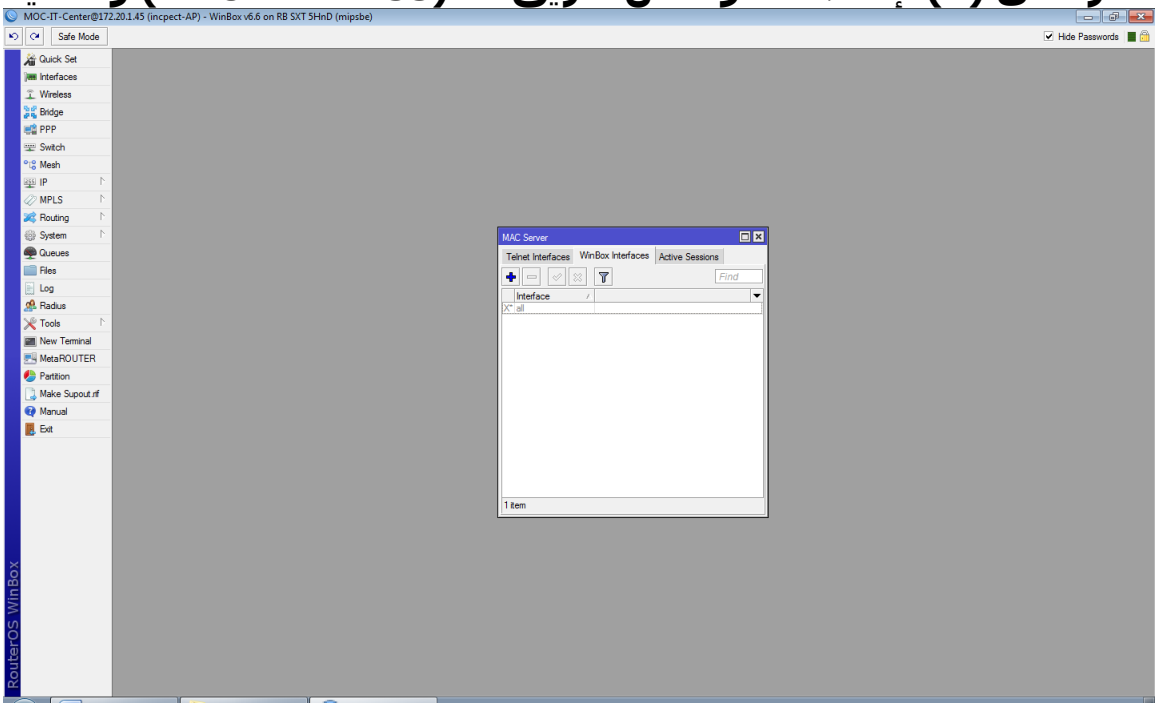
وبهذا قمنا بأغلاق الدخول الى المايكروتك من اي جهاز عدا ما حددناه ولكن يبقى بالإمكان الدخول عن طريق ال (MAC address) ويمكن منعه ايضاً بالذهاب الى قائمة (tools) ثم (MAC server) وكما يلي:



والان نقوم بالنقر على كلمة (all)التي تظهر في النافذة ادناه:



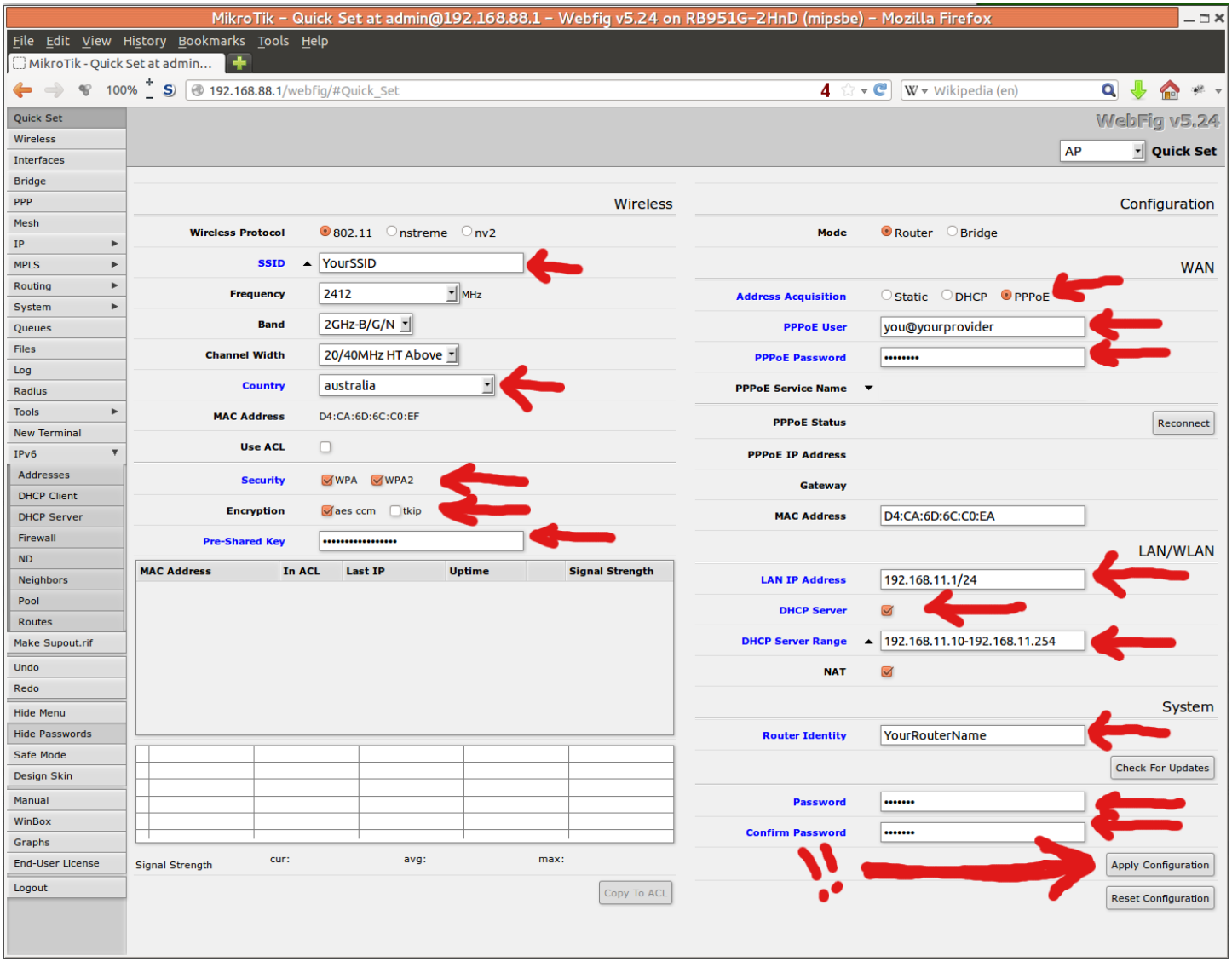
ننقر على (X) لإلغاء الدخول عن طريق ال (MAC ADDRESS) وكما يلي:



والان حين نحاول الدخول الى المايكروتك عن طريق ال (winbox) من اي عنوان (IP or MAC) فلن يستطيع الا حين نغير عنوان حاسوبنا الى العنوان الي حددناه سابقاً وليكن كمثال (172.20.1.10).

استخدام المايكروتك بدل ال(TP-Link) في الشبكات المنزلية والمحلية الصغيرة

يتساءل البعض عن امكانية استخدام اجهزة المايكروتك التي تحتوي على منافذ سلكية ولاسلكية كبديل لأجهزة ال (TP-link router) المنتشرة في المنازل والدوائر العامة بشكل كبير هذه الايام ويأتي الجواب بنعم كالعادة فالمرونة الكبيرة التي يتمتع بها هذا الجهاز تجعل من النادر الاجابة بلا عن اسئلة (هل يمكن؟) ورغم الفارق في السعر بين اجهزة ال (TP-link) والتي تتراوح بين ٣٠ الى ٤٠ دولار وبين اجهزة المايكروتك التي تحتوي منافذ سلكية ولاسلكية وبرخصة من المستوى الرابع فما فوق والتي يمكن ان تقوم بالدور المذكور وتتراوح اسعارها بين ٥٠ الى ٩٥ دولار في السوق هذه الايام، اقول رغم فارق السعر الا ان المايكروتك يوفر حلول امنية وكفاءة ووثوقية اكثر بكثير مما يوفرها ال(TP-link) واما كيفية ضبط اعدادات المايكروتك ليعمل على استلام الخدمة من مزود الخدمة (ISP) ويبث الانترنت للمشتركين والذين يستطيعون الدخول الى الانترنت بعد معرفة الكلمة السرية (security key) فبعد الدخول على الجهاز الذي يجب ان يحتوي منافذ سلكية (input) ولاسلكية (output) للبث وبنظام تشغيل (RouterOS) برخصة من المستوى الرابع فما فوق نقوم بالنقر على اول تبويب في الجانب العلوي الايسر (Quick set) وكما في النافذة التالية:

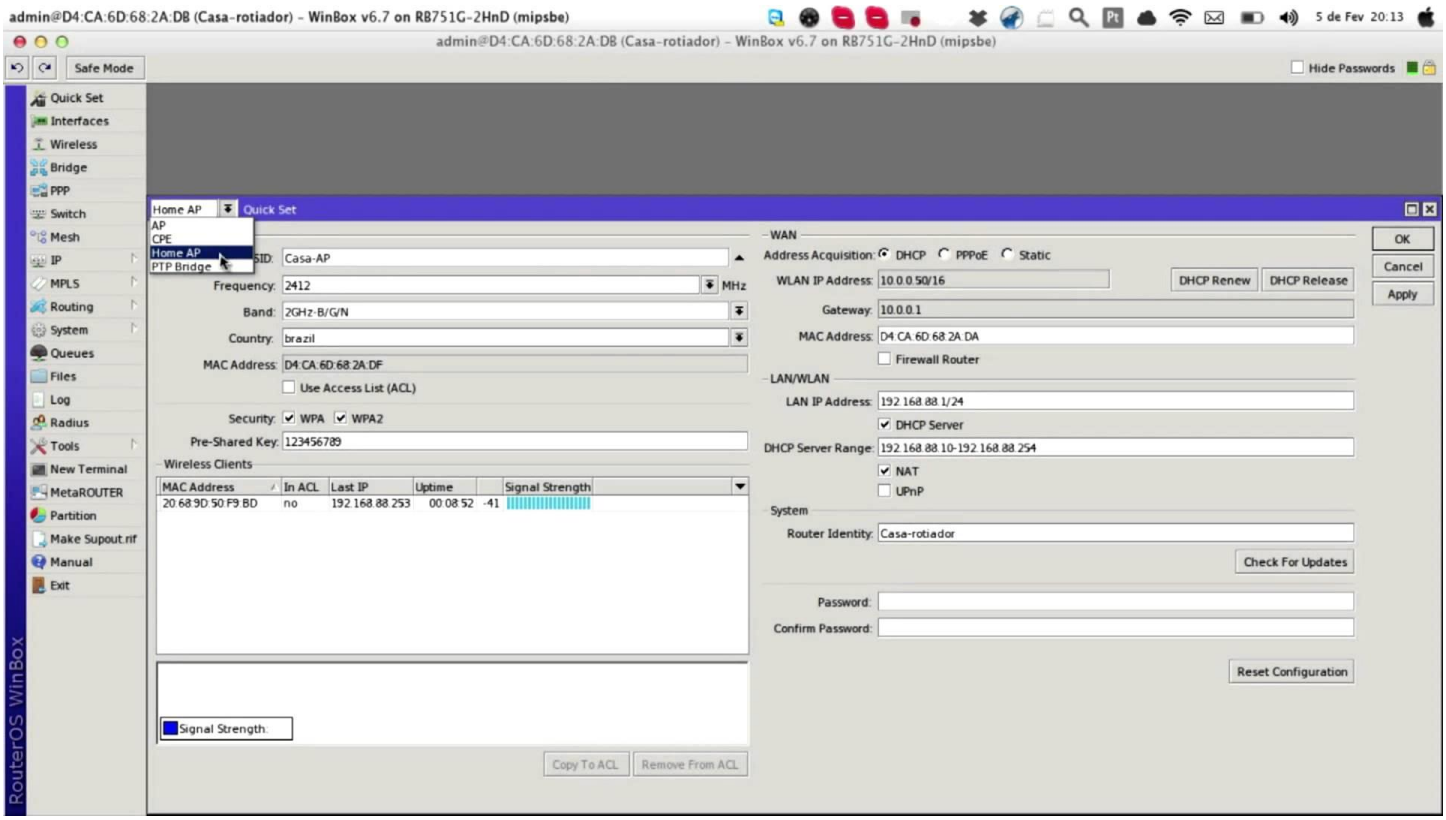


نقوم بتحديد نوع طور العمل ب (AP) او (Home AP) من الجهة العليا اليمنى وبعدها نقوم بملء المعلومات التالية:

١- نقوم بتحديد نمط العمل (mode) ب (PPPOE).
٢- نقوم بوضع اسم المستخدم الذي استلمناه من مزود الخدمة في حقل ال (PPPOE user).
٣- نضع كلمة المرور في حقل (PPPOE password) .
٤- نختار نوع الامنية (security) ليكون (WPA or WPA2) .
٥- نكتب مفتاح الامان للشبكة والذي يجب اعطائه للمستخدمين ليستطيعوا الدخول عن طريقه للشبكة في حقل (Pre-shared key).
٦- يفضل ابقاء بقية اعدادات الجهاز كما هي واخيراً ننقر على (apply configuration) .
٧- يجب التأكد من ان جهازنا يعمل على البروتوكول (802.11 b or g or a) اي انه يبث الانترنت بتردد (2.4 GHz) ليكون بإمكان اجهزة الحاسوب المزودة بكرت

شبكة لاسلكية واللابتوبات واجهزة الهواتف الذكية والاجهزة اللوحية الاتصال مباشرة بالشبكة لأن جميعها تعمل متوافقة مع ال (Wireless Fidelity WIFI).

٨- ملاحظة اخيرة وهي ان النافذة اعلاه هي ليست من برنامج ال (Winbox) وانما لبرنامج اخر من ادوات المايكروتك ويسمى (Web fig) ويتم الدخول اليه من خلال متصفح الانترنت ولن تكون نافذة ال(winbox) مختلفة كثيراً بل ستكون كما في الصورة التالية:

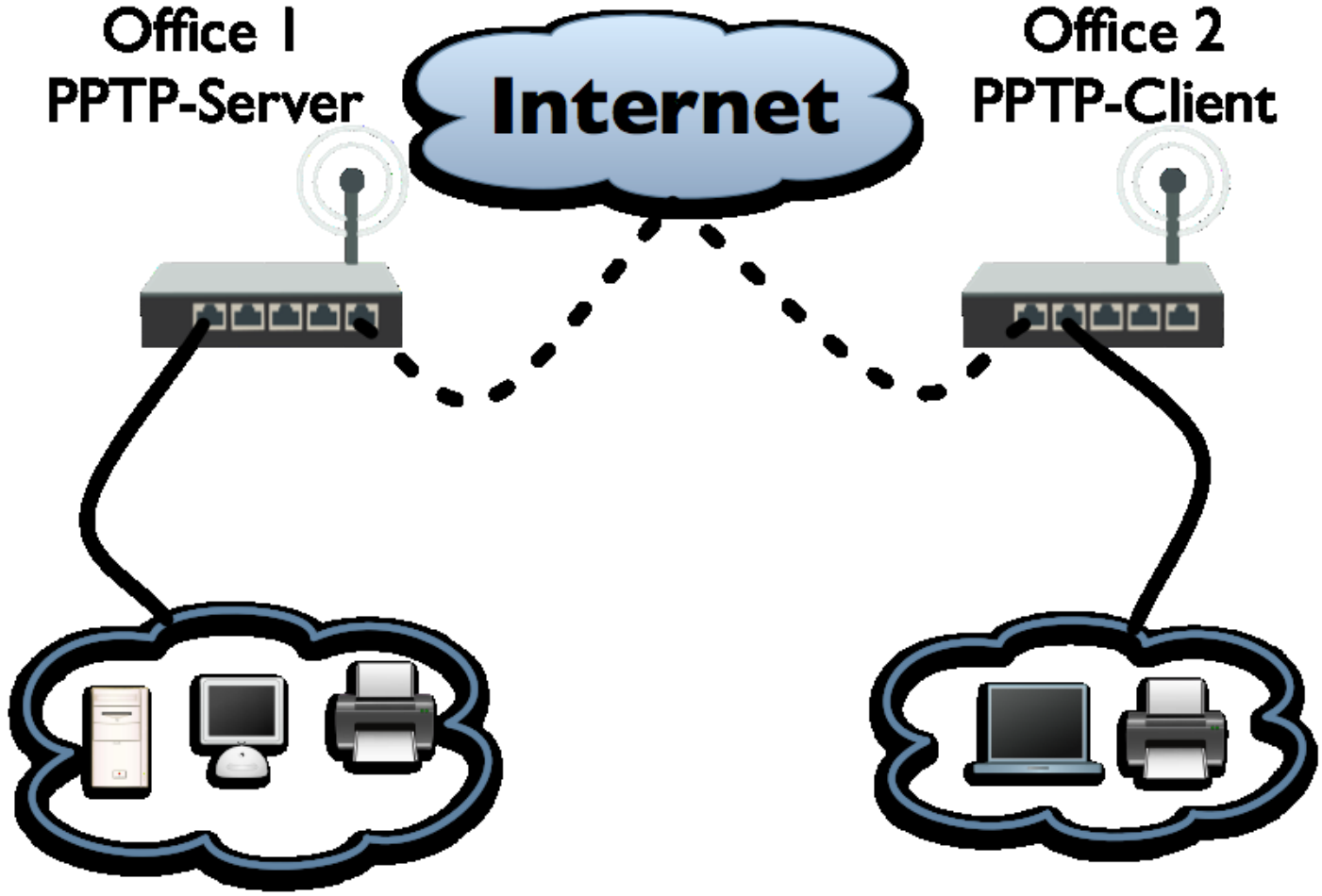


بروتوكول التحكم بالجسر (Bridge Control Protocol BCP)

ذكرنا في الدرس السابق انواع الاتصال النفقي عبر بيئة سلكية او لاسلكية ونكمل اليوم حديثنا عن دعم هذه الانواع في نظام تشغيل المايكروتك حيث يوفر النظام تطبيق يدعم بروتوكول التحكم بالجسور والذي يسمح بعمل جسر ايثرنت بين الروابط من نقطة الى نقطة وتعتبر عملية انشاء جسور ال BCP جزءاً من استراتيجية الاتصال من نقطة الى نقطة عبر نفق افتراضي وهي لا ترتبط لأي عناوين IP وانما تحصل عملية الاتصال النفقي مع التوجيه والعبور من الجسور bridging في نفس الوقت بشكل مستقل ويمكن استخدام بروتوكول BCP بدلاً من نفق الشبكة الخاصة الافتراضية VPN او روابط نظام التوزيع اللاسلكي WDS في الشبكات الكبيرة والصغيرة على حد سواء. وللعمل على هذا البروتوكول يجب تفعيله وتمكينه في كل من طرفي الاتصال (PPP client and PPP server) وفي ادناه شرح تفاصيل ذلك للسيناريو الطبيعي في المخطط ادناه:

مثال تطبيقي

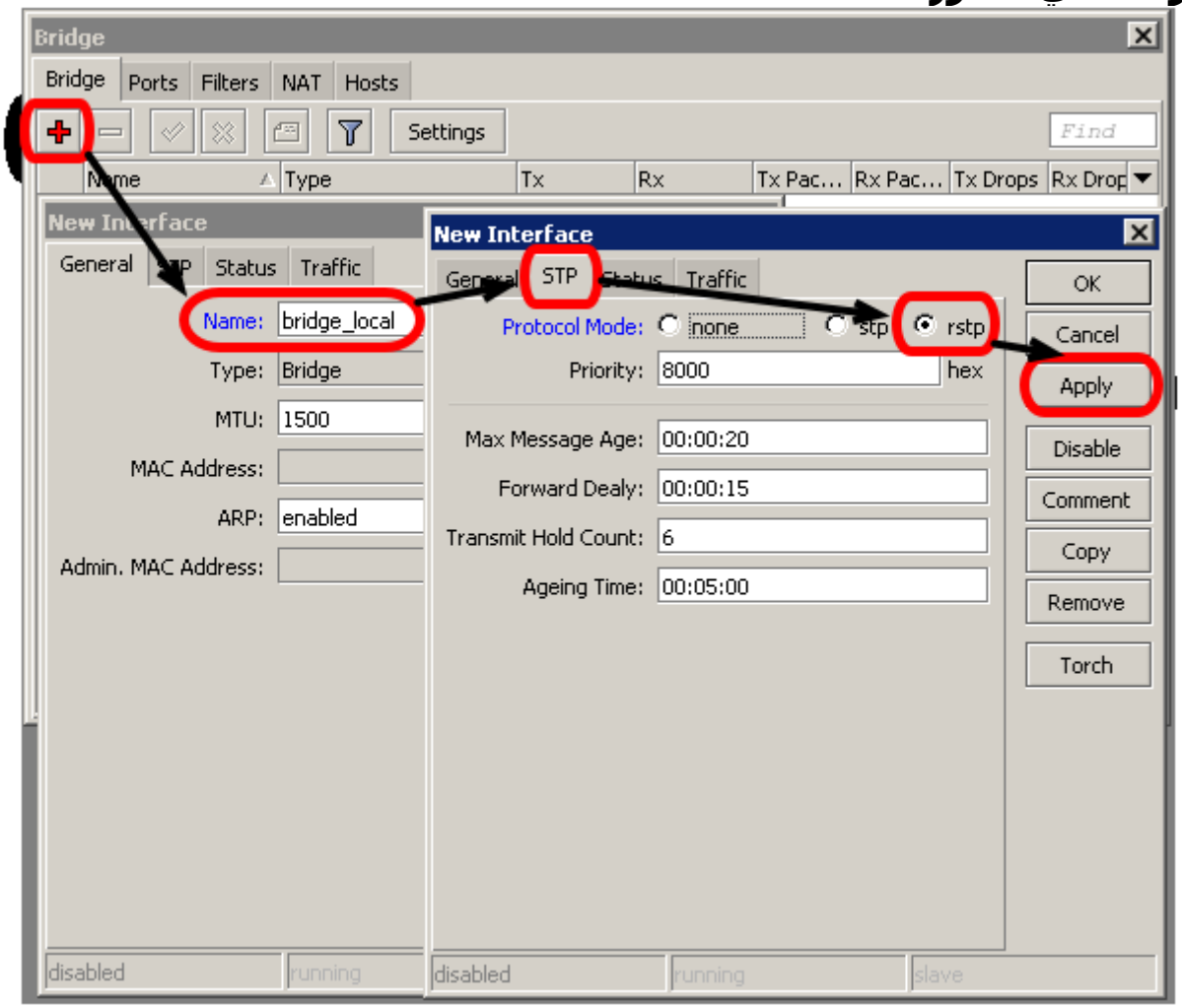
عادة نحتاج الى ربط بنايتين او شركتين متباعدتين بشبكة ايثرنت ليبدوان كأنهما جزء من شبكة واحدة ولضمان الامنية والخصوصية يجب تشفير وحماية البيانات المرسلة بين هاتين الشركتين والان سنرى كيف نجعل ذلك ممكناً باستخدام BCP وللشبكة في المخطط:



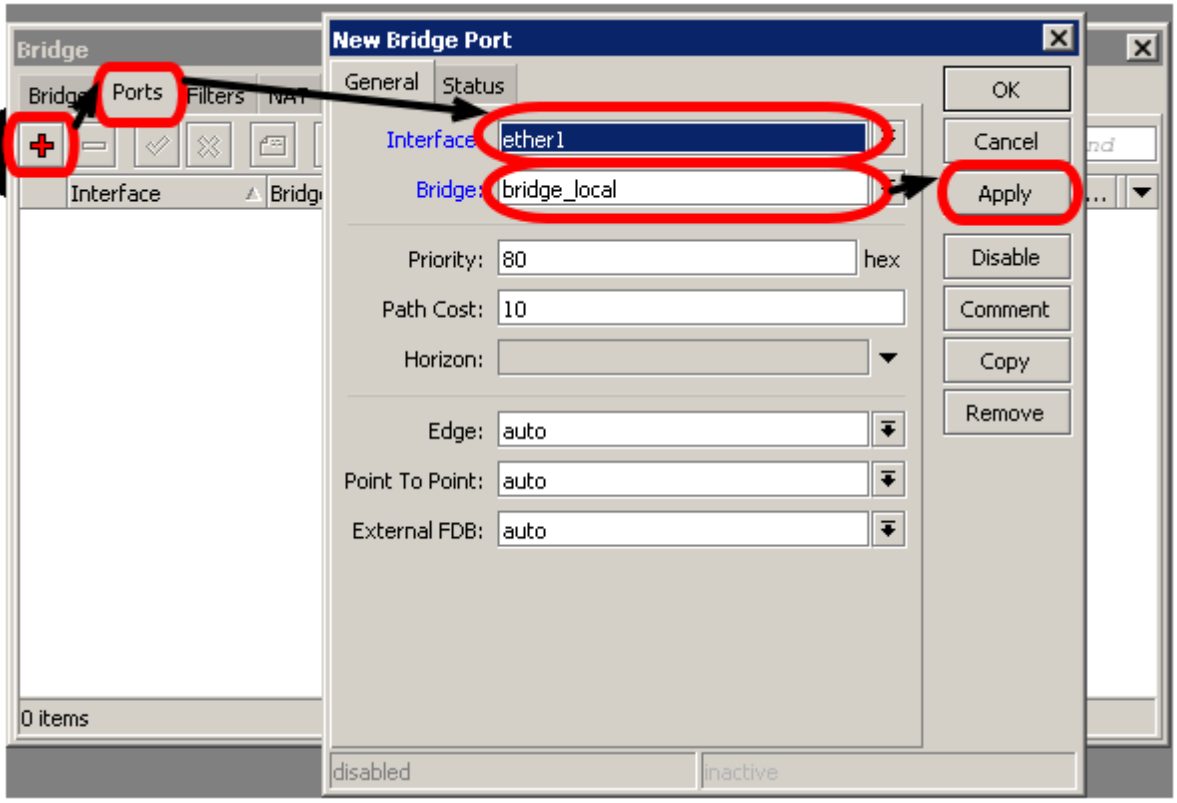
والان بعيداً عن سطر الاوامر وال new terminal نقوم بضبط اعداداتنا لطرفي الشبكة باستخدام برنامج win box ونبدأ بالبناية الاولى:

ضبط البناية الاولى:

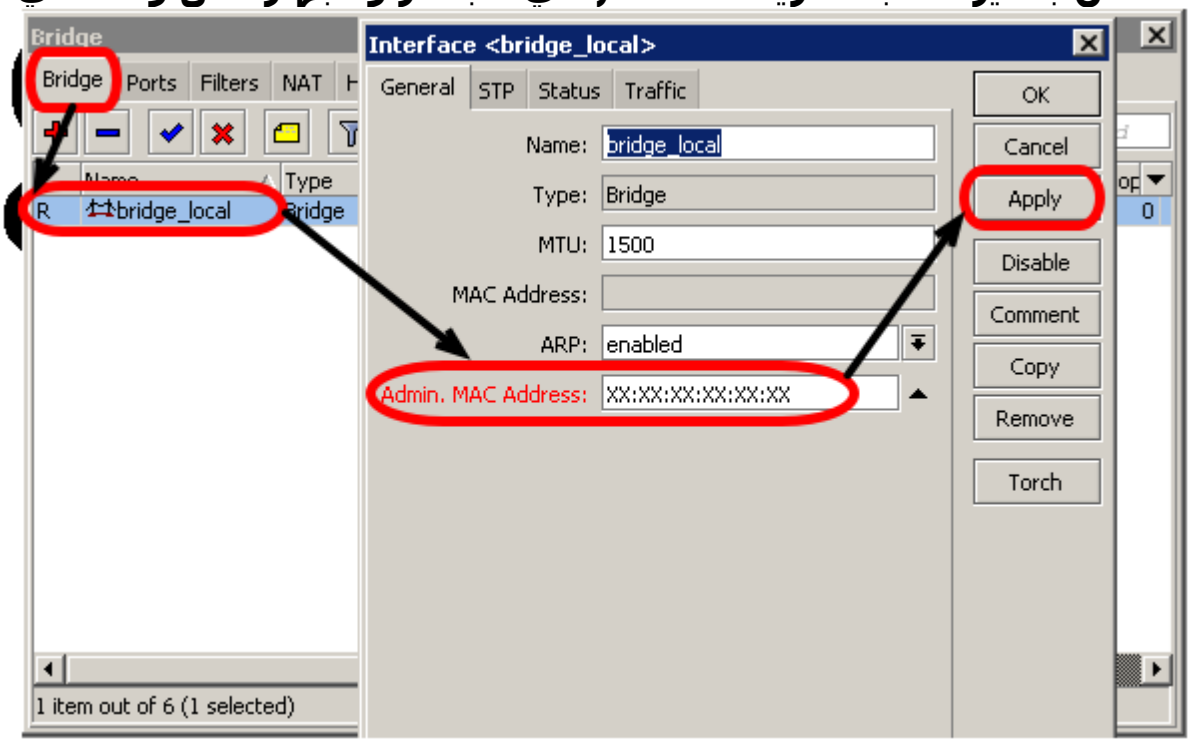
بعد ضبط الاعدادات الاولية للجهاز كما في الدروس السابقة نقوم بأنشاء جسر bridge وكما في الصورة ادناه:



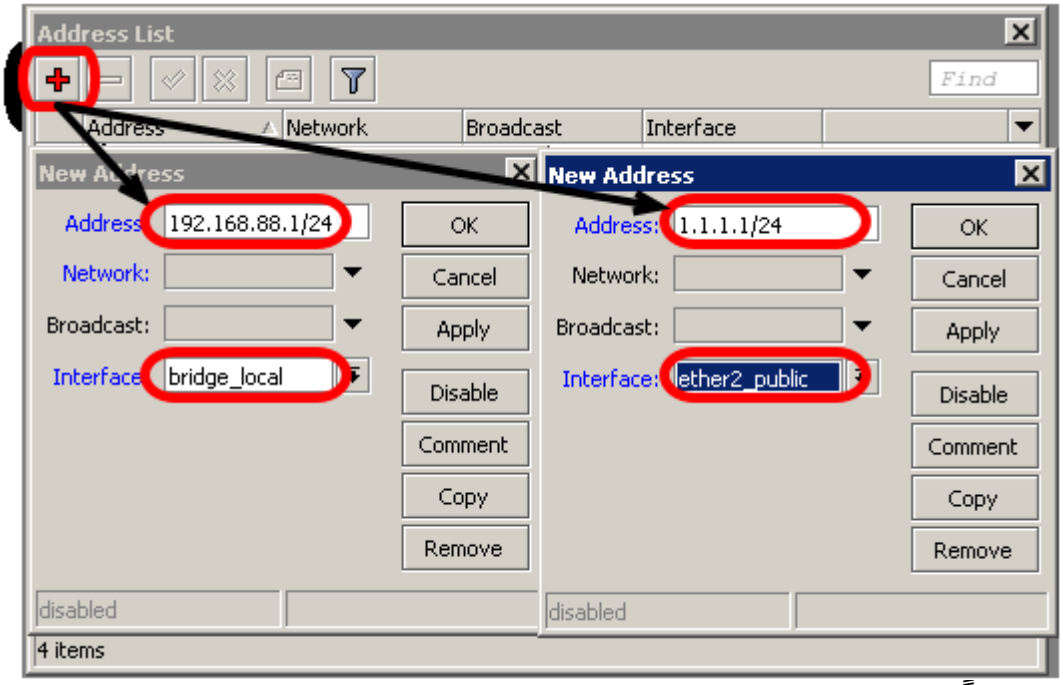
والان نضيف المنافذ الى الجسر وهي المنافذ التي نريد لها ان ترتبط بشكل مباشر وكما في الصورة ادناه:



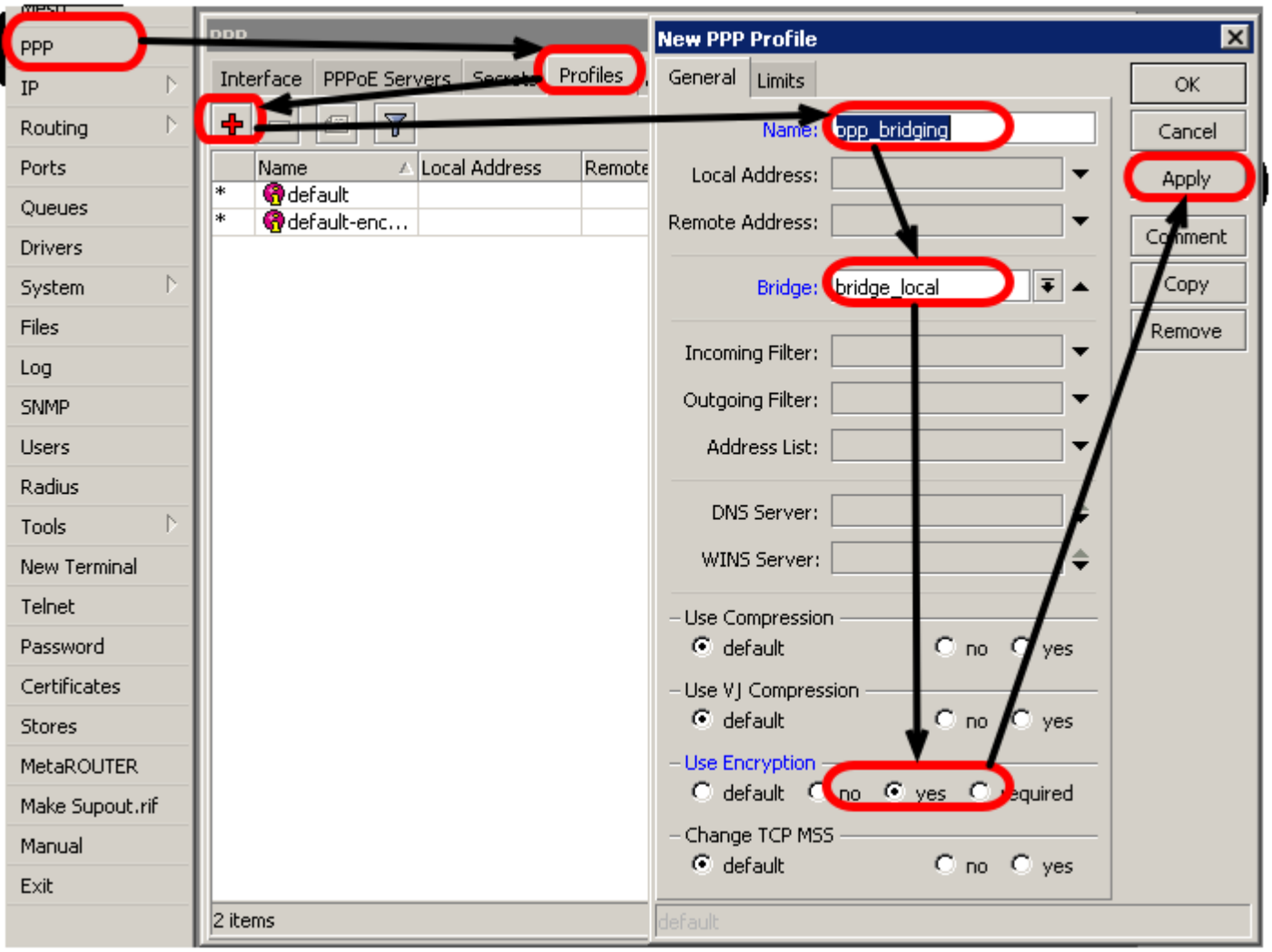
والان نضيف العنوان الفيزيائي الى الجسر ويجب ان يكون هو نفسه ال MAC address الخاص بمدير الشبكة لزيادة التحكم في الجسر والجهاز ككل وكما في الصورة ادناه:



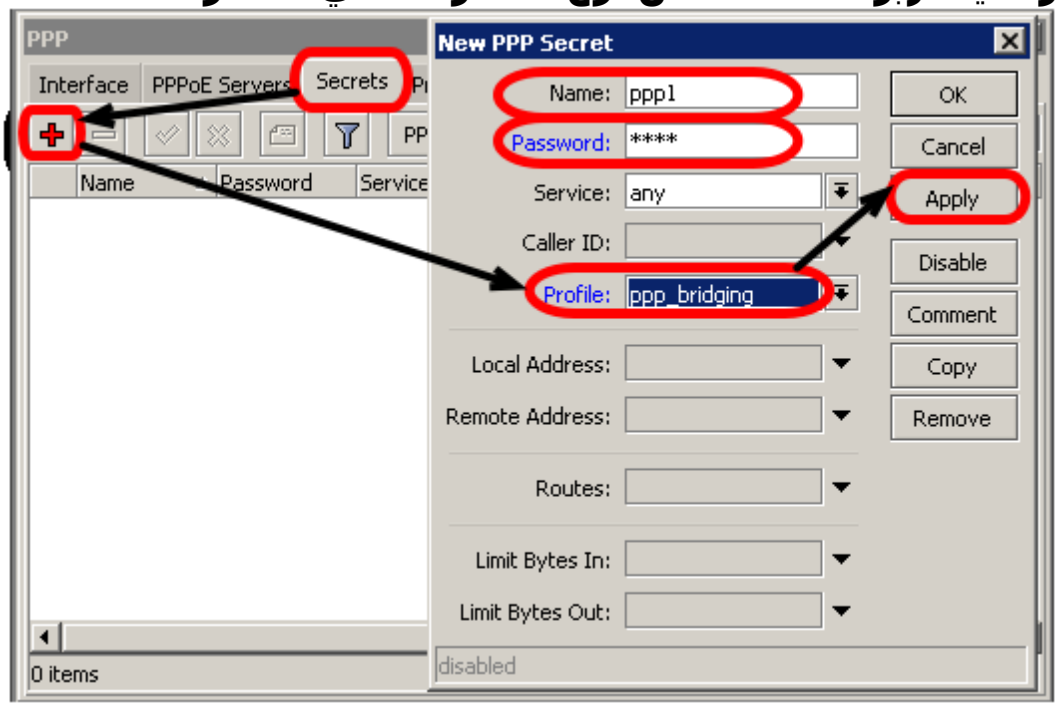
والان نسند العنوان المنطقي الى الجسر IP address وكما في الخطوات ادناه:



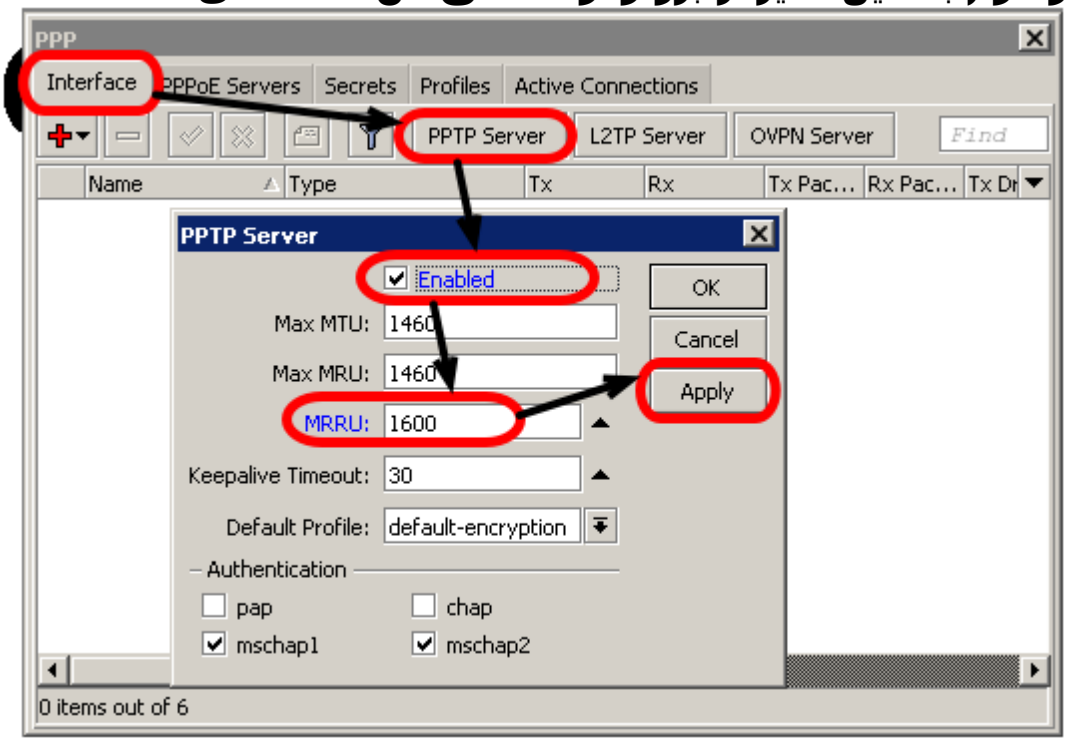
واخيراً نصل الى الخطوة الاكثر اهمية وهي انشاء بروفايل (حساب او اعداد) للاتصال من نقطة الى نقطة وكما في الخطوات الموضحة في ادناه:



ونضيف زبون للاتصال من نوع PPP وكما في الخطوات ادناه:



ونقوم بتفعيل سيرفر بروتوكول النفق من نقطة الى نقطة PPTP وكما يلي:

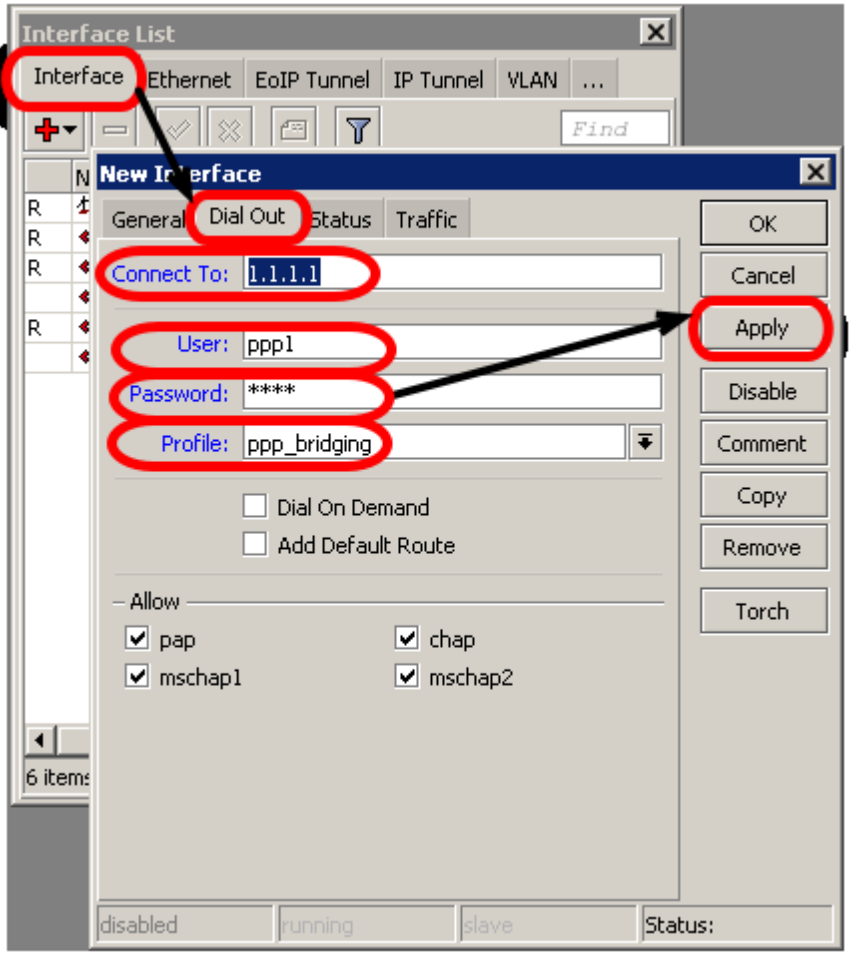


وبذلك تنتهي اعدادات الدائرة الاولى وننتقل الان ال اعدادات الدائرة او الشركة الثانية وكما يلي:

ضبط الشركة الثانية:

تتشابه الاعدادات الى حد كبير بين جزئي الشبكة ويختلف فقط ان ما تم ضبطه في الطرف الاول ك (client) فيجب ان يضبط الان ك (server) والعكس بالعكس وكما يلي:

نضيف زبون لل PPTP وكما يلي:



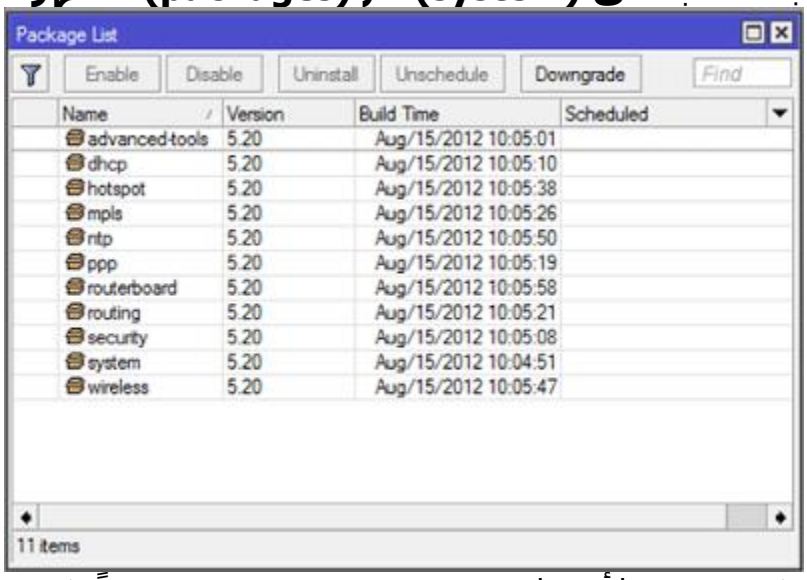
ونضبط اسم المستخدم وكلمة المرور التي يستطيع الزبون الدخول من خلالها والاتصال بالطرف الاخر والتي يتم ضبطها واعدادها في الطرف الاخر من قبل ال PPTP server وتعطى الى الزبون لحفظ السرية والامنية والفهم المتبادل لطرفي الشبكة .

مدير المستخدمين في المايكروتك (User Manager in Mikrotik)

بعد ان شرحنا في مقال سابق ما هو سيرفر ال (Radius) وعلمنا وظيفته التي تتلخص في (AAA) اي (Authentication, Authorization, and Accounting) وتعني انه السيرفر المسؤول عن التحقق من المستخدمين ومنح الصلاحيات الخاصة بكل منهم وتسجيل وخزن سجل بكل فعاليات كل منهم، بعد كل ذلك نأتي الى كيفية تفعيل هذه الخدمات في المايكروتك وكما هو واضح فأن المسؤول عن هذه الصلاحيات هو مدير الشبكة والذي يقوم بتفعيل مدير المستخدمين ليسهل عليه فعل الامور سابقة الذكر. اذاً باختصار فأن مدير المستخدمين هو سيرفر ال (Radius) الخاص بالمايكرو تك ويتم تفعيله وتشغيله كما يلي:

اولاً: تنصيب مدير المستخدمين:

بداية نتأكد من وجود الحزمة الخاصة بهذا التطبيق ضمن حزم وملفات المايكروتك بالذهاب الى (system) ثم (packages) لتظهر نافذة مشابهة للتالي:

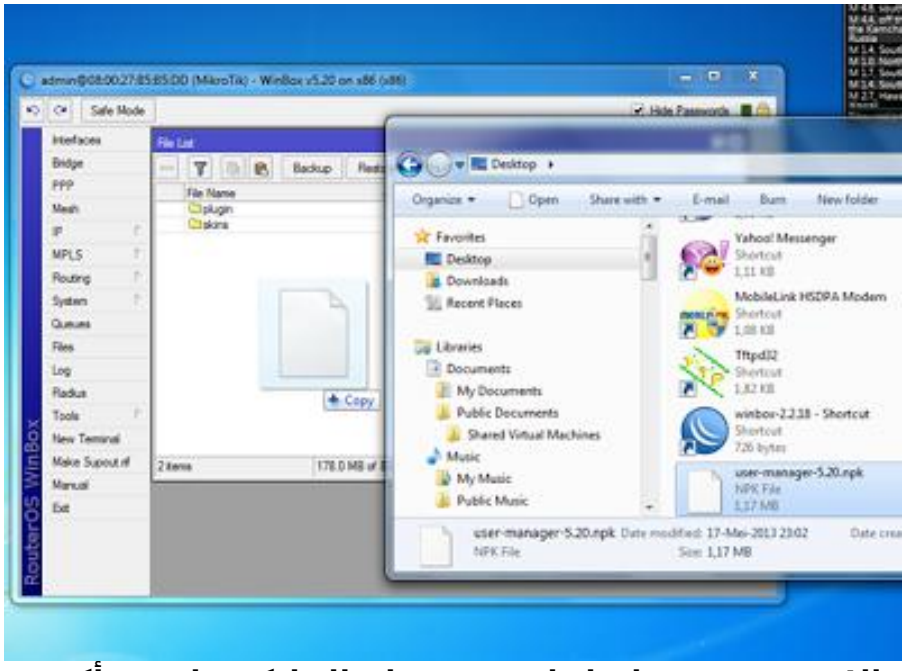


وكما نرى فأنه في الوضع الطبيعي تلقائياً يكون غير موجود لذا يتطلب الامر منا تنزيله من موقع الشركة (www.mikrotik.com) وبنسخة مماثلة للنسخة المنصبة حالياً في اجهزة المايكروتك خاصتنا واذا احتجنا الى نسخ قديمة في حالة كون نظام تشغيل المايكروتك المنصب لدينا الان قديم نستطيع تنزيلها من المواقع التالية:

http://files.shelbybb.com/mikrotik/

http://204.62.56.64/mikrotik/

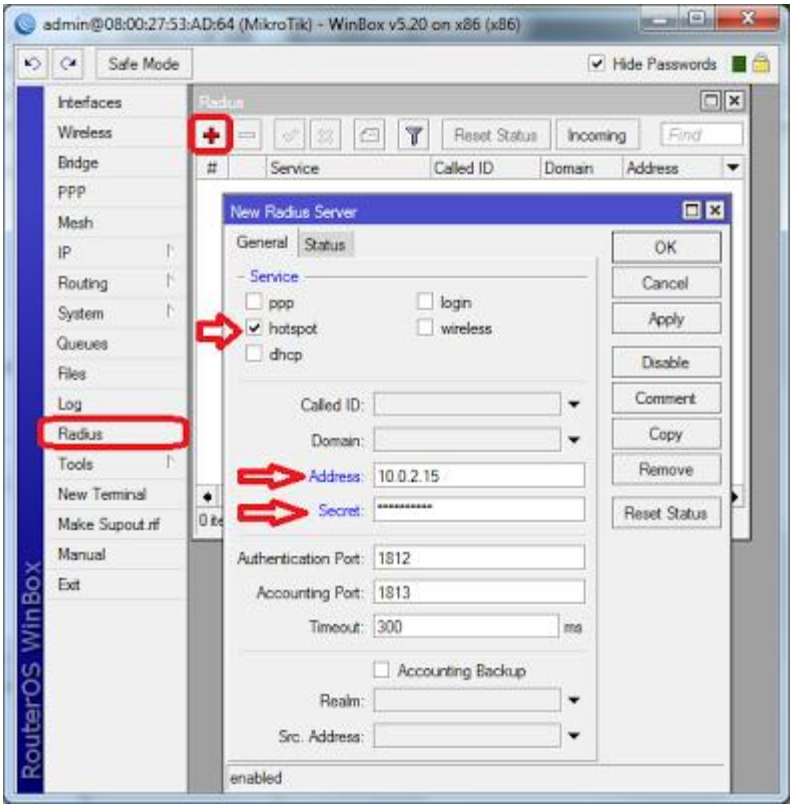
والان بعد تنزيل الحزمة نقوم بفتح ال(winbox) ونذهب الى تبويب الملفات (files) ثم نقوم بسحب وافلات الحزمة الى داخل نافذة ال(winbox) كما في الصورة التالية:



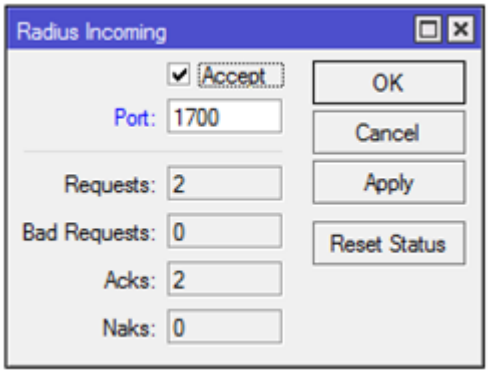
والان نقوم بعمل اعادة تشغيل المايكروتك ونتأكد من تفعيل الحزمة المضافة حديثاً (مدير المستخدمين) فنذهب الى تبويب الملفات فنجدها قد ظهرت.

ثانياً: ضبط اعدادات مدير المستخدمين:

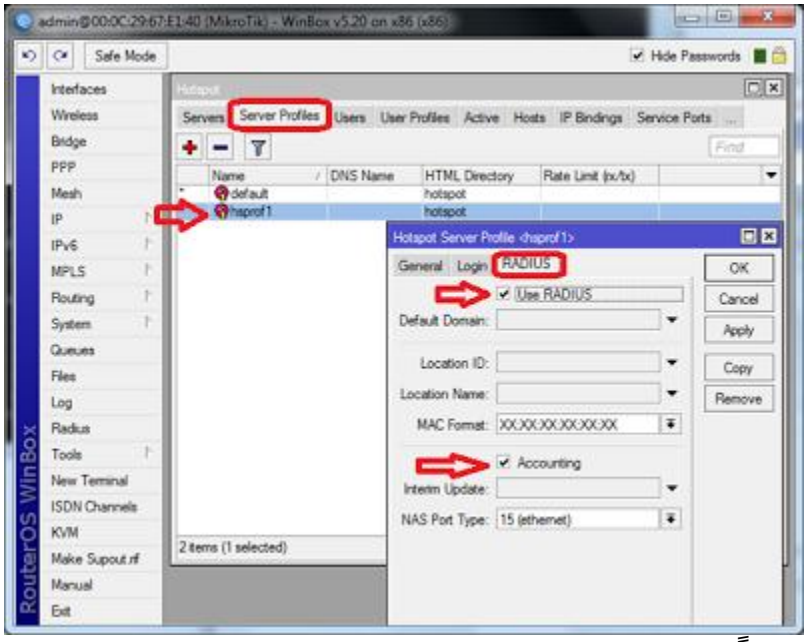
بداية يفترض اننا قمنا بتفعيل وتشغيل المايكروتك كهوت سبوت (كما تم شرح ذلك في مقالات سابقة ضمن سلسلة المايكروتك) والان نقوم بفتح ال(winbox) والذهاب الى (Radius) ثم النقر على اشارة (+) لتظهر نافذة نختار منها نوع السيرفر (hotspot) ونقوم بأدخال عنوان (IP address) الخاص بمنفذ ال(WAN) لراوتر المايكروتك او ببساطة نقوم بجعله (127.0.0.1) ونفعل منافذ التحكم ونقوم بأدخال كلمة سر خاصة بمدير النظام (secret) ولتكن (testing123) كمثال ثم (ok) وكما في النافذة التالية:



والان نعود الى نافذة ال (Radius) وننقر على (Incoming) ونؤشر امام خيار (accept) وندخل رقم المنفذ (1700) كما في النافذة ادناه:



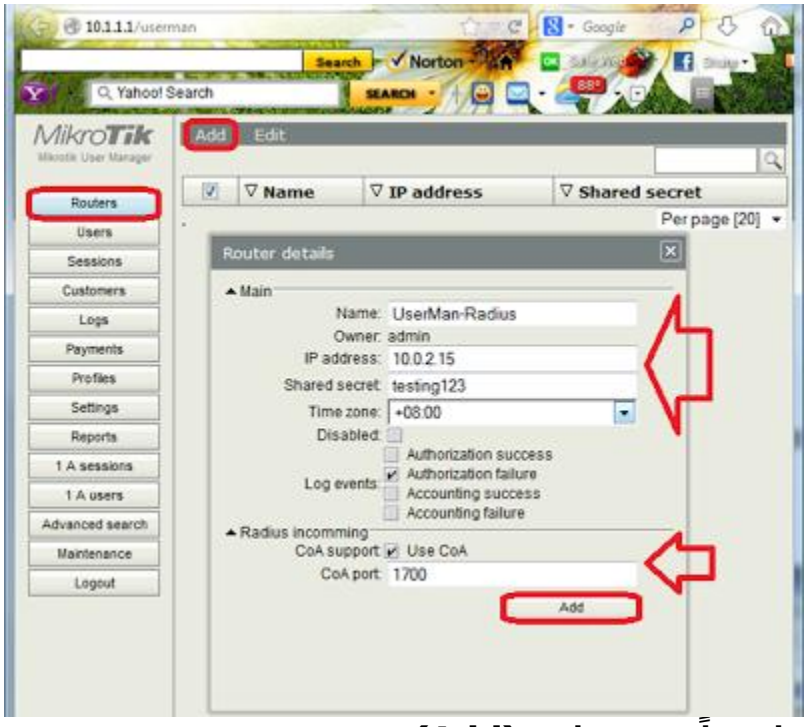
والان نذهب الى تبويب (IP) في ال (winbox) ثم الى (hotspot) ثم ننقر على (server profile) ثم نقرة مزدوجة على (hsprof1) وهو سيرفر الهوت سبوت الذي يفترض ان نسيطر على مستخدميه بواسطة مدير المستخدمين لتظهر نافذة نؤشر فيها امام خيار (use radius) وخيار (accounting) وكما في النافذة التالية:



ثالثاً: اعداد مدير المستخدمين في المايكروتك:

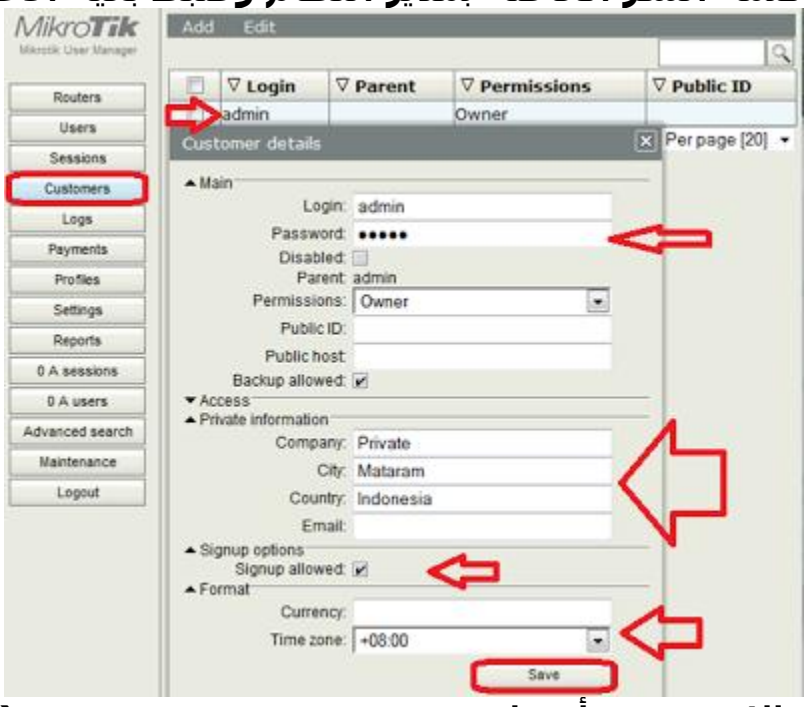
نذهب الى متصفح الانترنت ونكتب في خانة العنوان (IP address/userman) وهنا نقصد ب(IP address) هو العنوان الذي ادخلناه في بداية الشرح في سيرفر ال (Radius) والذي قلنا انه اما ان يكون عنوان (Router WAN address) او (127.0.0.1) وعندما يطلب اسم المستخدم وكلمة المرور فهي كالعادة لكل منتجات مايكروتك (admin) لأسم المستخدم وفراغ لكلمة السر في نافذة كما يلي:

والان نبدأ اعدادات المايكروتك في مدير المستخدمين بالذهاب الى تبويب (Router) ثم (Add) ثم (new) ثم نقوم بأدخال المعلومات كما في النافذة ادناه:



واخيراً ننقر على (Add)

والان وقبل بدء انشاء المستخدمين لأدارتهم يجب الانتباه الى المسألة الامنية بتغيير كلمة السر الخاصة بمدير النظام وضبط بقية الاعدادات كما في النافذة ادناه:



والان نقوم بأنشاء مستخدم جديد من تبويب (users) ومنحه اسم مستخدم وكلمة مرور والذهاب الى حاسوب هذا المستخدم وتجربة الدخول الى الانترنت من خلال حاسبته فأن نجح في الدخول الى الانترنت فهذا يعني نجاح عملية انشاء مدير المستخدمين وبدء العمل على ادارة المستخدمين من خلاله.

ضبط اعدادات مدير المستخدمين في المايكروتك

بعد ان عرفنا كيفية تفعيل مدير المستخدمين في المايكروتك وكيفية الوصول اليه عن طريق متصفح الانترنت، نأتي اليوم الى ضبط اعداداته والتحكم في المستخدمين فيه وكما يلي:

يحتاج مدير الشبكة بصورة عامة الى ضبط الامور التالية التي تخص المستخدمين:

١- اسم المستخدم وكلمة المرور.
٢- مدة استخدام الانترنت بحسب طريقة الدفع ومقدار الدفع (يومي، اسبوعي، شهري، .... الخ).
٣- نوع الامنية التي تستخدم في تشفير وتأمين البيانات وخصوصية المستخدم.
٤- بروفايل المستخدم الذي يتضمن الحد الاعلى لسرعة ارسال واستقبال البيانات ولكل نوع من انواع الاشتراك.

في ادناه سنقوم بشرح كيفية اجراء هذا الخطوات في مدير المستخدمين لأنظمة المايكروتك فنبدأ على بركة الله تعالى:

بداية يجدر الاشارة الى ان هناك طريقتين لضبط قوائم الدفع بالنسبة للمستخدمين استناداً الى وقت معين (شهر واحد مثلاً) او الى فاتورة دفع بمبلغ معين كأن تكون واحد كيكا بايت بسعر خمسين دولار نافذة لمدة شهر (كما هو حاصل في الاشتراك الشهري للأنترنت في شركات الهاتف المحمول في الكثير من الدول الشرق اوسطية) علماً انه يمكن دمج الطريقتين في بروفايل واحد كما سنرى وباختصار يمكن ان تكون فاتورة الدفع للمستخدمين بالشكل التالي:

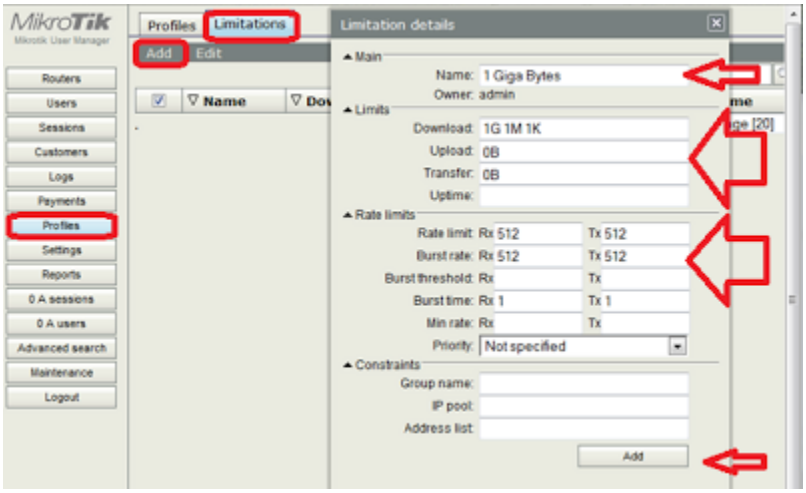
١- فاتورة بسعر (٥٠ دولار مثلاً) لساعتين في اليوم ونافذة لمدة ١٠ ايام (مثلاً).
٢- فاتورة بسعر (٦٠ دولار مثلاً) لحجم تحميل اقصى مقداره ١٠ كيكا بايت ونافذة لمدة شهر مثلاً.

المرحلة الاولى: الدخول الى مدير المستخدمين

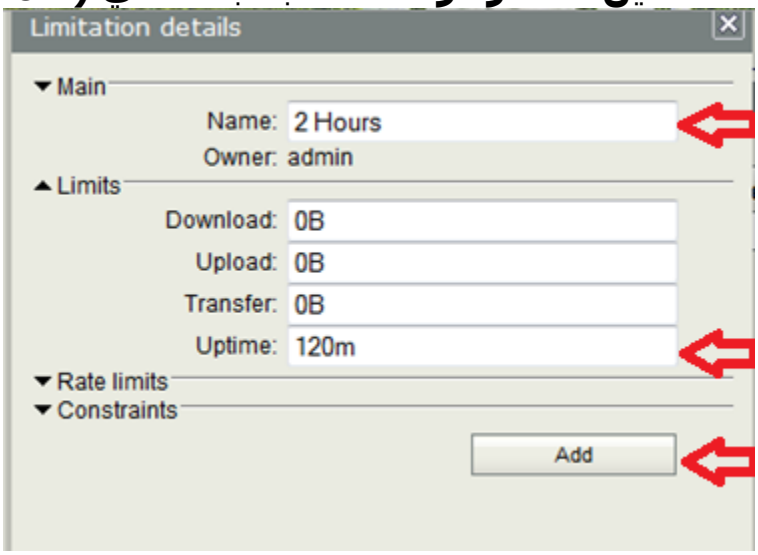
وكما كرنا سابقاً تتم بالدخول الى متصفح الانترنت وكتابة عنوان ال (IP address) الخاص بمنفذ ال (WAN) للمايكروتك او اي عنوان اخر تم ضبطه ثم (/ back slash) ثم (userman) لتظهر نافذة الدخول التي نضع فيها اسم المستخدم (مدير النظام) وكلمة المرور كما فعلنا في الدرس الماضي.

المرحلة الثانية: ضبط اعدادات البروفايلات الخاصة بكل نوع من انواع المستخدمين:

بعد الدخول الى مدير المستخدمين ننقر على تبويب (profiles) ثم على تبويب القيود (limitations) ثم ننقر على زر الاضافة (add) ونقوم بملء الخيارات المتاحة بحسب ما نريد حيث نعطي اسم للبروفايل وليكن (1 Giga Bytes) ونحدد الحد الاعلى للتنزيل (download) وليكن واحد كيكا بايت ونحدد كذلك اقصى معدل ارسال (Tx) واستقبال (Rx) وبقية القيود الاخرى بحسب الحاجة ثم ننقر على (Add) وكما في النافذة التالية:

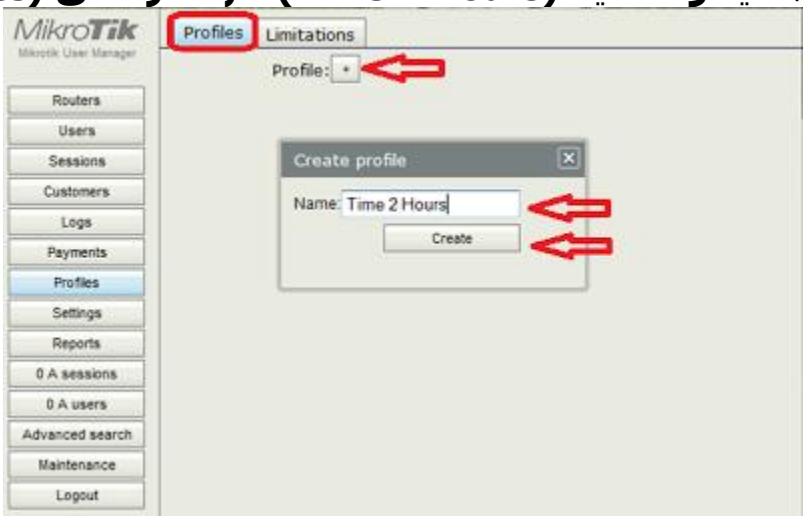


والان نكرر نفس العملية السابقة وبدل ان نختار اسم البروفايل (1 Giga Bytes) نسميه هذه المرة (2 Hours) والفائدة منه جعل مدة عمل هذا البروفايل يعمل لساعتين فقط وهو ما قمنا بضبطه في (up time= 120m) وكما في النافذة التالية:

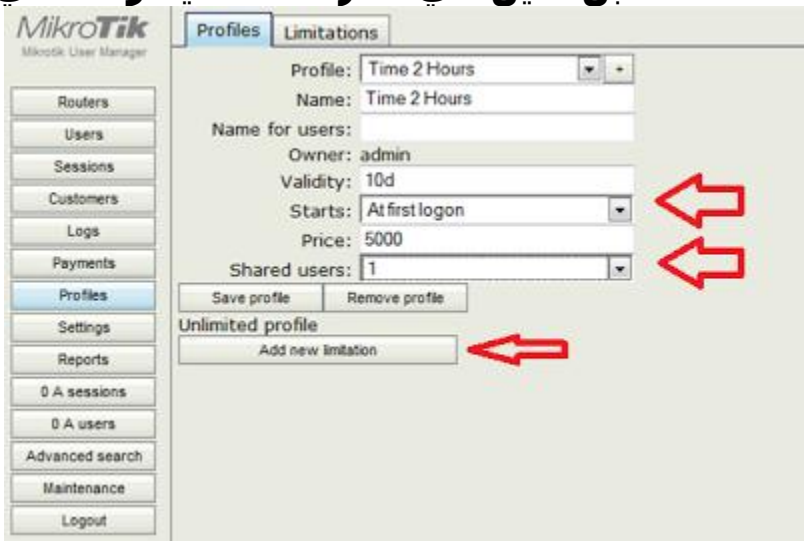


المرحلة الثالثة: خلق بروفايل جديد وتطبيق القيود عليه حسب الحاجة:

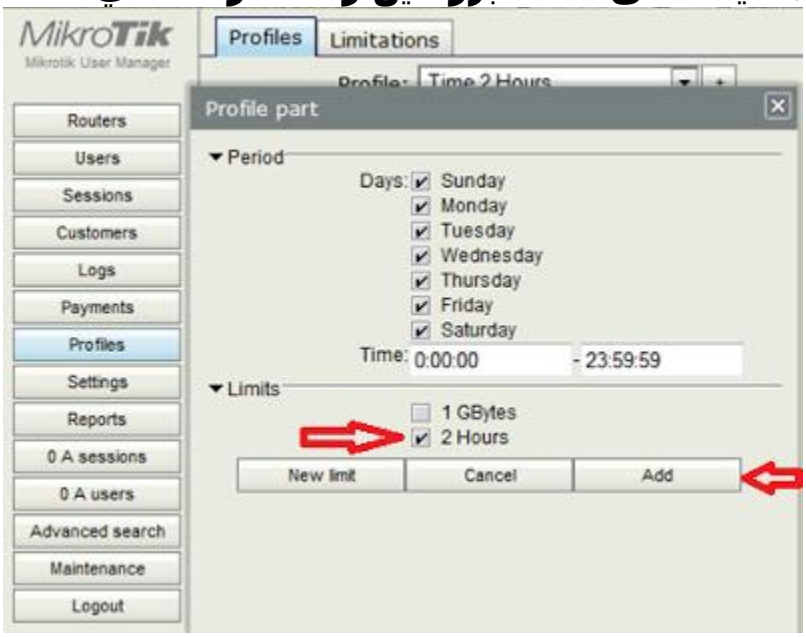
الان ننقر على تبويب (profiles) مجدداً ثم ننقر على زر الاضافة (+) لخلق بروفايل جديد ونسميه (Time 2 Hours) ثم ننقر على (create) وكما في النافذة ادناه:



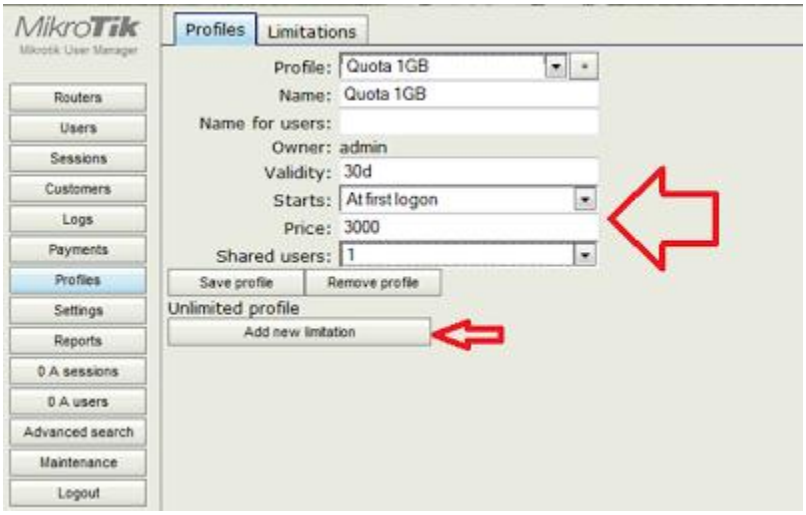
بعدها نكمل ملء الخيارات لأسم البروفايل ومدة صلاحيته ومتى يبدأ ولا ننسى ان ننقر على (Add new limitation) لأضافة قيود هذا البروفايل وهي واحدة من القيود التي انشأناها قبل قليل في المرحلة الثانية وكما في النافذة ادناه:



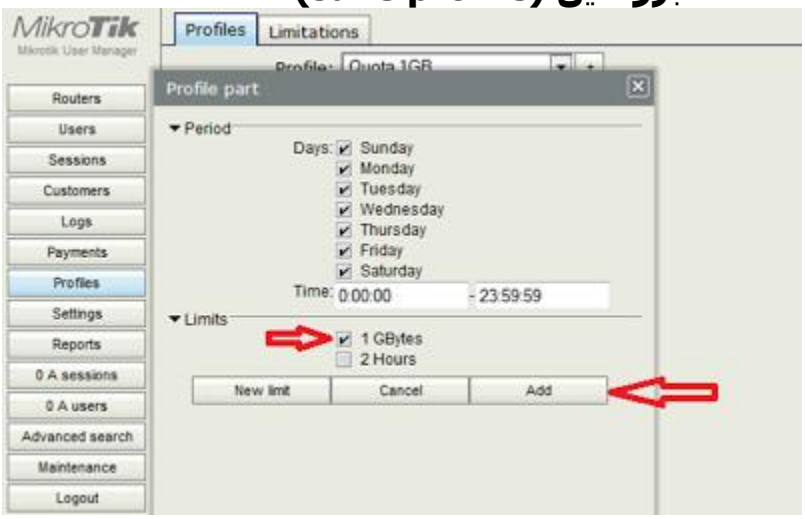
بعد النقر على اضافة قيود جديدة الى البروفايل ستظهر النافذة ادناه والتي نحدد منها في خانة ال (Limits) نوع القيود التي نريد فرضها على المستخدمين لهذا البروفايل ونلاحظ اننا في خانة الفترة (period) حددنا له ٢٤ ساعة الا صانية واحدة اي انه سيقوم بتفعيل هذه القيود ل ٢٤ ساعة ثم يعود الى البداية ليقوم بتفعيلها من جديد ل٢٤ ساعة اخرى وهكذا وبعدها ننقر على (add) ولاحظ اننا هنا نستطيع دمج عدة قيود في بروفايل واحد فنحن نستطيع تأشير علامة الصح امام كل القيود لفرضها جميعاً على هذا البروفايل وهكذا وكما في النافذة ادناه:



والان اكتملت عملية انشاء فاتورة الدفع للبروفايل ونستطيع انشاء المزيد بشروط دفع وتفعيل اخرى حسب نوع الخدمة والمستخدمين ومقدار الدفع وشروط الدفع لكل منهم فقط بأعادة نفس الخطوات ولكن بشروط مختلفة وحسب حاجة مدير الشبكة. وكما في المثال ادناه في النافذتين التاليتين:

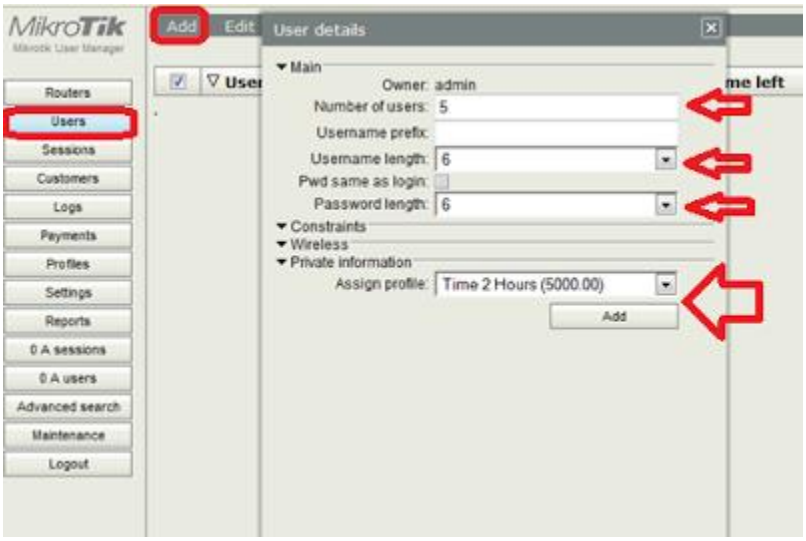


وحين تظهر النافذة الثانية نملأ الخيارات كما في ادناه: ولا ننسى النقر اخيراً على حفظ البروفايل (save profile):

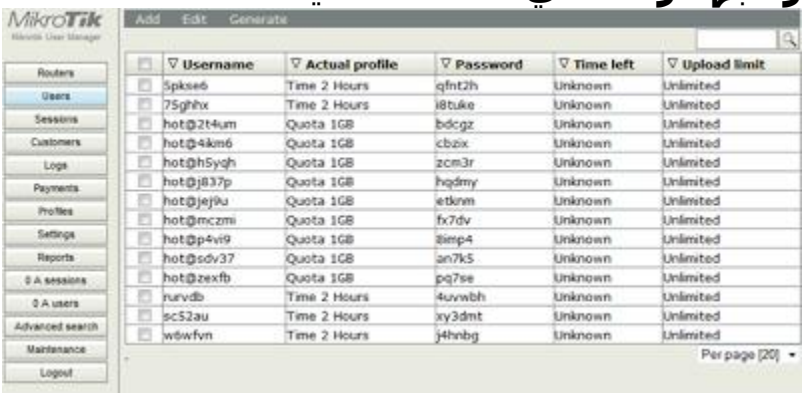


المرحلة الرابعة: انشاء المستخدمين

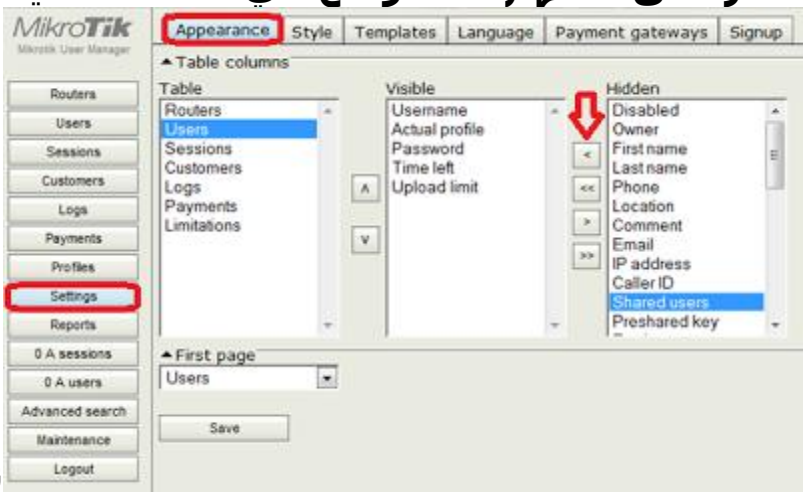
في مرحلة سابقة ذكرنا ان انشاء المستخدمين في المايكروتك هو عملية مملة وطويلة حيث يجب اضافة المستخدمين واحداً تلو الاخر بعدة نوافذ ولذا جاء مدير المستخدمين لتسهيل هذه العملية حيث يتم انشاء أي عدد من المستخدمين ويتكفل المايكروتك بأنشاء اسماء مستخدمين وكلمات مرورهم بشكل تلقائي ونقوم فقط بتحديد البروفايل الخاص بكل مجموعة من المستخدمين وكما يلي:
ننقر على تبويب (users) ثم (add) ثم حزمة (batch) ونملأ خانات عدد المستخدمين وطول اسم المستخدم وكلمة السر لكل مستخدم ونسند بروفايل لهذه المجموعة من المستخدمين وهو اي بروفايل من المجاميع التي انشأناها قبل قليل ثم ننقر على (Add) ونقوم بأنشاء عدم مجاميع من المستخدمين حسب الحاجة وكما في النافذة التالية:



والان نرى ان المايكروتك قد قام بخلق العدد المطلوب من المستخدمين وانشأ لكل منهم كلمة السر بالمواصفات المطلوبة مما يوفر على مدير الشبكة الكثير من الوقت والجهد وكما في النافذة التالية:



في حالة عدم القدة على رؤية كلمات المرور في النافذة اعلاه نقوم بالذهاب الى تبويب الاعدادات (setting) ثم المظهر (appearances) فنجد جدول بعدة اعمدة ننقر بداية على (users) في عمود الجدول (table) ثم نضبط اعدادات اعمدة جدول المستخدمين واحدها هو عمود التبويبات الظاهرة (visible) والاخر هو التبويبات الغير ظاهرة (hidden) فنقوم بنقل ال (password) من المخفي الى الظاهر بتاشيره ثم النقر على السهم كما موضح في النافذة التالية:



ثم ننقر على (save).