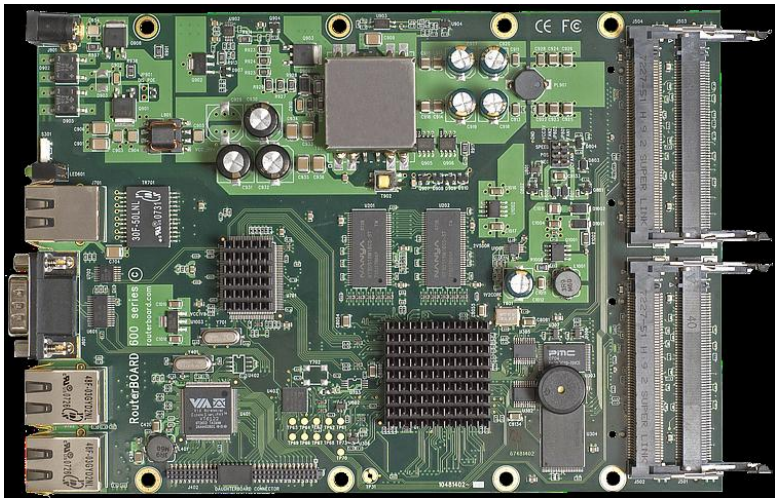
دورة اساسيات التعامل مع منتجات شركة مايكروتك ١

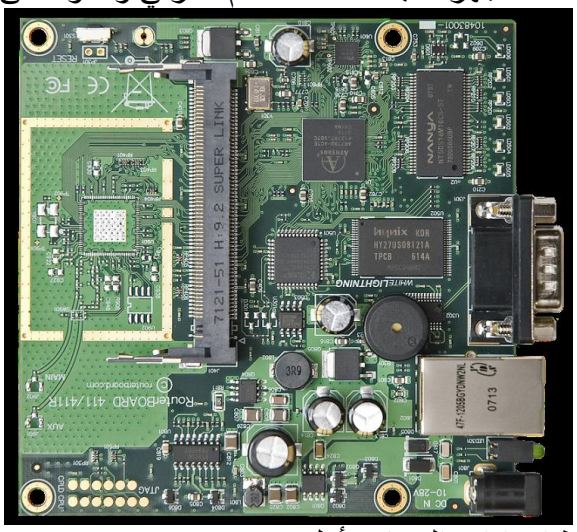
دورة ادارة الشبكات لمنتجات شركة مايكروتك (Mikrotik)

الدورة تستند الى منهج شهادة زميل الشبكات من مايكروتك (Mikrotik Certified Network Associate MTCNA) ومصادر اخرى اضافية ولا ننسى التذكير بأن الدخول في هذه الدروس يتطلب من صاحبه معرفة اولية مبسطة في اساسيات الشبكات ومكونات الحاسوب والشبكات البرمجية والهاردويرية.

الدرس الاول: كلمات لا بد منها قبل البدء تمهد الطريق نحو فهم ما نحن مقبلون عليه:

- مايكروتك هي شركة تصنيع هاردوير وسوفتوير متخصصة في مجال حلول الشبكات الصغيرة والمتوسطة الحجم.
- تعمل الشركة على تزويد المؤسسات ومزودي خدمة الانترنت (ISP) والافراد بمنتجاتها التي تهدف الى تقديم حلول انترنت اسرع واكفأ وارخص ولحيز اكبر من المستخدمين.
- اسست الشركة عام ١٩٩٥ وانتجت اول سوفتوير يعمل على تحويل جهاز الحاسوب الى موجه (router) عام ١٩٩٧ وانتجت اول لوحة هاردوير تعمل كموجه (Router Board) عام ٢٠٠٢ وتم عقد اول مؤتمر لمستخدمي المايكروتك عام ٢٠٠٦ (Mikrotik User Meeting MUM) وهو مؤتمر سنوي يلتقي فيه مستخدمي المايكروتك ويتبادلون الخبرات واساليب العمل والمجالات الجديدة للعمل ويلتقون بالخبراء والمختصين في تطوير معدات وبرمجيات النظام.
- نظام تشغيل المايكروتك المسمى (RouterOS) هو نظام تشغيل يجعل الجهاز الذي ينصب فيه يعمل كموجه مخصص ومحدد عرض نطاق ومرشح مرور شفاف (Transparent packet filter) وجهاز ذو قابلية اتصال لاسلكي بأي جهاز يعمل ضمن المقياس الدولي العالمي للشبكات اللاسلكية (IEEE 802.11a,b,g) ويمتاز هذا النظام انه يمكن ان يكون نظام تشغيل ال (RouterBoard) او ينصب على جهاز حاسوب مكتبي ليحوله الى ما تم وصفه سابقاً من موجه ومرشح ومحدد وغيرها.
- اجهزة شركة مايكروتك المسماة (RouterBoard) هي المعدات التي تصنعها شركة مايكروتك لتتراوح في عملها كأجهزة شبكات للأستخدام لمنزلي وصولاً الى ادارة الشبكات الكبيرة كما في الصور ادناه.



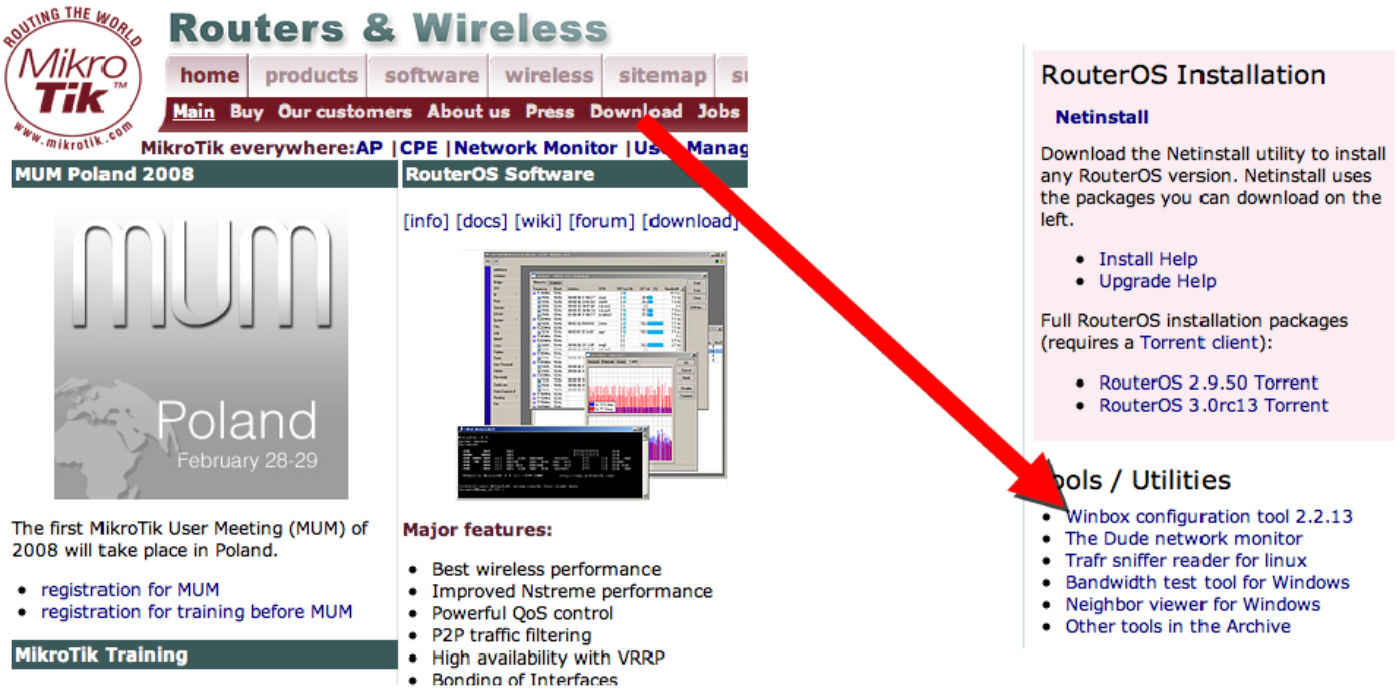


ضبط اعدادات الجهاز لأول مرة:

لضبط اعدادات الاجهزة المصنعة من شركة مايكروتك فأول خطوة نقوم بها بعد تنصيب السوفتوير في الحاسوب المكتبي او تشغيل البورد (RouterBoard) لأول مرة هي ضبط اعدادات الجهاز بإحدى الطرق التالية:

- واجهة سطر الاوامر (CLI) والتي يمكن الوصول اليها بواسطة البرامج الملحقة بنظام التشغيل الوندوز مثل (Telnet, SSH) وبسلط من النوع التسلسلي (serial cable) وشاشة ولوحة مفاتيح تربط الى الجهاز (البورد).
- بواسطة واجهة الويب عن طريق تطبيق يسمى (WebFig) كما سنرى لاحقاً.
- باستخدام الاداة الاكثر استخداماً والتي تسمى (WinBox) وهو برنامج صغير يتم تنزيله مجاناً من موقع الشركة (www.mikrotik.com) وكما في الصورة التالية:

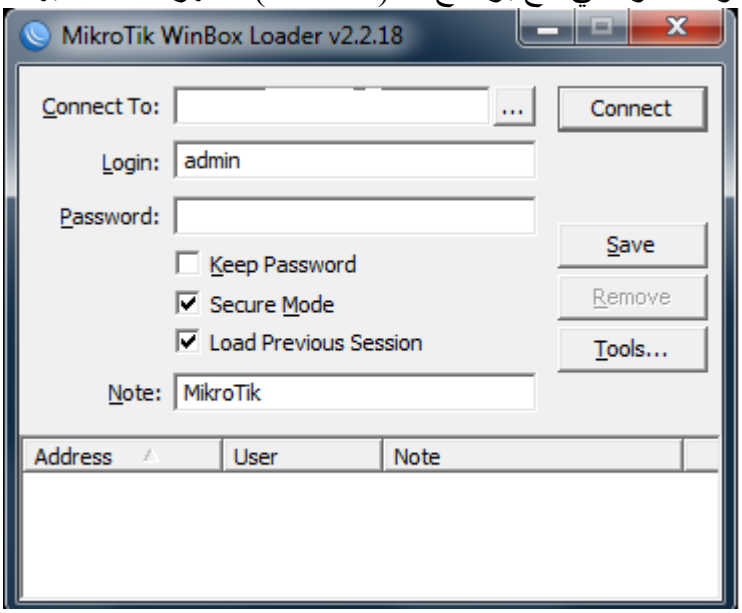
دورة اساسيات التعامل مع منتجات شركة مايكروتك ٢



ملاحظة مهمة: مما تجدر الاشارة اليه ان كل موجهات الشركة تكون بعنوان (IP) تلقائي يساوي (192.168.88.1/24) للمنفذ (ether1) وباسم مستخدم تلقائي (admin) وكلمة مرور فارغة. اما بقية الاعدادات فتعتمد على خصوصيات كل منتج ونوعه وتطبيقاته.

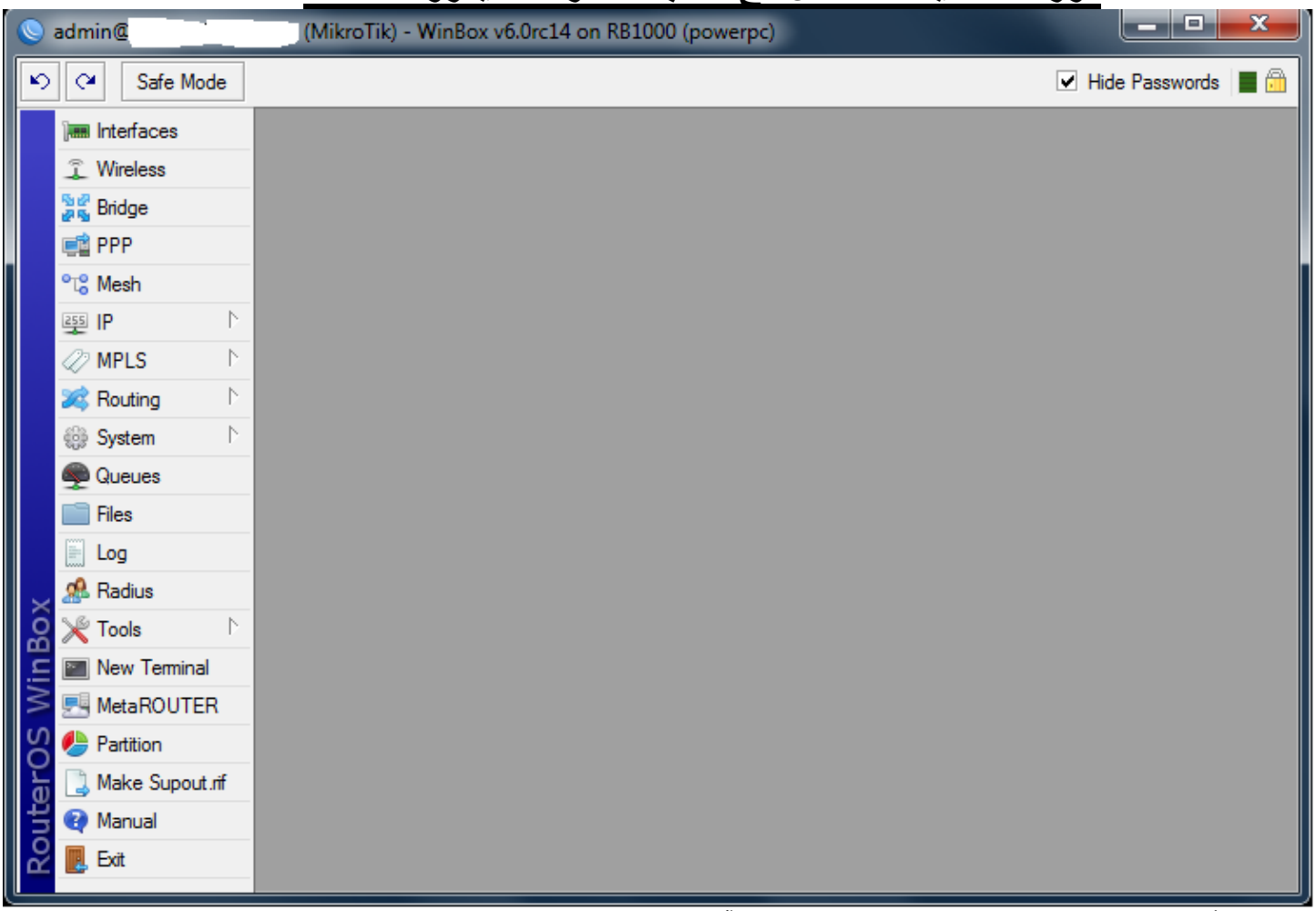
ضبط اعدادات الراوتر بأستخدام ال(WinBox)

اول خطوة هي فتح برنامج ال (winbox) لتظهر نافذة مشابهة للنافذة التالية:

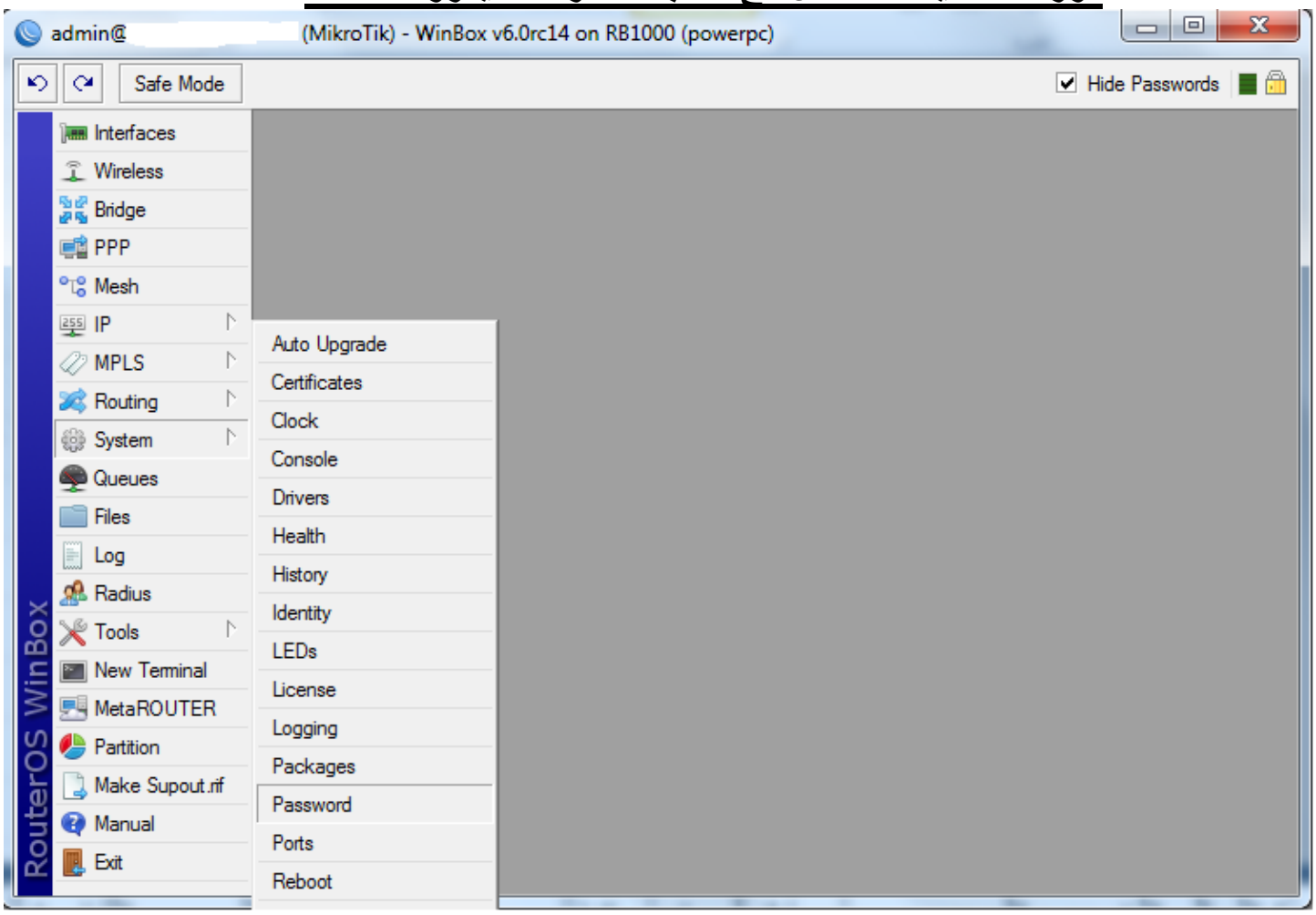


نقوم بالنقر على زر (...) لتظهر نافذة تحتوي اسماء وعناوين الراوترات المتصلة بحاسبتنا ونختار منها الراوتر المراد ضبط اعداداته بالنقر على (MAC Address) الخاص به وبعدها نقوم بأدخال اسم المستخدم والذي يكون (admin) لأول استخدام تلقائياً وكلمة المرور التي تكون فارغة لأول استخدام وننقر على (Connect) لتظهر لنا النافذة التالية:

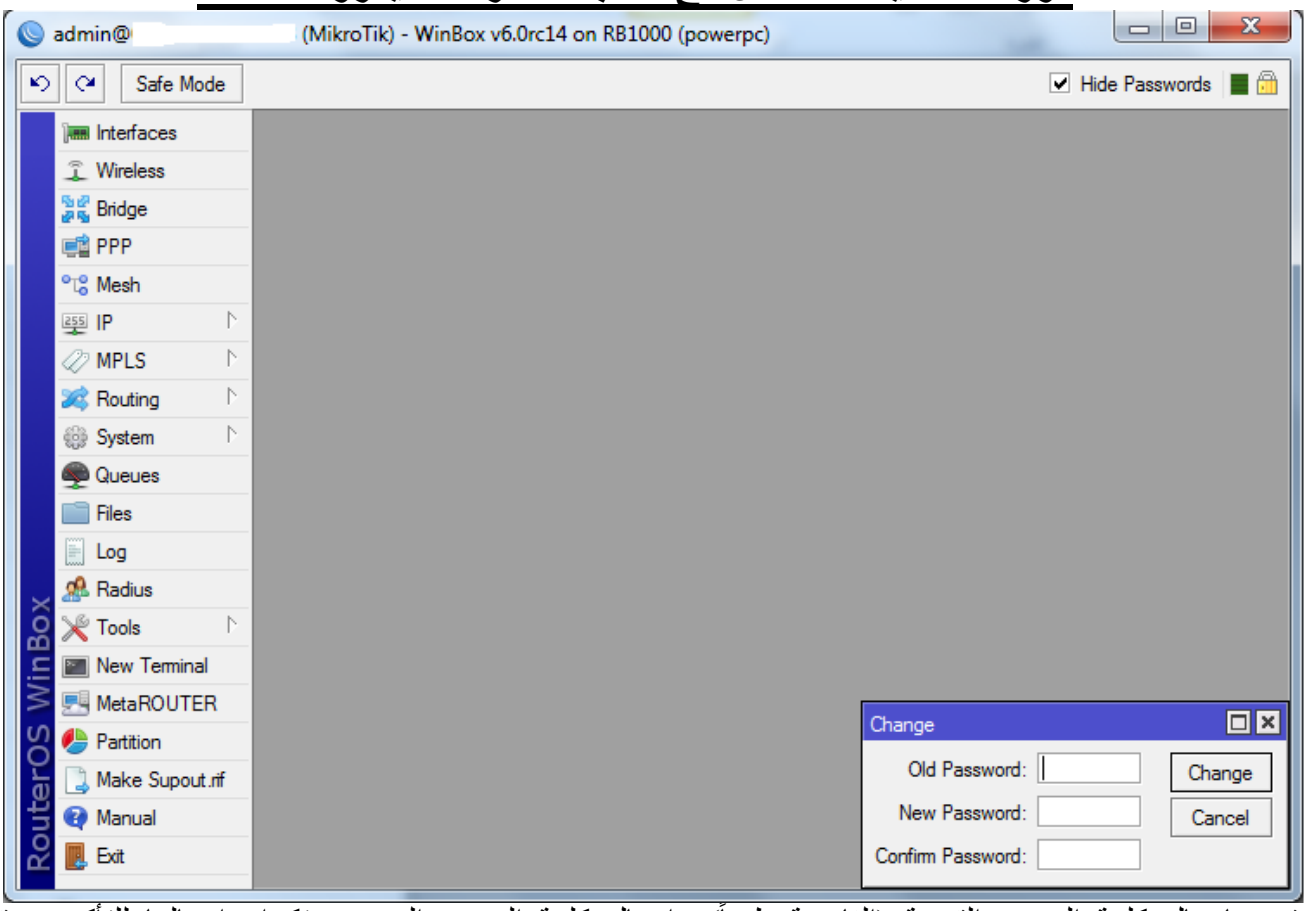
دورة اساسيات التعامل مع منتجات شركة مايكروتك ٣



والان نبدأ التجوال في هذا العالم الغريب العجيب وطبعاً اول خطوة نقوم بها تبديل كلمة المرور الفارغة الى كلمة اخرى اكثر امناً لمنع اي مستخدم اخر متصل بالشبكة من الدخول الى الراوتر بسهولة وتغيير اعداداته ونقوم بذلك بالذهاب الى تبويب (system) من القائمة الى اليسار ومنه نختار تبويب (password) كما في النافذة التالية:

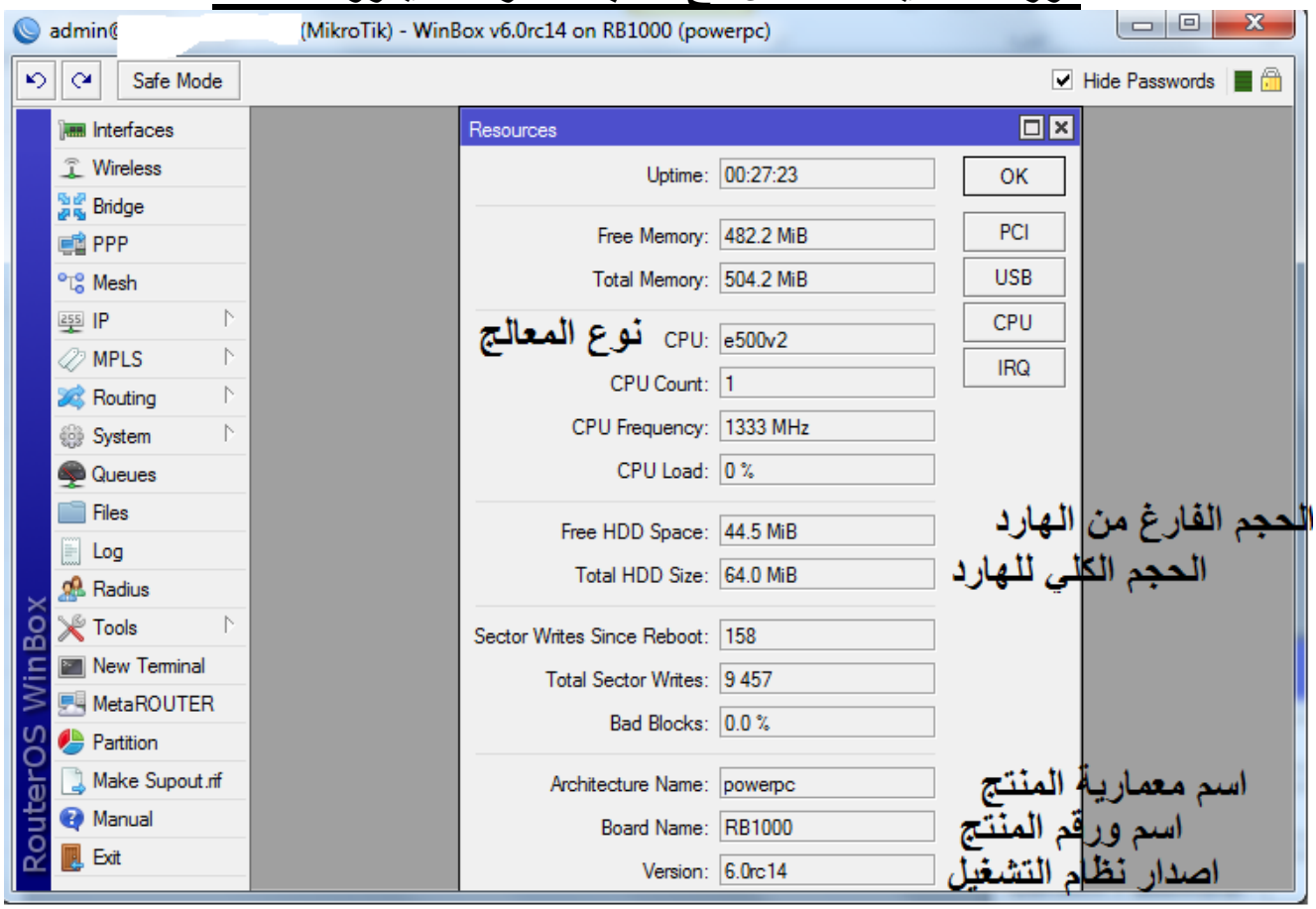


بعد النقر على زر (password) تظهر لدينا النافذة التالية:



نقوم بإدخال كلمة المرور القديمة (الفارغة طبعاً) وادخال كلمة المرور الجديدة وتكرار ادخالها للتأكيد وننقر على (change).

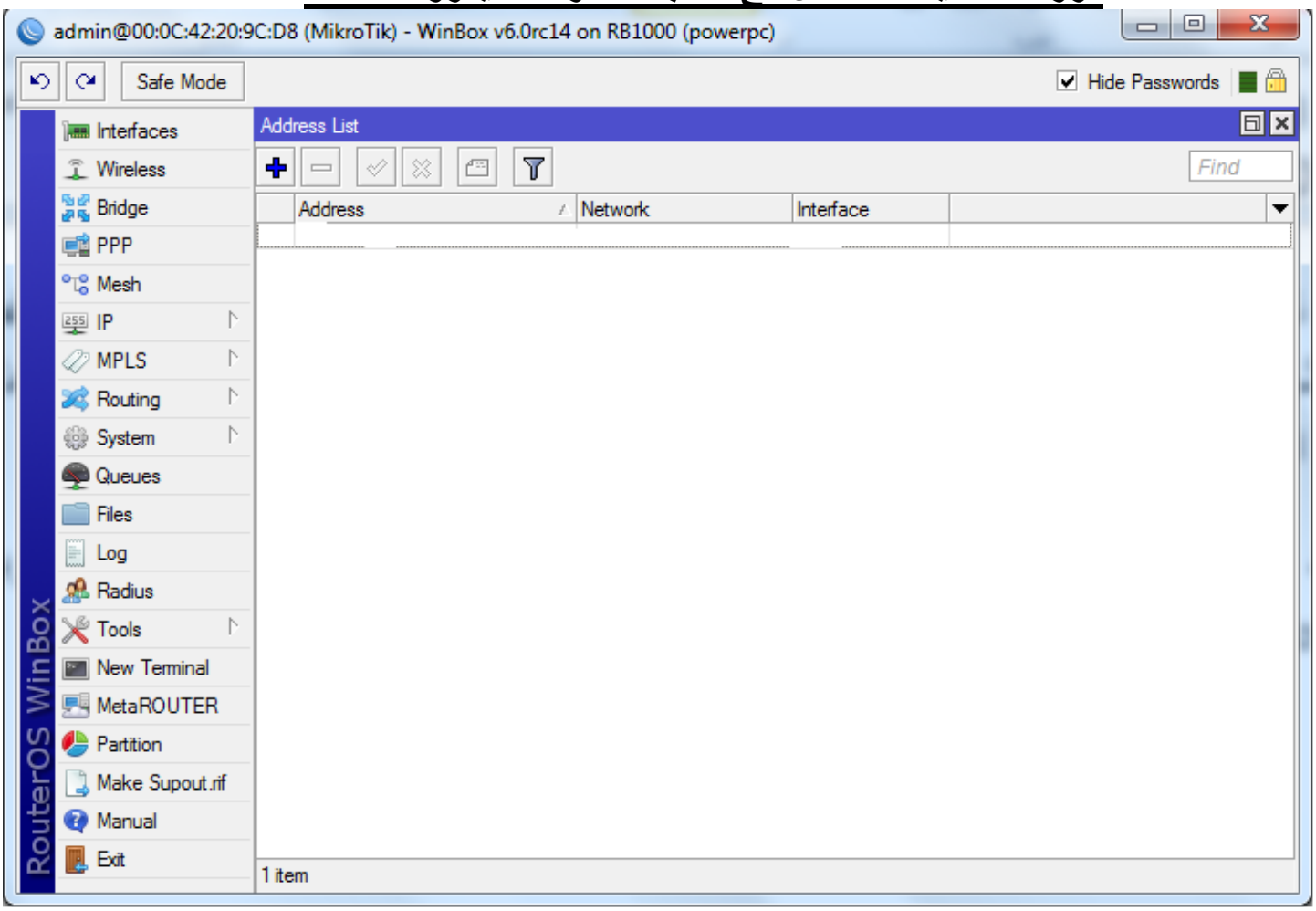
الخطوة المقبلة برأيي هي معرفة نوع واصدار الهاردوير والسوفتوير الخاص بجهازنا الجديد (طبعاً اذا لم نكن نعرفه مسبقاً) ويتم ذلك بالذهاب الى (System) ومنها الى (Resources) لتظهر لنا النافذة التالية:



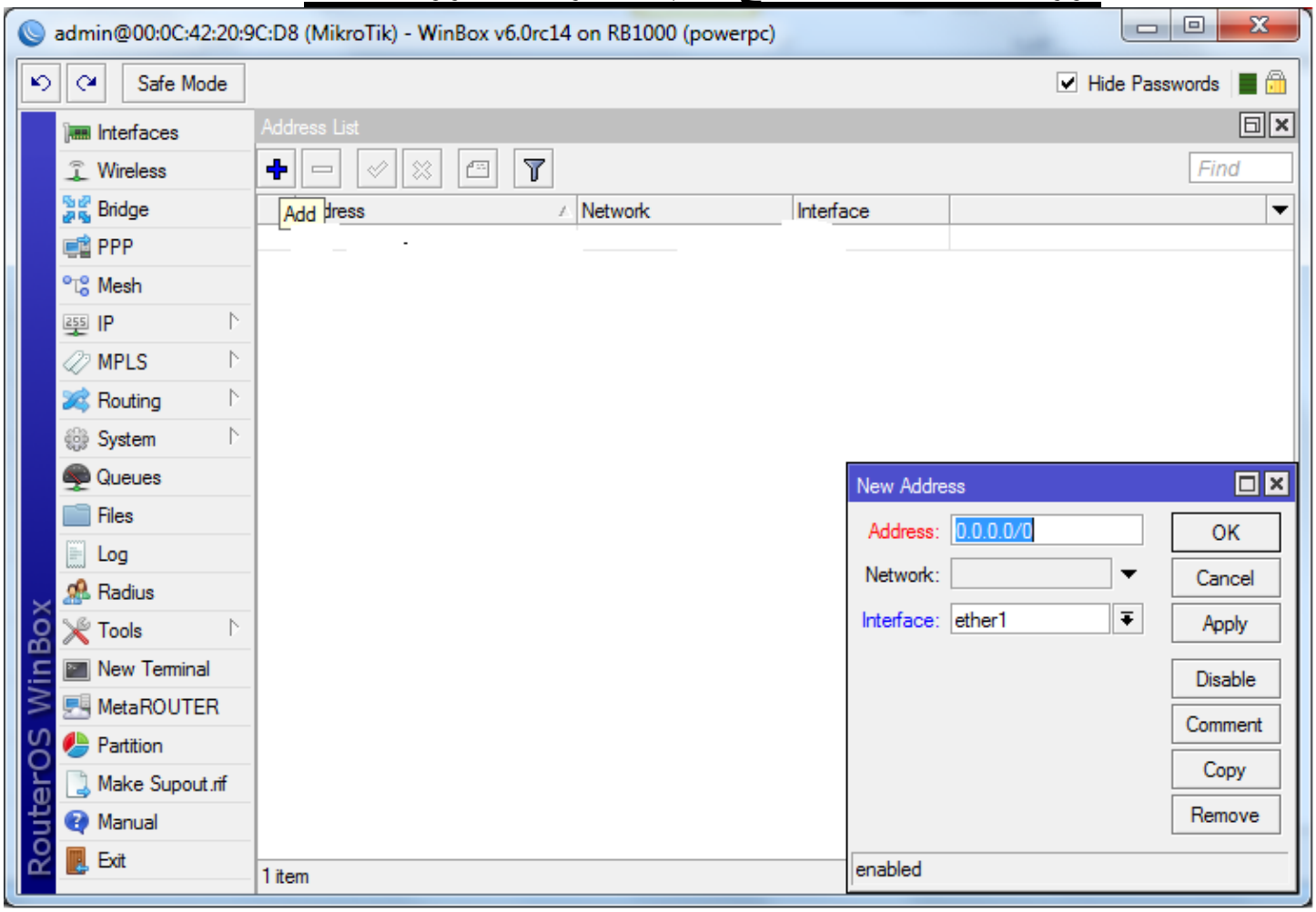
ومن خلال النافذة اعلاه نستطيع معرفة معلومات عامة عن المنتج وبعدها نستطيع بسهولة البحث عن خصائصه ومواد تعليمية عنه في موقع الشركة (www.mikrotik.com) او موقع (wiki.mikrotik.com) او غيرها من المواقع الكثيرة للتعليم حول هذا النظام ومنتجاته المختلفة.

الخطوة الثالثة هي اسناد عناوين لكل منفذ او واجهة (interfaces or ports) من واجهات الجهاز الاربعة والمسماة (ether1, ether2, ether3, ether4) وكما يلي:

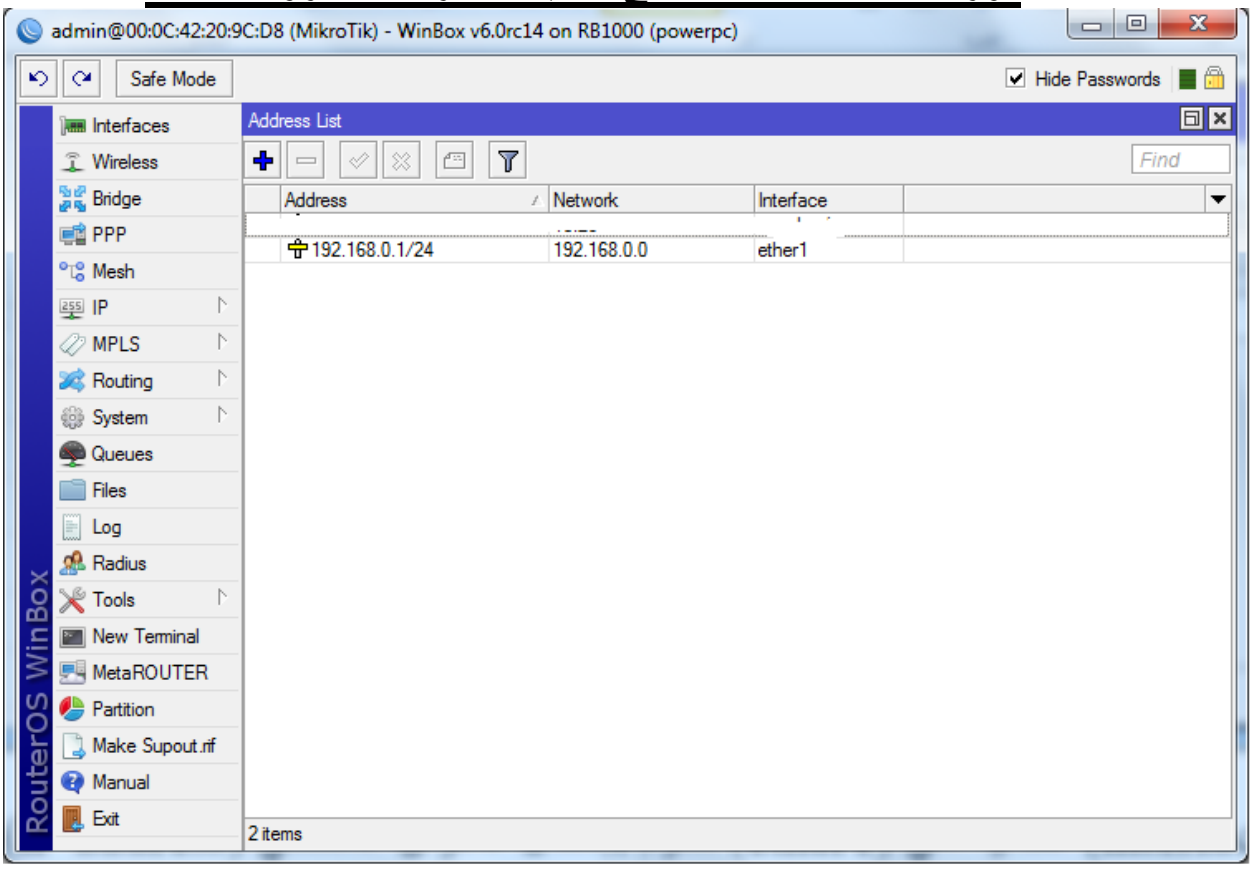
نفتح تبويب (IP) ومنه نختار (Addresses) لتظهر لنا النافذة التالية:



ومن هنا نستطيع اسناد عناوين المنافذ الخاصة بالجهاز سلكية ولاسلكية لتقسيم الجهاز الى شبكات متعددة من نوع (LAN and WAN) ويتم ذلك بالنقر على اشارة (+) لتظهر النافذة التالية:

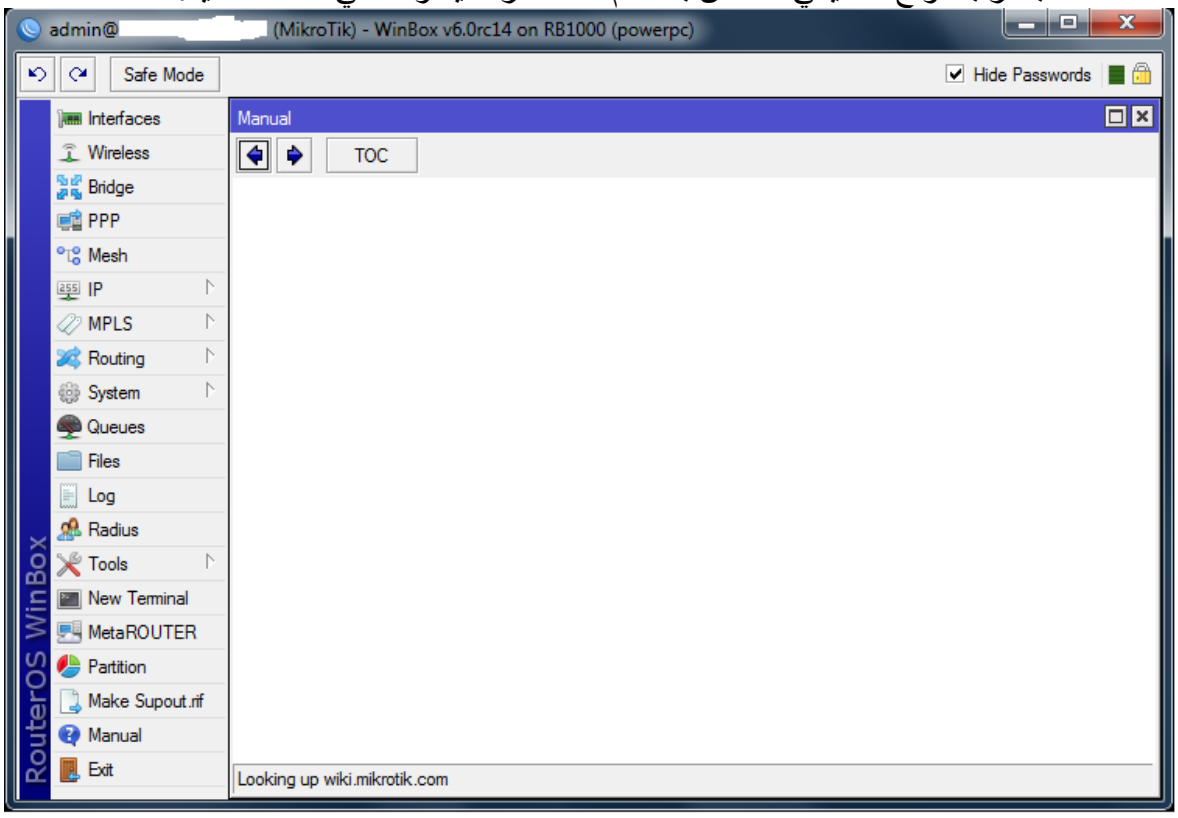


ونلاحظ ان الواجهة (interface) الحالية هي (ether1) فنقوم بإدخال العنوان المنطقي (IP address) الخاص بها وحسب الحاجة وليكن (192.168.0.1/24) ونلاحظ اننا كتبنا العنوان وقناع الشبكة الفرعية الخاص به (subnet mask) ليدل على انه ضمن الصنف الثالث (class c) ثم ننقر على (ok) لتظهر النتيجة التالية:



نكرر نفس العملية مع بقية الواجهات ولا اشكال في اسناد اي عنوان ضمن اي صنف لهذه الواجهات التي يمكن ان تجمع في شبكة واحدة او عدة شبكات منفصلة كما سنرى لاحقاً.

لا يفوتني ان اشير الى ان نظام المايكروتك يوفر دعماً دائماً للمستخدمين من خلال توفير تبويب (manual) الذي يتيح الاتصال المباشر بالموقع التعليمي الخاص بالنظام عند النقر عليه وكما في النافذة التالية:



دورة اساسيات التعامل مع منتجات شركة مايكروتك ١٠

الدرس الثاني من دورة اعداد المايكروتك

بعد ان تعرفنا في الدرس السابق على:

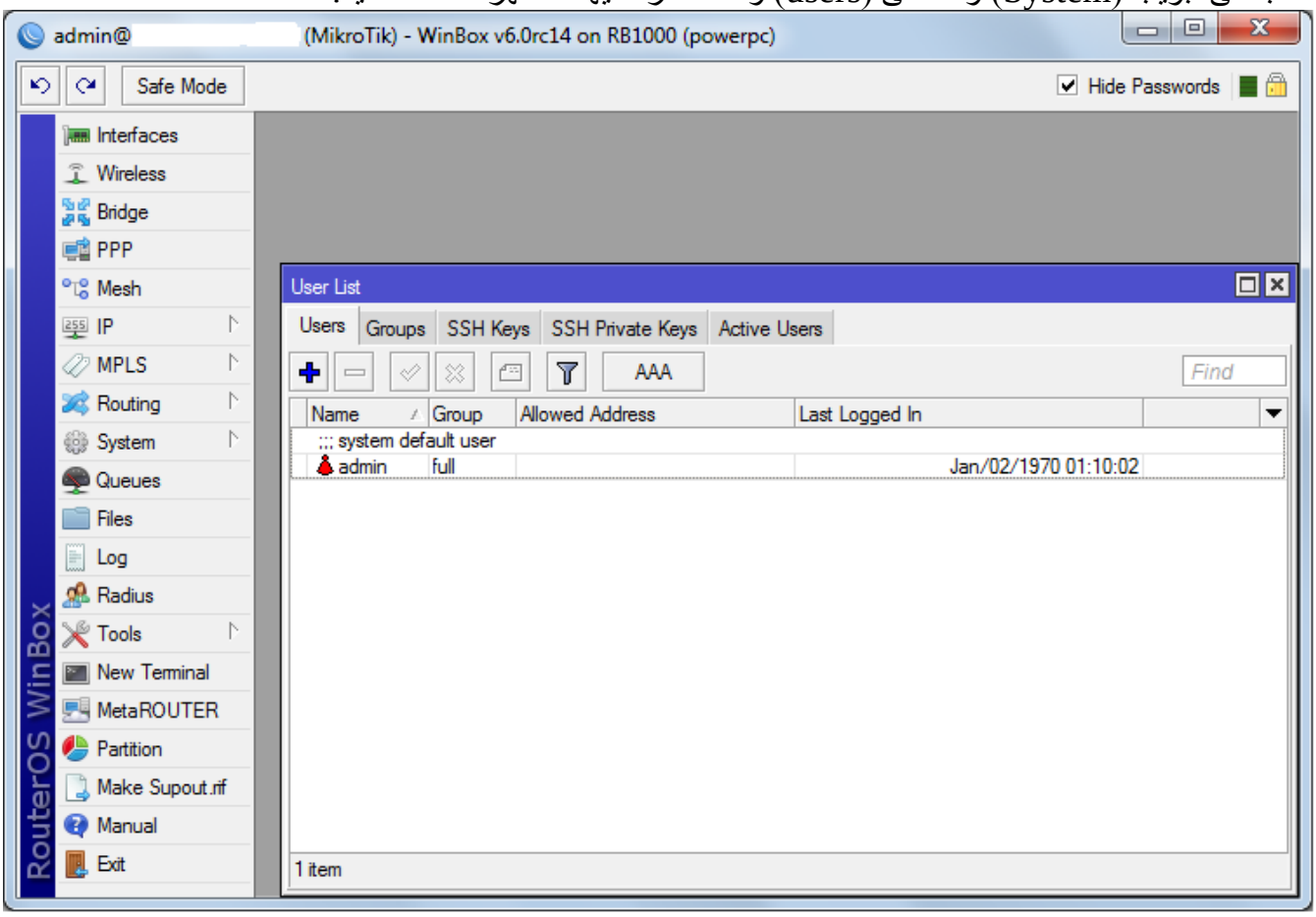
١- كيفية تغيير كلمة مرور ال (admin).
٢- تسمية واسناد عناوين الى منافذ الجهاز.
٣- كيفية الوصول الى صفحة التعليم والمساعدة الخاصة بالنظام (manual).

نستمر معاً اليوم ان شاء الله في شرح اساسيات التعامل مع واجهة برنامج ال (winbox) والتعرف على خصائص منتجات شركة مايكروتك وامكانياتها العجيبة وكالاتي:

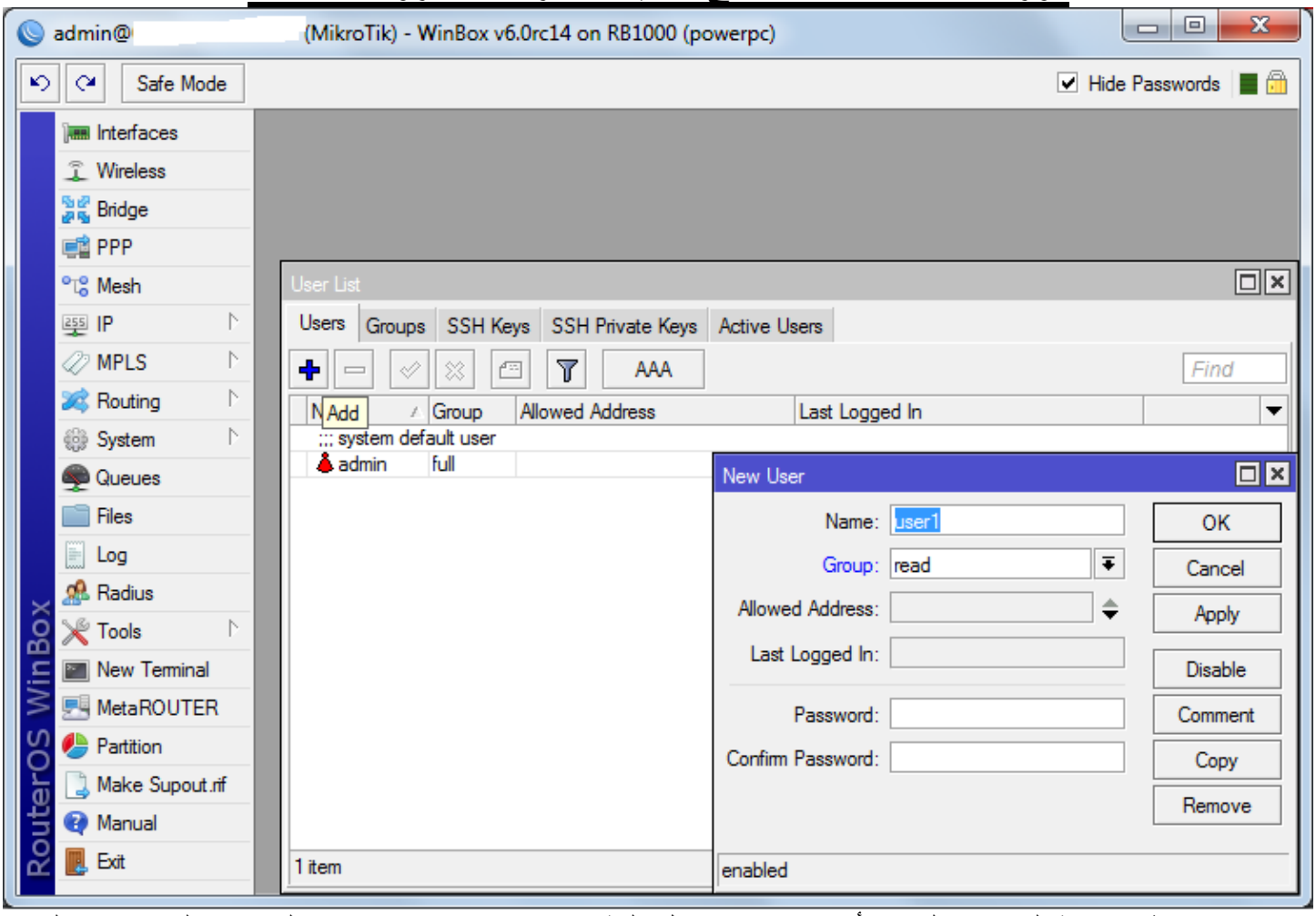
١- انشاء مستخدم جديد واسناد صلاحيات وكلمة مرور له.
٢- منح اسم خاص للجهاز (identity).
٣- ضبط طور عمل النظام على الطور الامن (safe mode).
٤- ضبط ساعة النظام وبروتوكول وقت الشبكة (NTP).
٥- حفظ نسخة احتياطية من ملف الاعدادات واسترجاعها.

١- بعد الدخول الى الجهاز لأول مرة سيطلب منا عدة خيارات ومنها انه يحتوي اعدادات تلقائية من المصنع ويسأل هل نحتاج الى حفظها او حذفها وهنا يأتي الخيار لنا في امكانية الاستفادة من الضبط الافتراضي في حالة كون المستخدم مبتدئ او حذفه والبدء من الصفر للمتقدمين من مدراء الشبكات وبعد ان نوافق على حفظ الضبط الافتراضي نتجه الى انشاء مستخدم جديد بدل ال (admin) او اضافة له حتى نزيد من امنية الجهاز وصعوبة اختراقه من قبل اي شخص اخر ونحدد صلاحيات هذا المستخدم الجديد وكما يلي:

نذهب الى تبويب (System) ومنه الى (users) وعند النقر عليها ستظهر النافذة التالية:



ونلاحظ وجود مستخدم واحد اسمه (Admin) ولديه صلاحيات كاملة (full) والان لإضافة مستخدم جديد ننقر على اشارة (+) لتظهر النافذة التالية:



ونرى اننا نستطيع تسمية المستخدم الجديد بأي اسم بوضعه بدل كلمة (user1) ونحدد صلاحيات المستخدم الجديد وكما يلي:

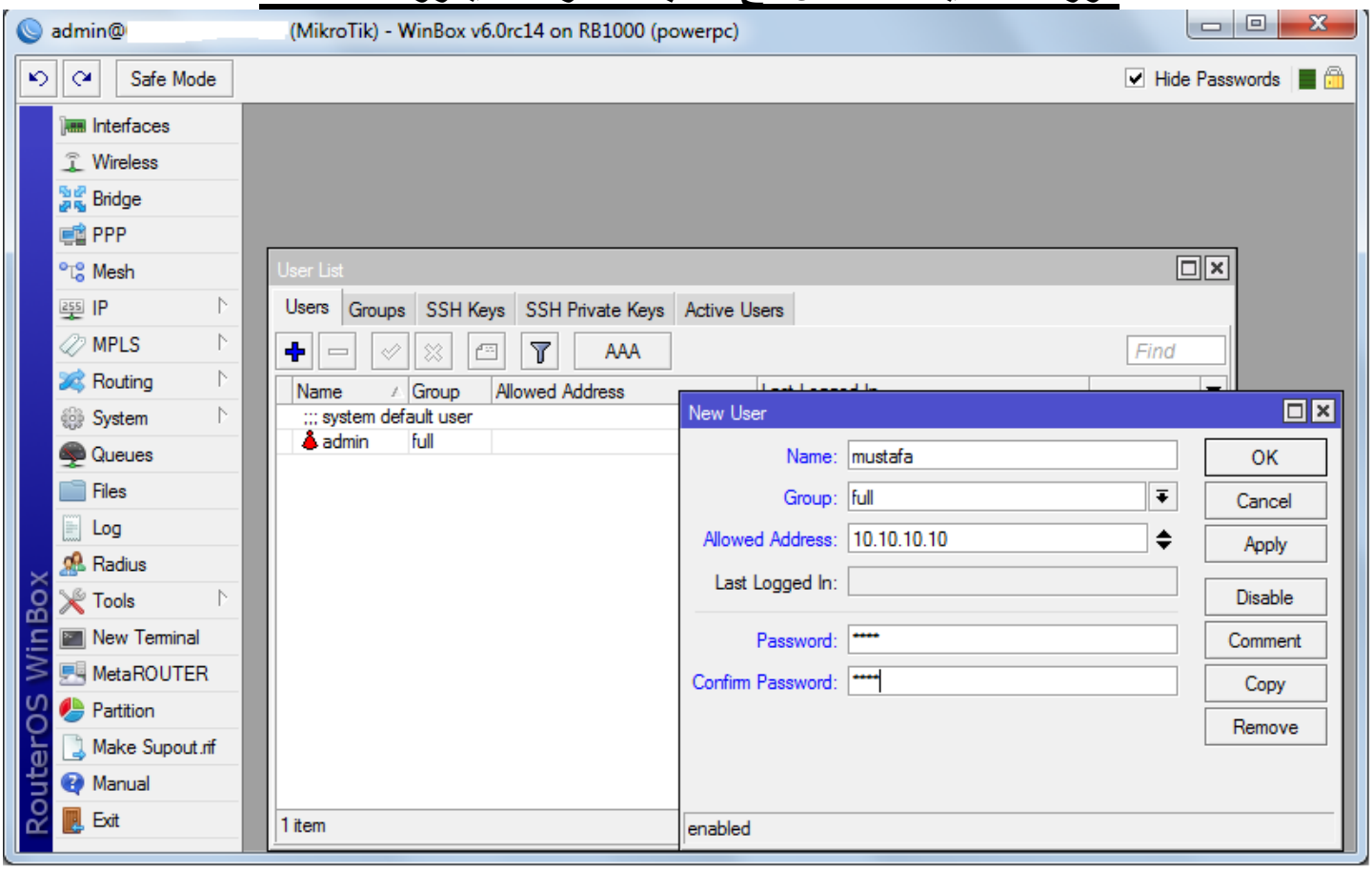
١- (read): يعني امكانية القراءة فقط وتمنح للمستخدم المراد جعله مراقب فقط (for monitoring only).

٢- (write): يعني ان المستخدم صاحب هذه الصلاحية يمتلك امكانية القراءة والكتابة (الاضافة) ولكنه لا يمتلك قابلية التعديل على ما هو موجود اصلاً.

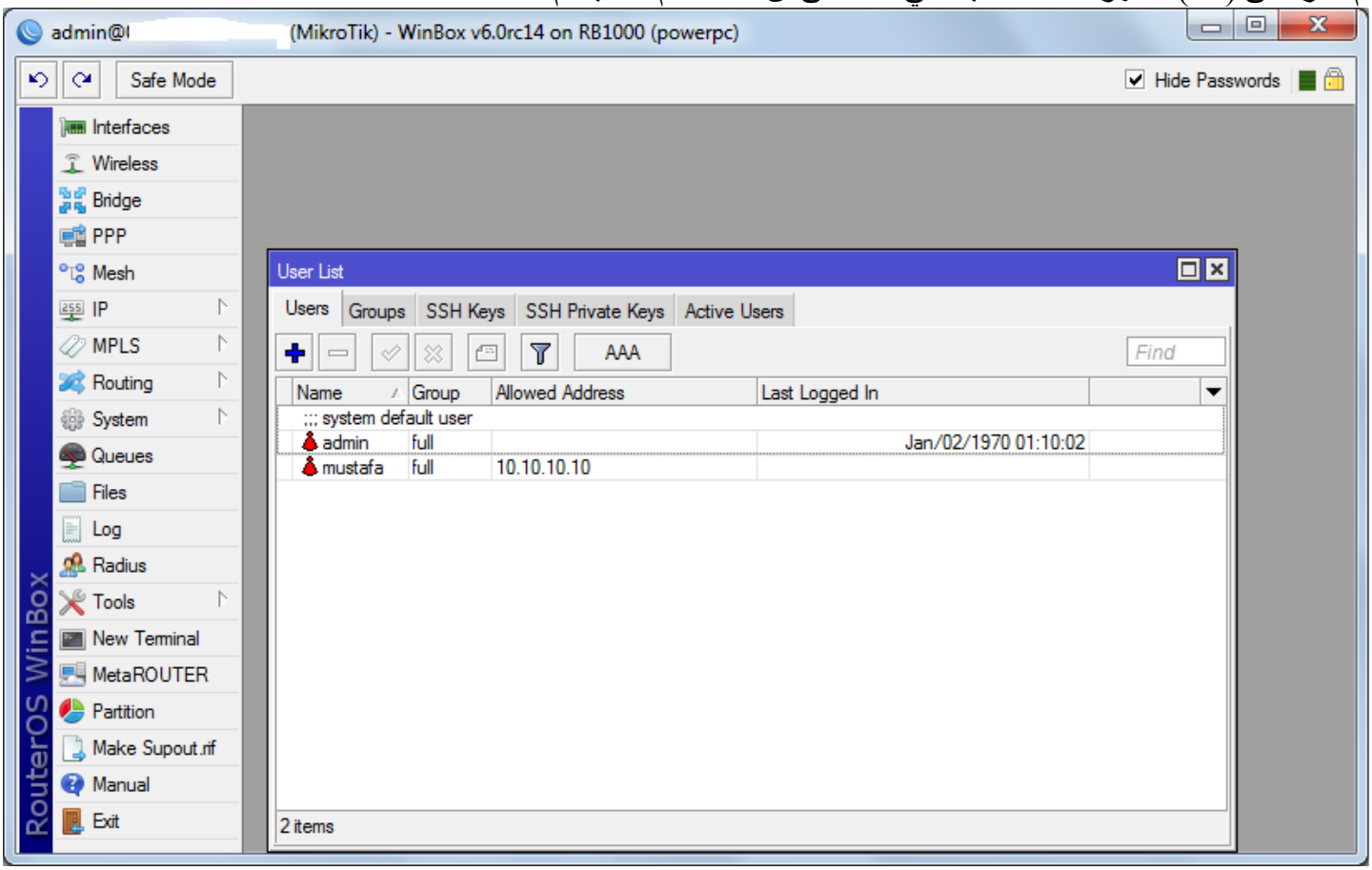
٣- (full): وصاحب هذه الصلاحيات يمتلك القدرة على فعل اي شيء من قراءة وكتابة وتعديل وتحديث اي انه يمتلك نفس صلاحيات المستخدم (Admin).

ملاحظة: يمكن اضافة مجاميع اخرى غير الثلاثة المذكورة سابقاً من الذهاب الى تبويب (groups) واختيار اشارة (+) وانشاء مجموعة جديدة بصلاحيات نحددها نحن وحسب الحاجة.

بعد ان نسند الاسم ونحدد الصلاحيات نتجه الى تحديد قيد اخر وهو العنوان المنطقي المسموح لهذا المستخدم باستخدامه وهو ما يسمى (Allowed address) ونحدده ثم نتجه اخيراً الى كتابة كلمة المرور وتأكيدها لتكون النافذة كما يلي:



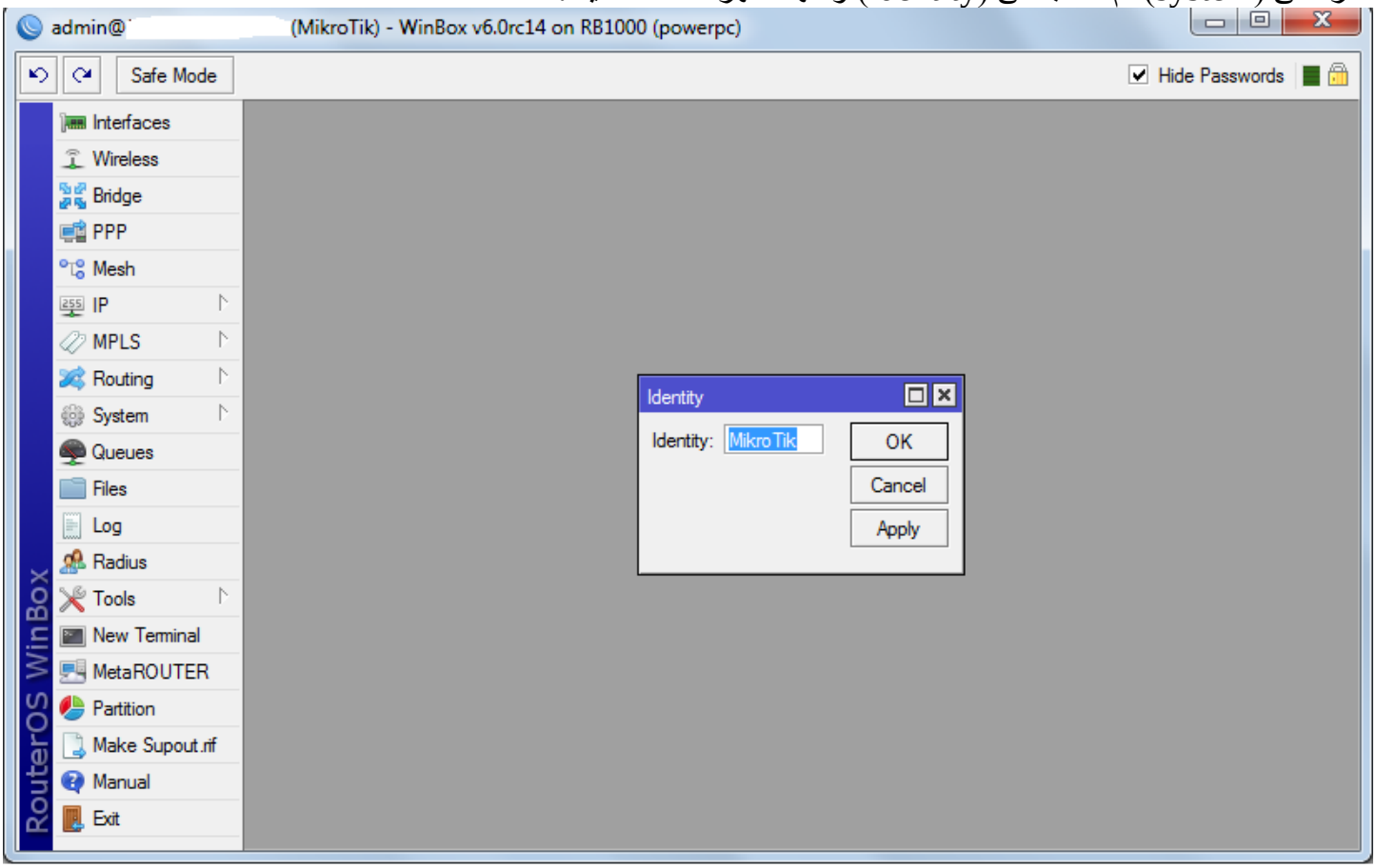
ثم ننقر على (ok) لتظهر النافذة التالية التي تدل على ان المستخدم الجديد تم اضافته:



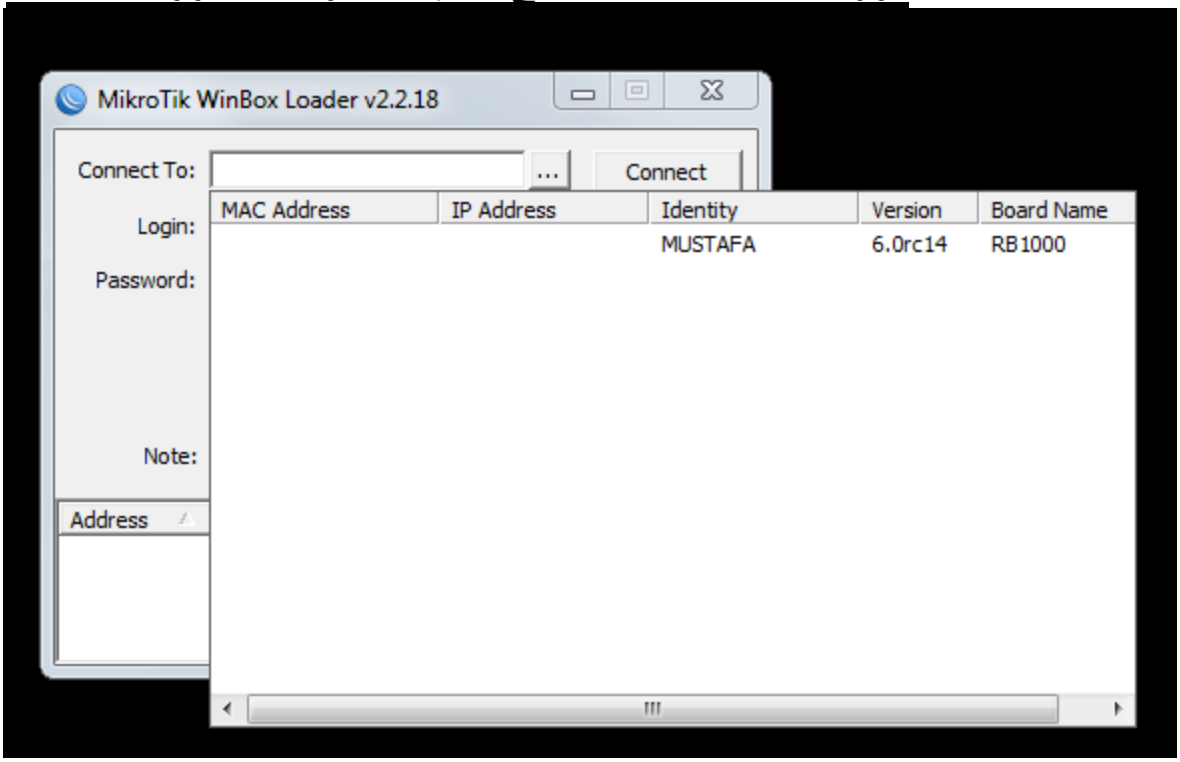
والان يفضل بعض مدراء الشبكات حذف المستخدم القديم (Admin) والاقتصار على المستخدمين الجدد الذين يتم اضافتهم وحسب حاجة النظام وعدد المسؤولين عن النظام كمراقبة وادارة وغيرها.

٢- الان نتجه الى اعطاء اسم الى الجهاز الخاص بنا والذي نعمل عليه لتمييزه عن بقية الاجهزة في الشبكة وهو الاسم الذي يظهر حين البحث عن الراوترات بعد فتح ال (winbox) والنقر على (...) وكما يلي:

ننقر على (system) ثم نذهب الى (identity) ومنها تظهر النافذة التالية :

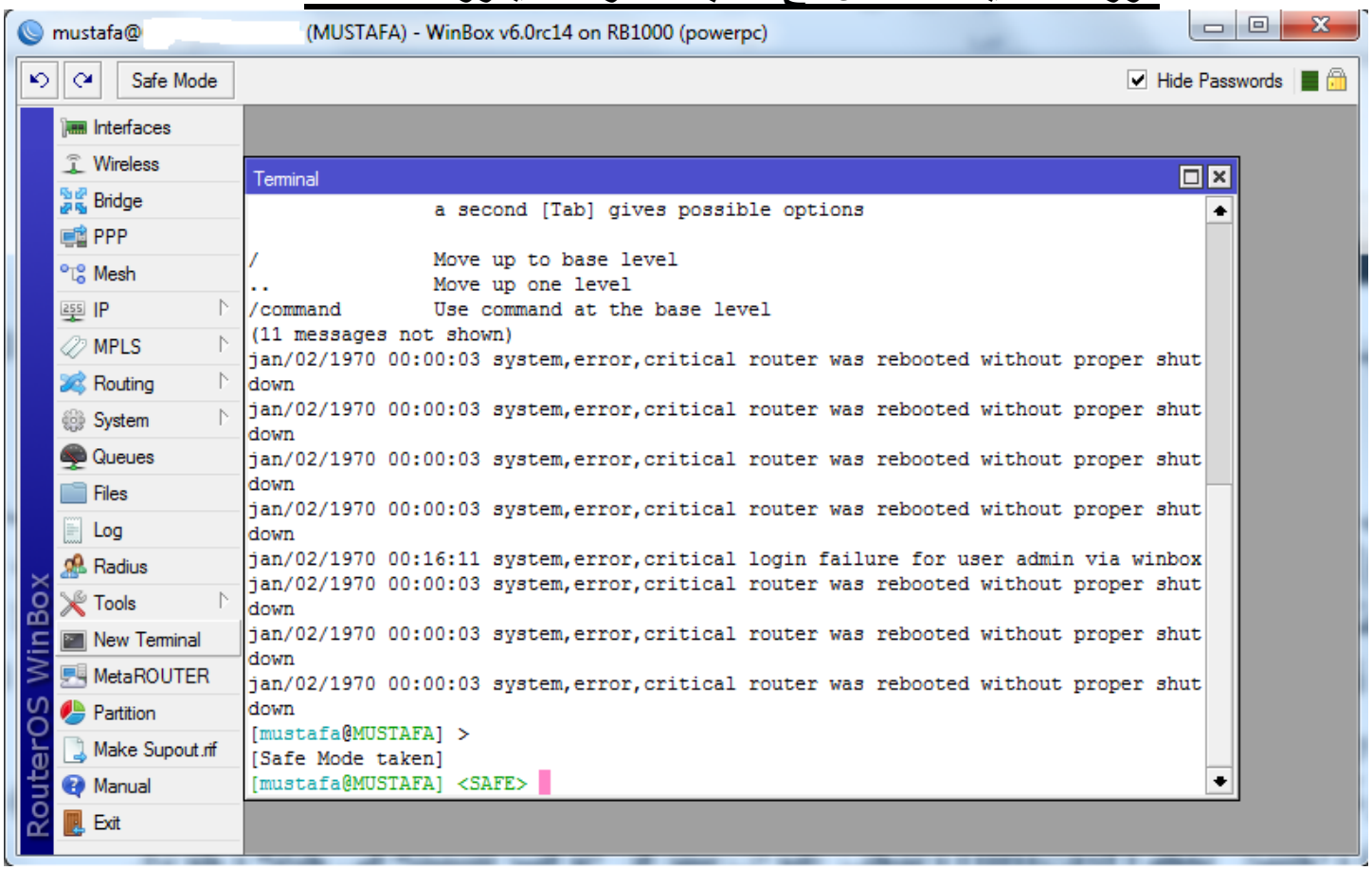


ونغيره وليكن (MUSTAFA) ننقر بعدها على (ok) والان نخرج من البرنامج ونعيد الدخول ونرى ما يحصل:

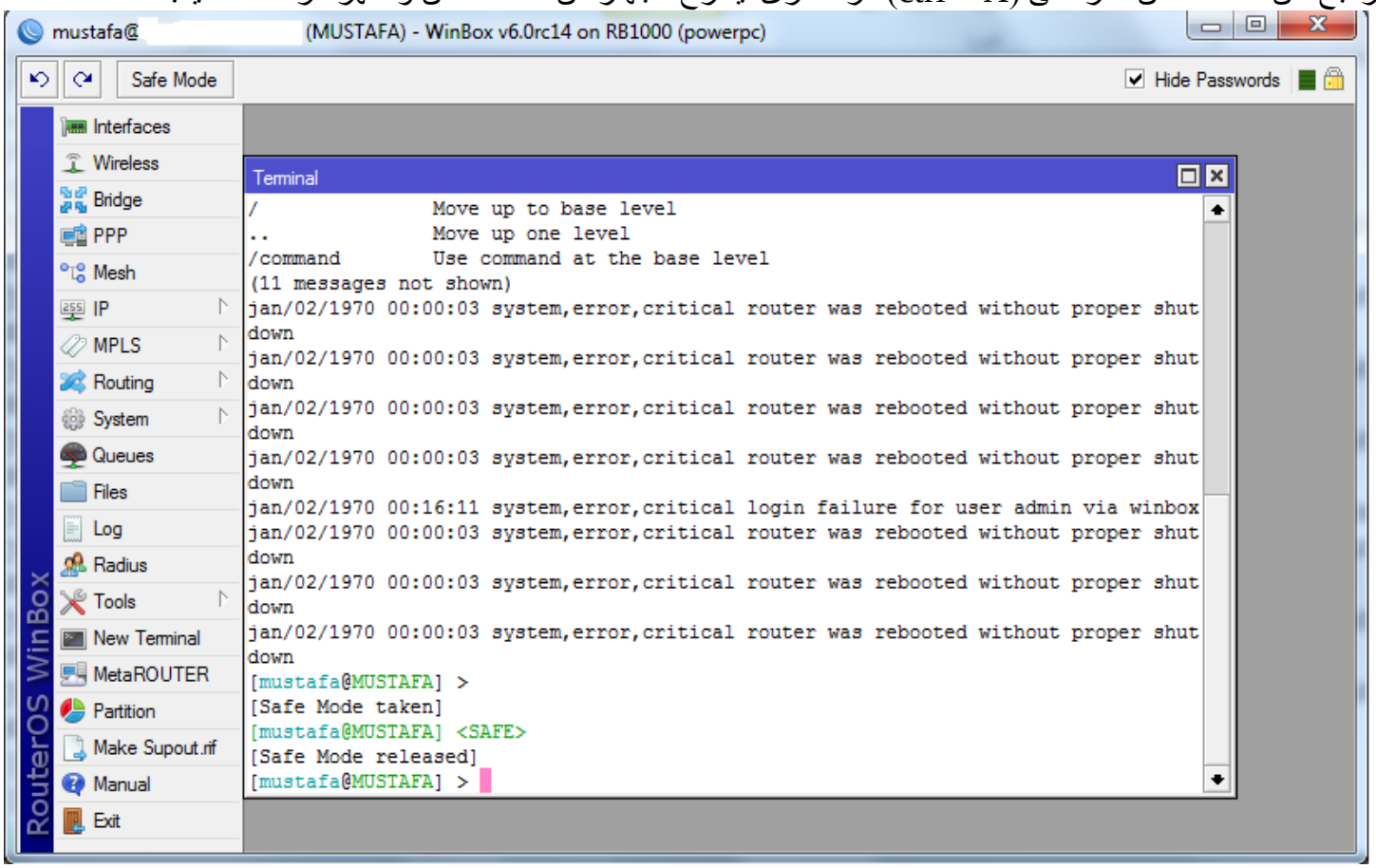


نرى ان الاسم الجديد ظهر لدينا (Mustafa) وبعدها نختار المستخدم المراد الدخول باسمه ونكتب كلمة المرور الخاصة به وندخل.

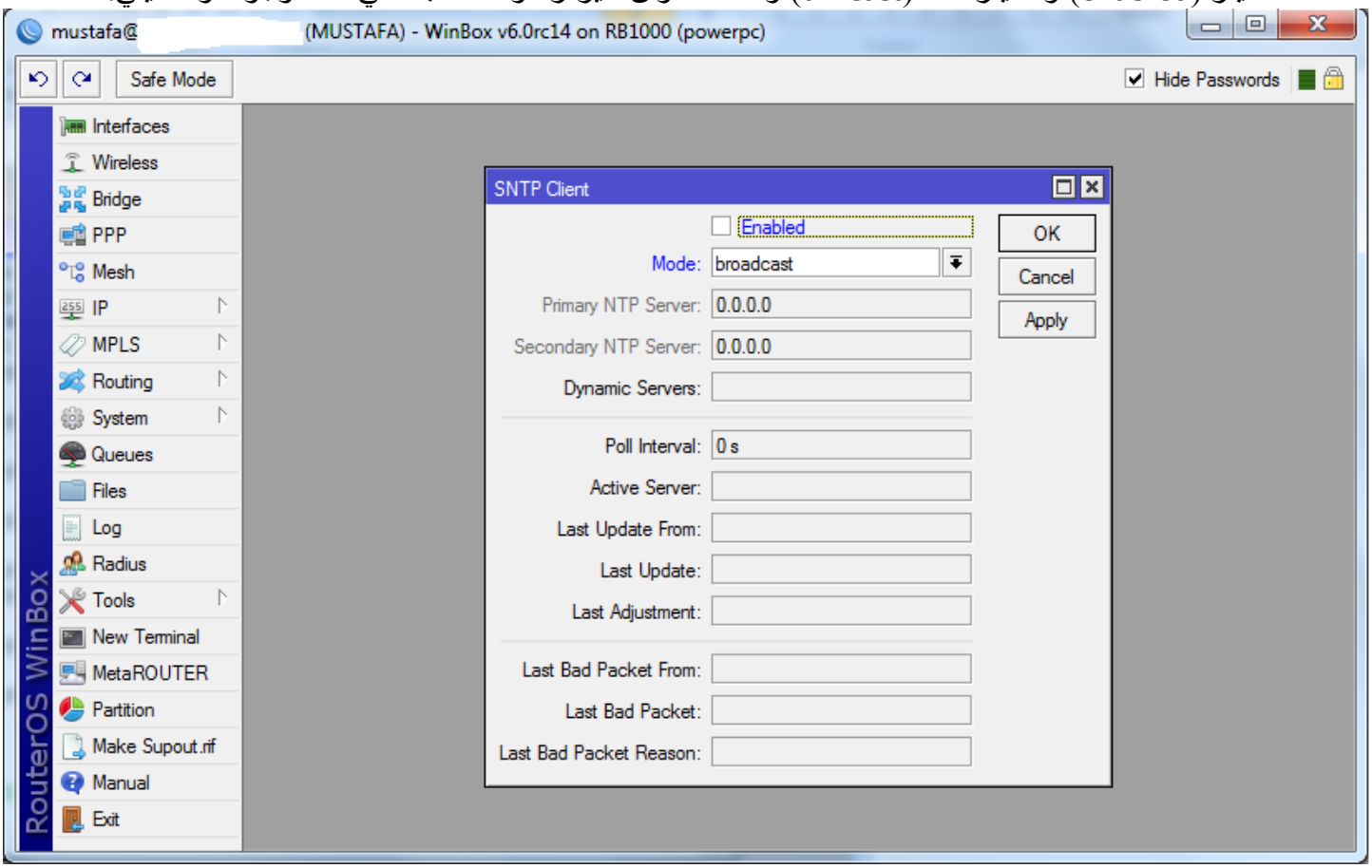
٣- قبل البدء في تعديل اعدادات الجهاز يجب ضبط الجهاز على الطور الامن (safe mode) بالدخول الى سطر الاوامر من تبويب (new terminal) ثم النقر على (ctrl + X) وبعدها نستطيع التعديل على الاعدادات مع الاطمئنان انها لن تخزن حتى نقرر ذلك بحيث انه لو انقطعت الكهرباء عن الجهاز قبل انهاء الاعدادات وخزنها فستعود الاعدادات الى اللحظة قبل ادخال الجهاز الى الطور الامن وبذلك فهي سلاح ذو حدين قد يفيد في الرجوع الى نقطة امنة وقد يضيع تعب واعدادات تستمر ساعات احياناً.



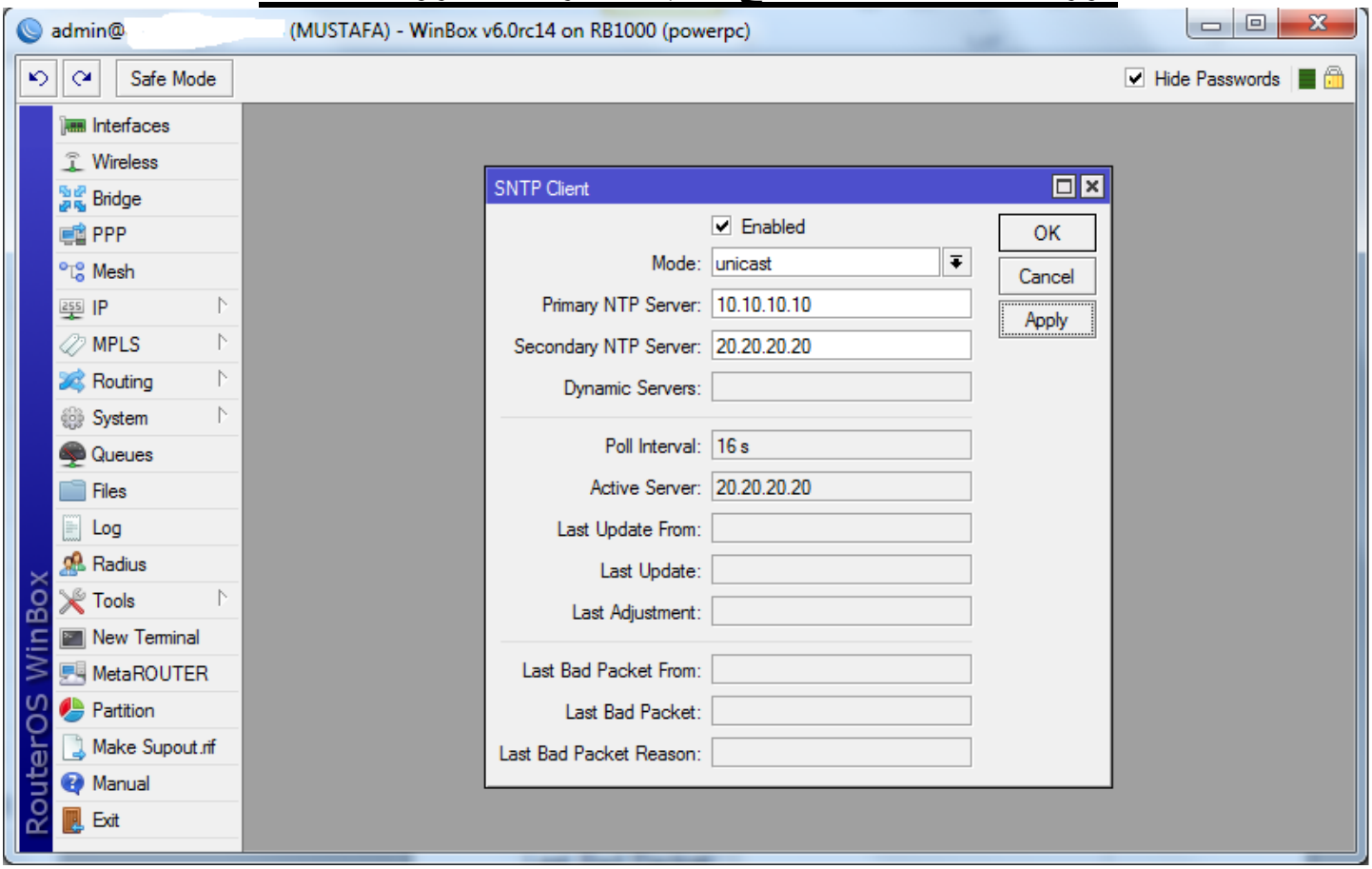
وللتراجع عن النمط الامن ننقر على (ctrl + X) مرة اخرى ليخرج الجهاز من النمط الامن وتظهر الرسالة التالية:



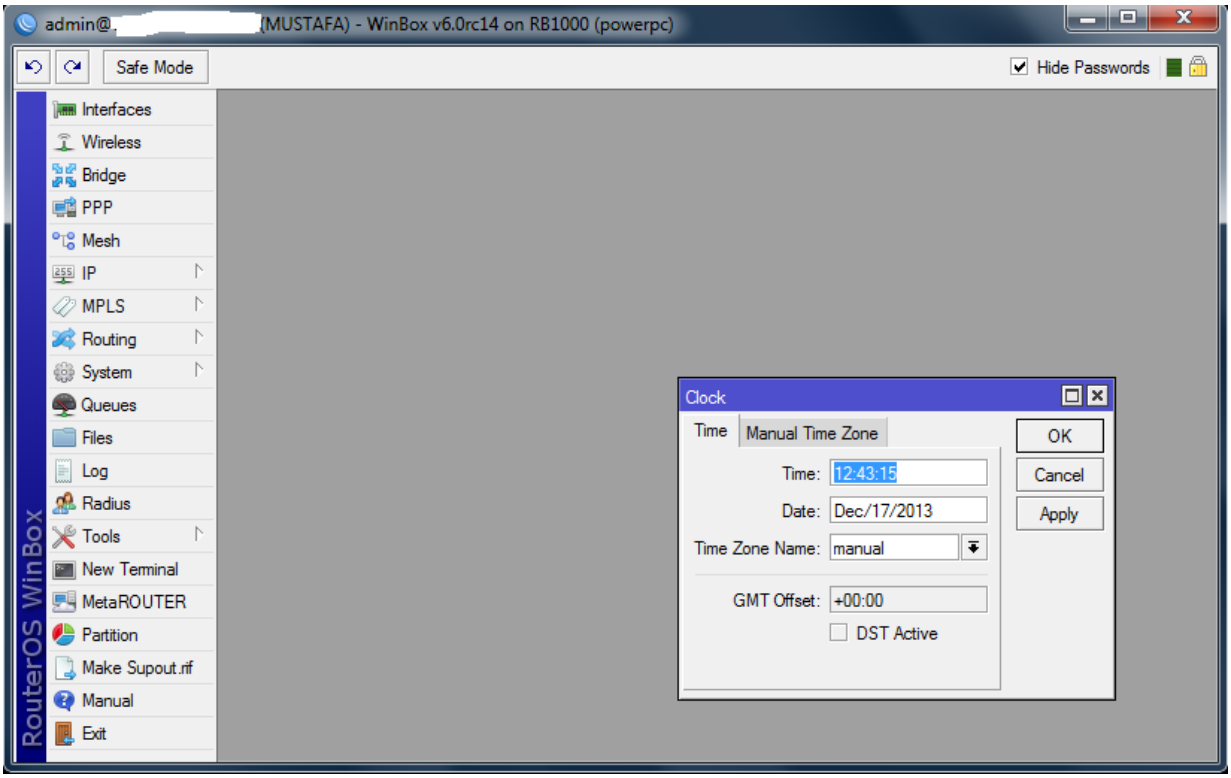
٤- ضبط بروتوكول وقت الشبكة (SNTP client) بالدخول الى تبويب (system) ثم (SNTP client) ونشغله من اختيار (enabled) واختيار نمط (unicast) وندخل عنوان سيرفر الوقت للشبكة في حالة وجوده وكما يلي:



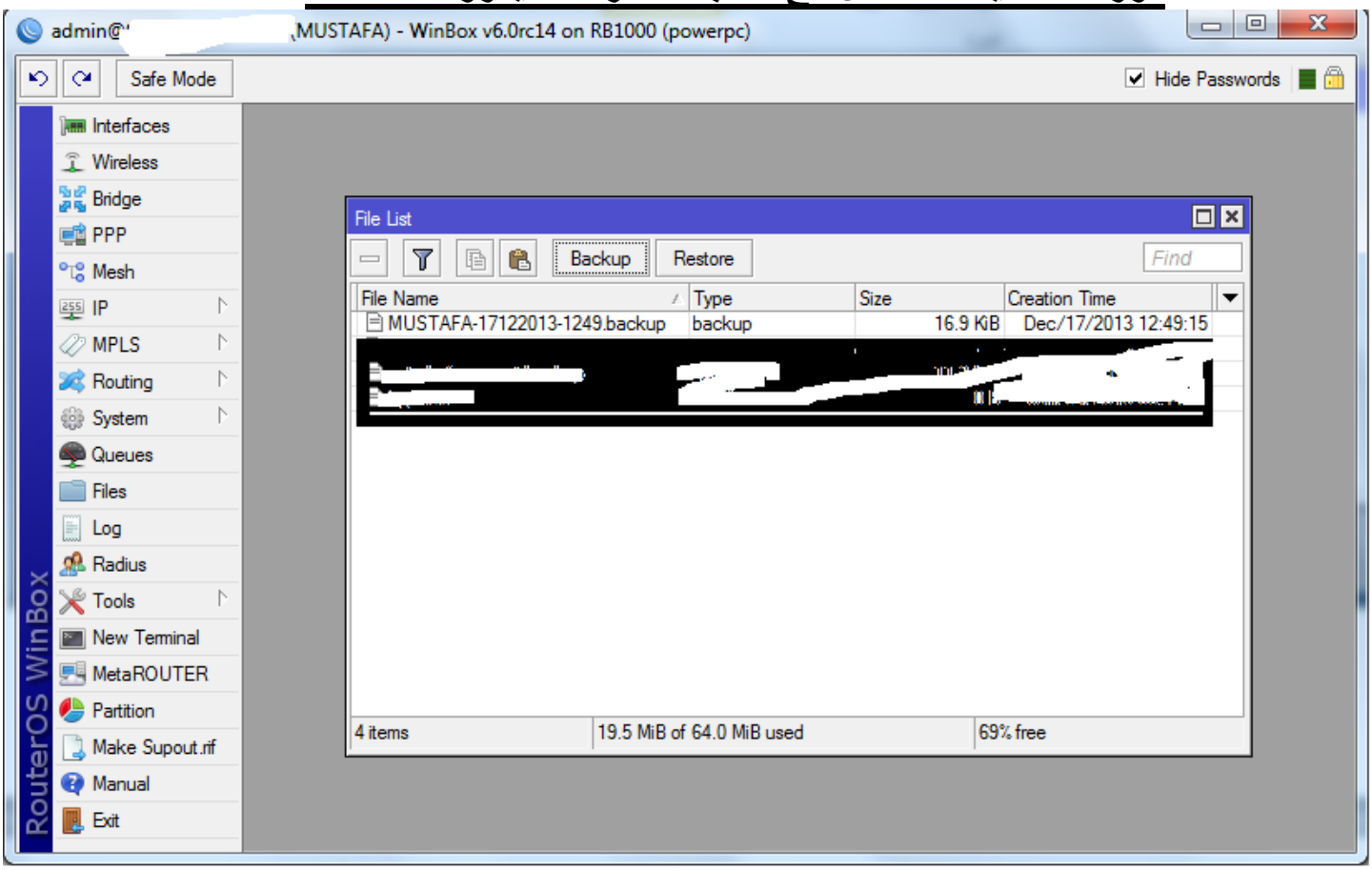
وبعد ضبط الاعدادات تكون النتيجة كالاتي:



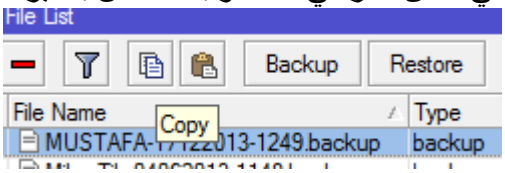
وبخصوص ساعة النظام فنذهب الى (system) ثم (Clock) ونضبط الاعدادات للوقت والتاريخ الخاص بالجهاز لتظهر النافذة التالية:



٥- حفظ نسخة احتياطية من الاعدادات ويتم ذلك بالذهاب الى (files) ثم النقر على زر (backup) لتظهر لدينا نسخة من ملف الحفظ الاحتياطي وكالاتي:



والان نستطيع الرجوع الى نقطة الخزن الاحتياطي بالنقر على زر (restore) وكذلك يمكن حفظ نسخة من هذه الاعدادات في مكان اخر في الحاسوب الخاص بمدير النظام بالنقر على اسم الملف والنقر بعدها على اشارة ال(copy)



وعمل لصق (paste) في اي مكان في الحاسوب الخاص بنا.

الى هنا ينتهي الدرس الثاني وعذراً للأطالة.

دورة اساسيات التعامل مع منتجات شركة مايكروتك ١٩

الدرس الثالث من دورة المايكروتك

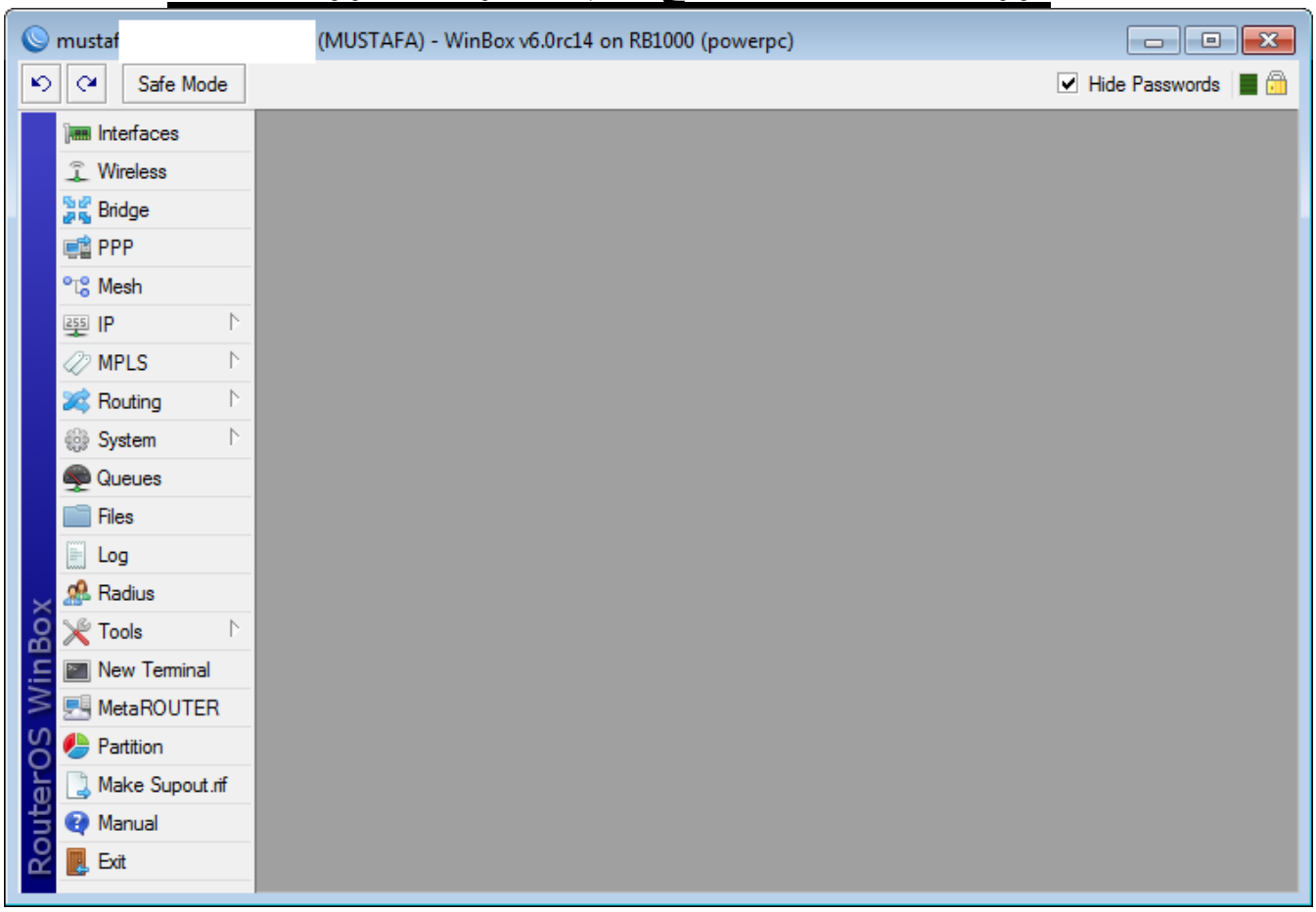
مرحباً بكم احبتي متابعي هذه الدورة التي ما زالت في بداياتها واود قبل البدء بدرس اليوم التذكير والاشارة الى بعض الامور:

١- ان الجهاز الذي نعمل عليه هو (RB 1000) ويحتوي على اربع منافذ من نوع (Ethernet) علماً ان منتجات شركة مايكروتك تضم مجموعة كبيرة من الاجهزة المختلفة من حيث الاداء والمكونات والوظائف والسعر طبعاً ويجمعها جميعاً الميزة الجميلة في انها كلها يمكن تهيئتها وضبط اعداداتها باستخدام البرنامج الجميل (winbox) لذا استوجب التذكير بذلك.
٢- ان اغلب الدورات في هذا المجال تنتهج البحث في شرح القوائم واحدة تلو الاخرى الامر الذي يرهق الدارس ولا يوصله الى نتيجة مفيدة فعلى كل حال فال(winbox) هو اداة ووسيلة لتحقيق شيء اكبر وهو تصميم وادارة وصيانة الشبكة ولا فائدة من معرفة كل قوائمه ما لم ينتج عن ذلك الدخول في سيناريوهات عملية تشرح خطوات بناء الشبكة وخيارات استخدام مكوناتها وصيانتها وهذا ما سنتطرق له ان شاء الله بعد استيفاء اساسيات التعامل مع البرنامج.
٣- قد تختلف الواجهة المعروضة هنا بعض الشيء من جهاز الى اخر بسبب اختلاف نسخة نظام التشغيل (RouterOS) المنصبة على الجهاز وقد يحصل تقديم وتأخير في بعض الخطوات لا يؤثر على السياق العام للدورة ولا ضير في اتباعه عند العمل الفعلي.

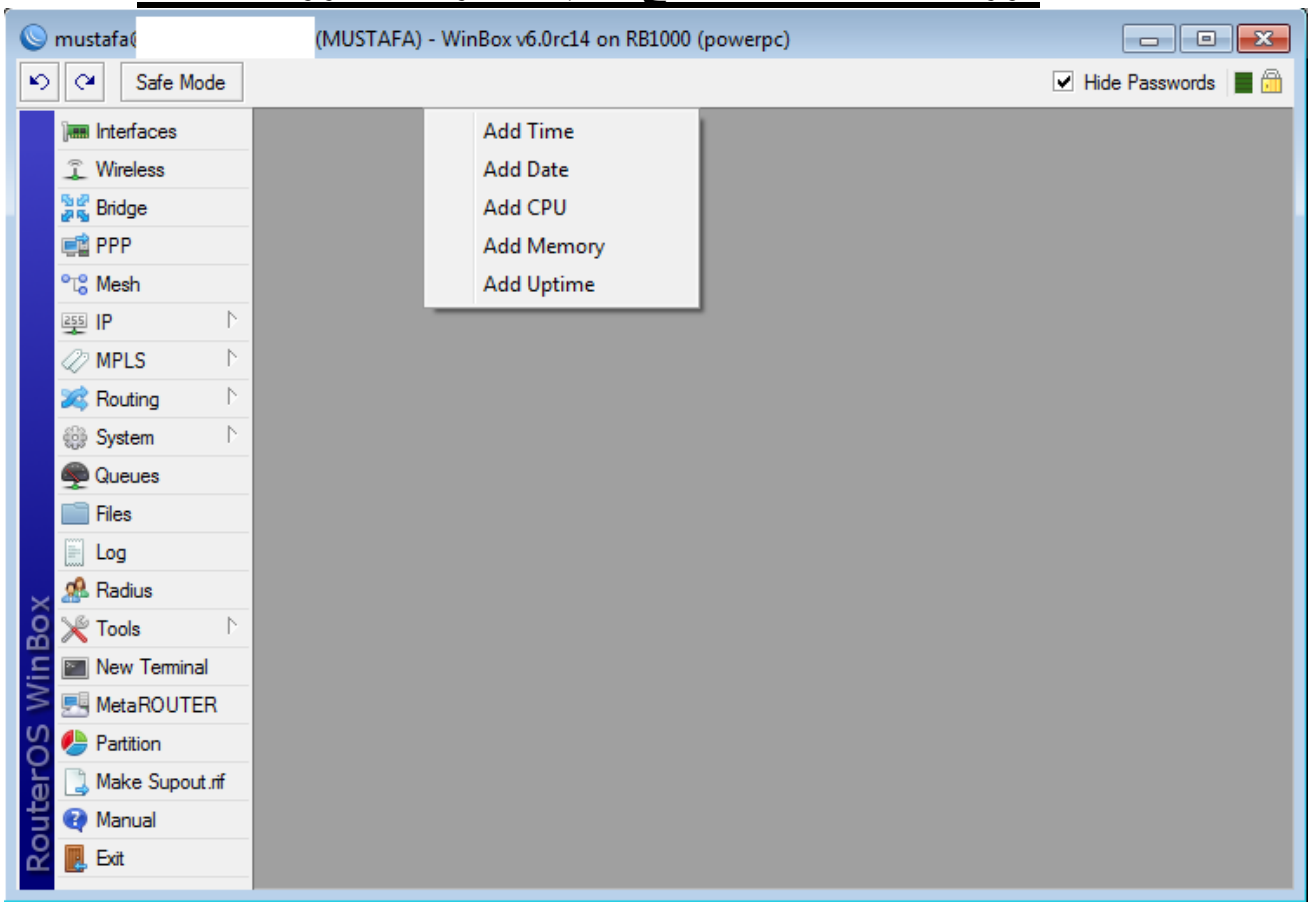
ينقسم درس اليوم الى الفقرات التالية:

١- اضافة الوقت والتاريخ وحالة المعالج والذاكرة الى الشريط العلوي لنافذة ال (winbox).
٢- كيفية عمل اعادة تشغيل للجهاز لحفظ التغييرات (rebooting).
٣- فتح واجهة الضبط بسطر الاوامر وكيفية التعامل معه.
٤- ضبط استجابة لكل حالة طارئة او حدث معين باستخدام ال (logging)
٥- الاطلاع على مجمل احداث الجهاز من سجل تسجيل الاحداث (log).
٦- استعادة ضبط المصنع للجهاز (reset configuration).

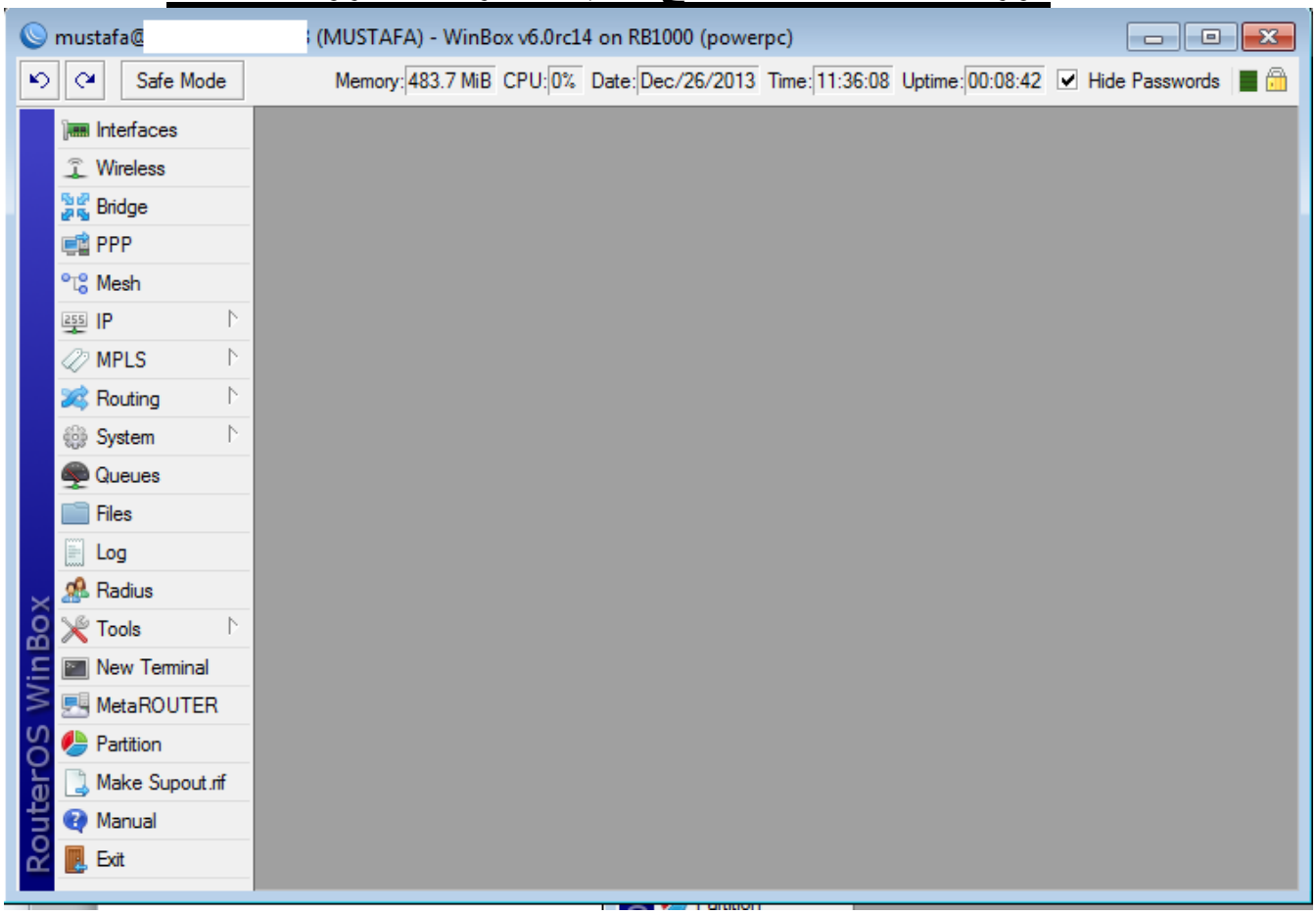
بداية يمكن اضافة معلومات عامة عن الوقت والتاريخ والحالة الحالية للمعالج والذاكرة الى الواجهة وتحديداً في القائمة العلوية لنافذة ال (winbox) كما يلي: تكون نافذة البرنامج بالشكل التالي تلقائياً قبل الاضافة:



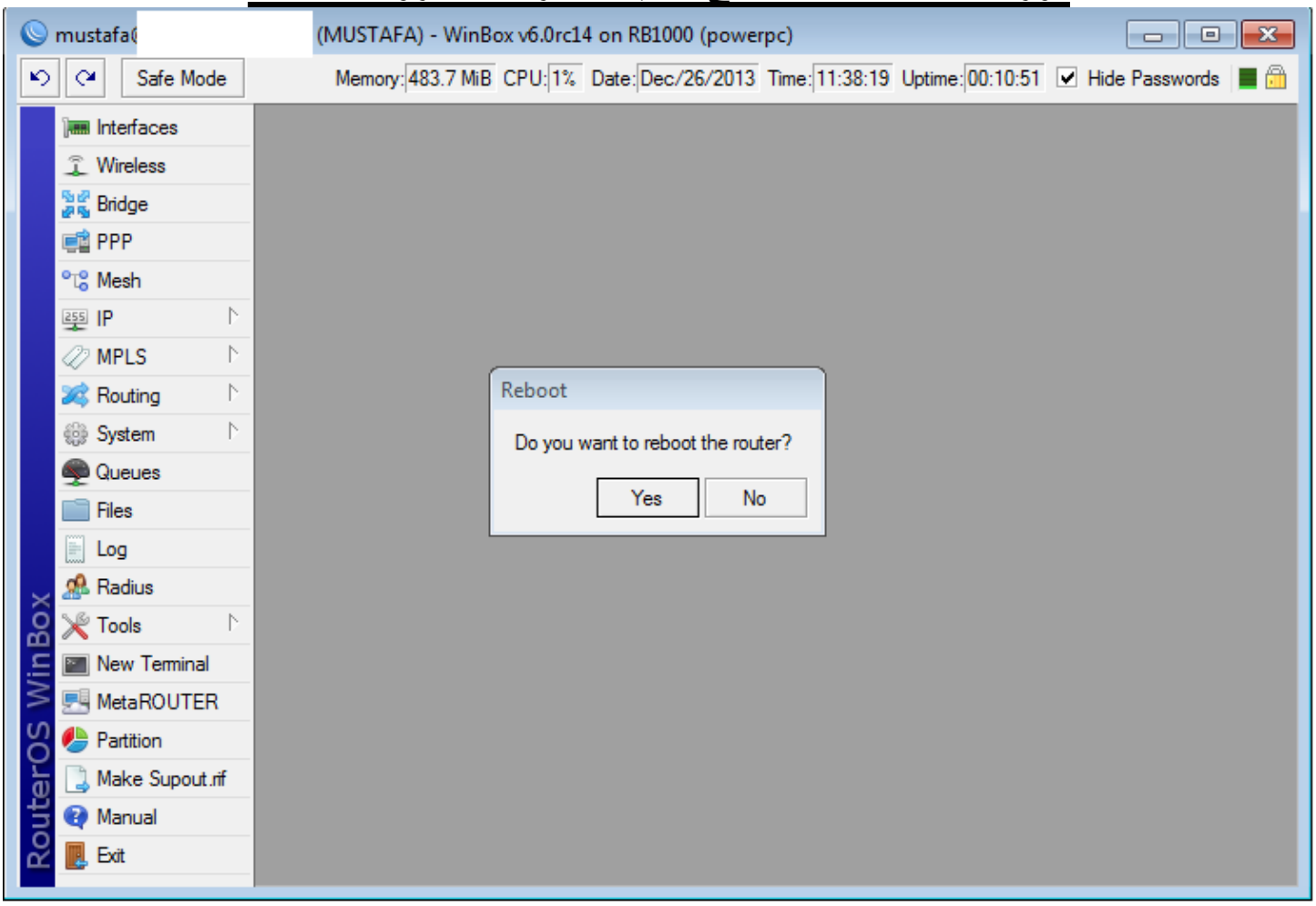
الان ننقر بالزر الايمن للماوس على جزء فارغ بالقرب من زر (safe mode) لتظهر نافذة كما في الصورة التالية:



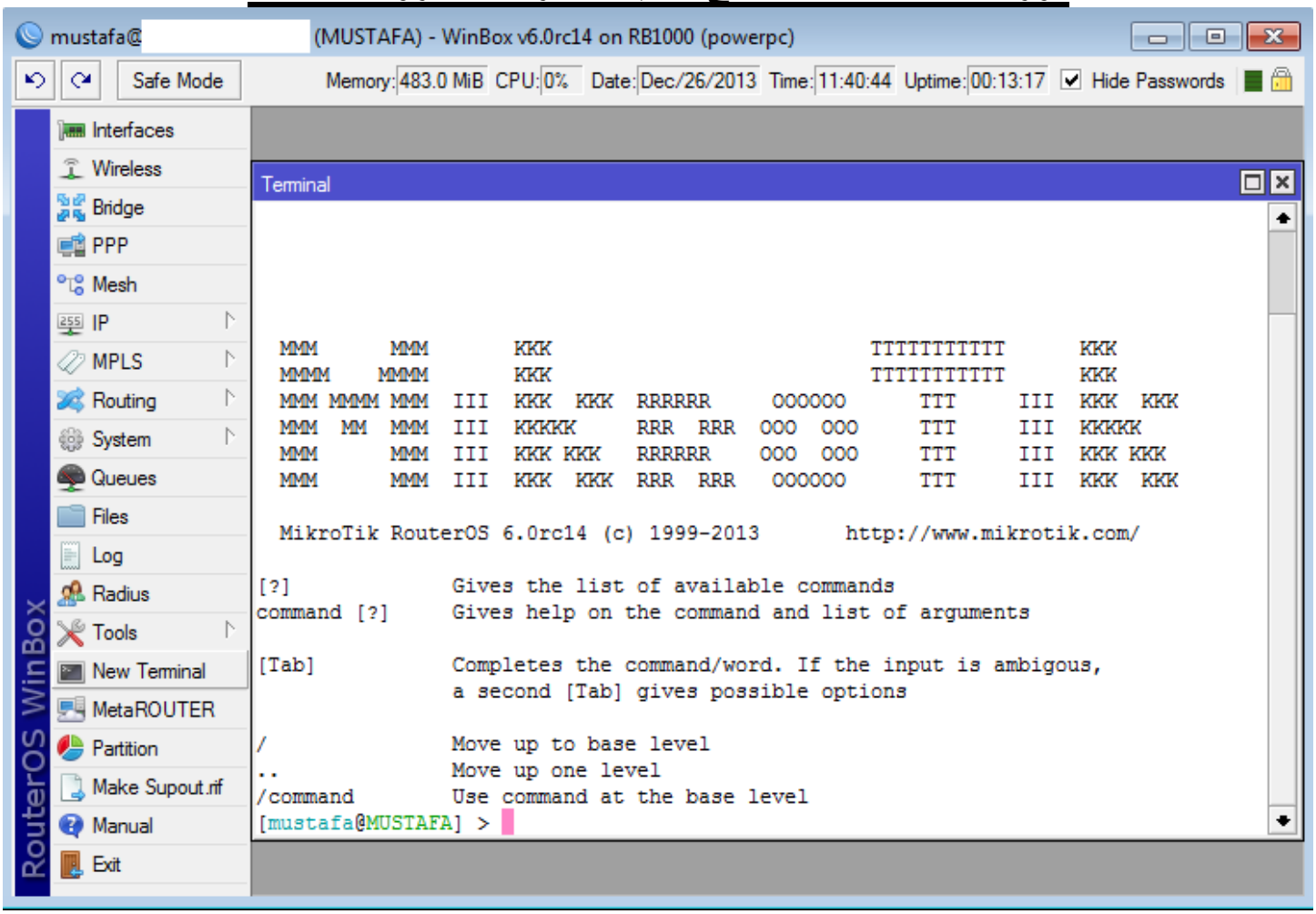
وعند النقر على كل خيار تضاف البيانات المقابلة من وقت وتاريخ وحالة معالج وحالة ذاكرة ولحذف اي منها ننقر عليه بالزر الايمن ثم (Remove)



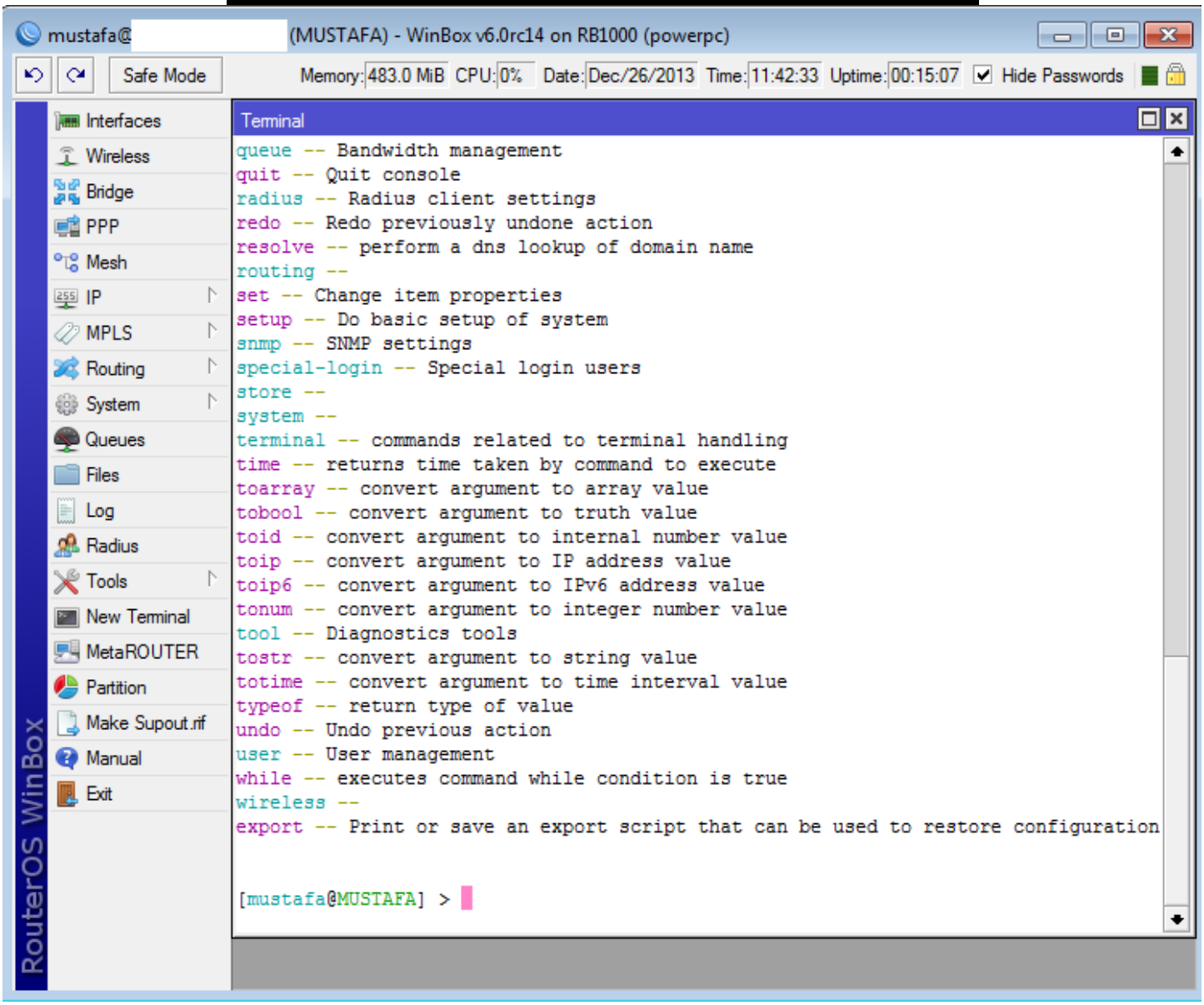
الان نصل الى الجزء الثاني من الدرس وهو ببساطة كيفية عمل اعادة تشغيل للجهاز بالذهاب الى (system) ثم (reboot) لتظهر نافذة طلب التأكيد وننقر على (ok) للموافقة وبعدها سيطلب الدخول من جديد وكما يلي:



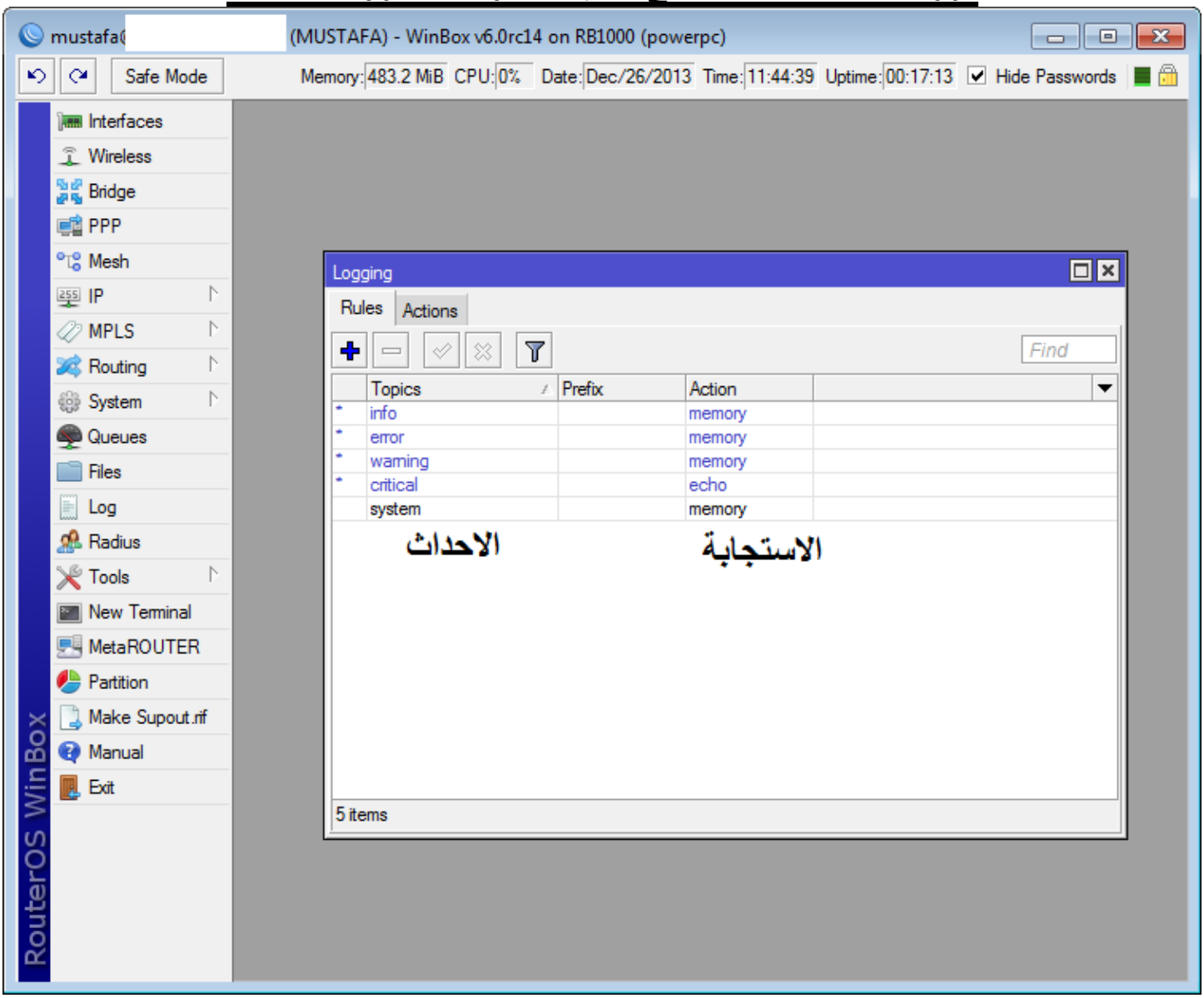
كغيره من انظمة الشبكات يدعم المايكروتك ادخال الايعازات بواسطة سطر الاوامر (command line) ونستطيع الدخول اليه بواسطة النقر على (new terminal) لتظهر الواجهة التالية:



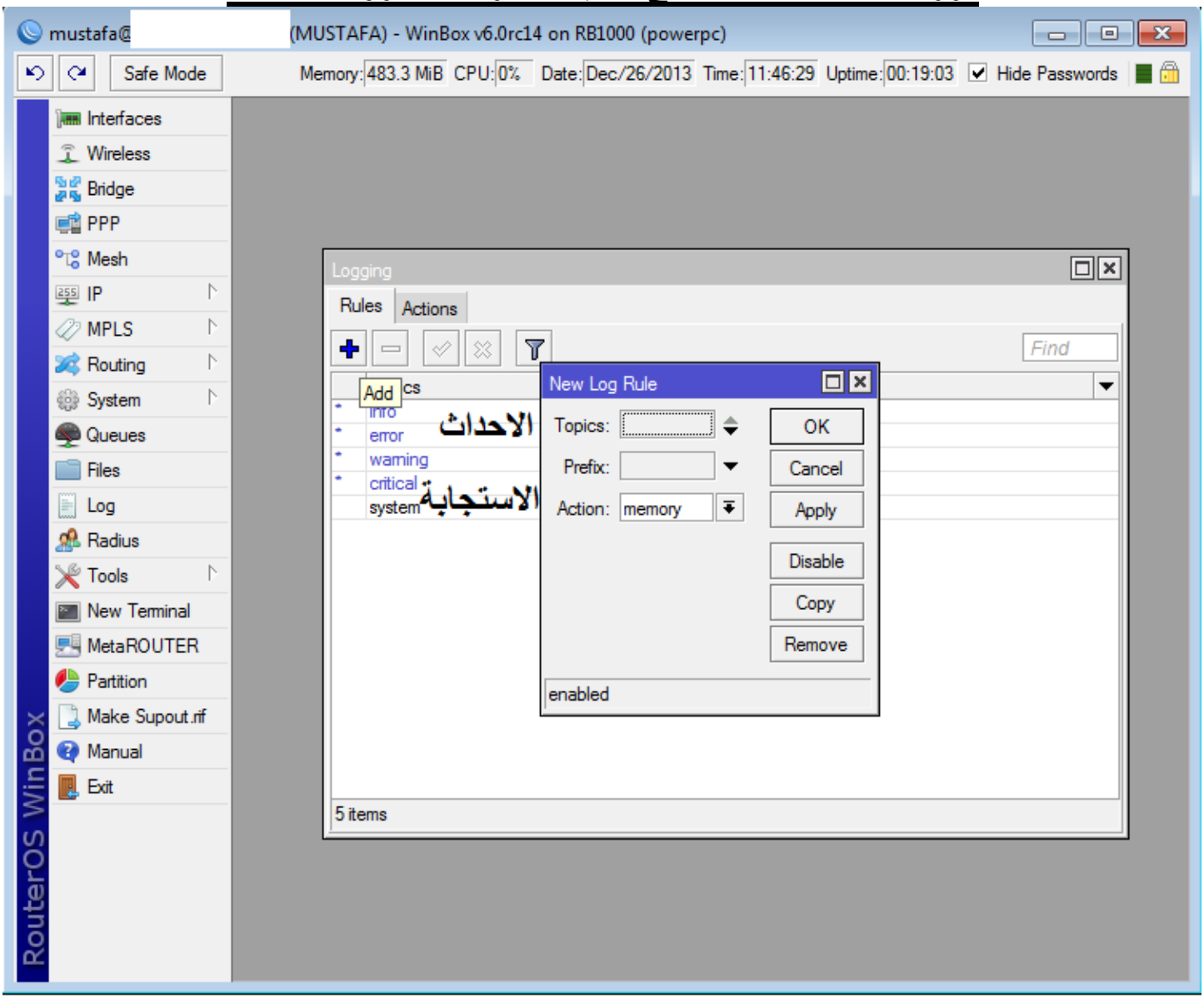
والان لمعرفة الايعازات الممكن استخدامها هنا كل ما عليك فعله هو النقر على زر (؟) لتظهر الايعازات كلها في هذه المرحلة وكما يلي:



يحتوي الجهاز حسب ضبط المصنع استجابة معينة لكل حالة طارئة او حدث اثناء عمله وللتعديل على هذه الاستجابة نذهب الى (System) ومنها الى (logging) لتظهر النافذة التالية:



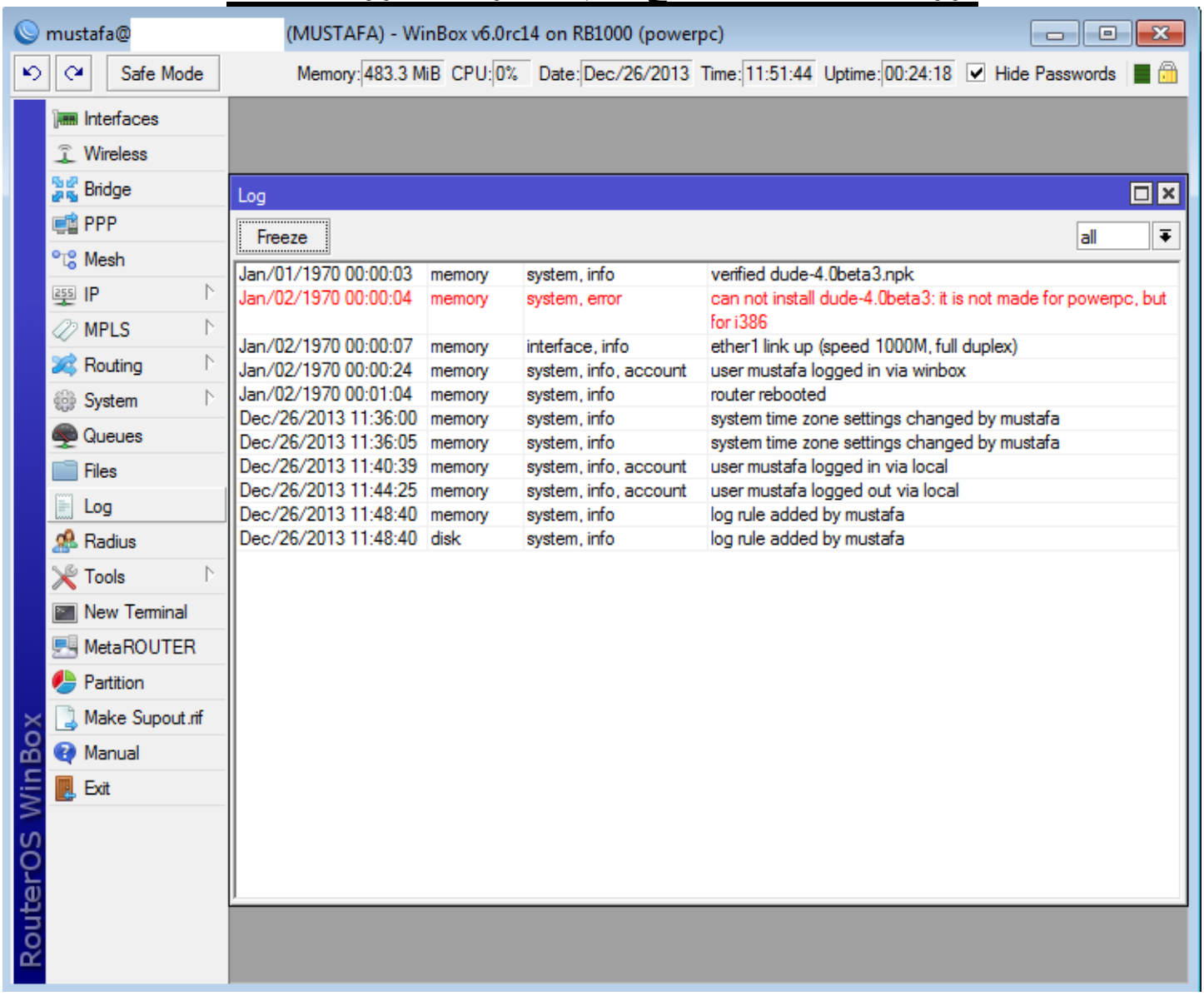
ويمكن اضافة استجابة جديدة لقاعدة (rule) معينة بالنقر على زر (+) لتظهر النافذة التالية:



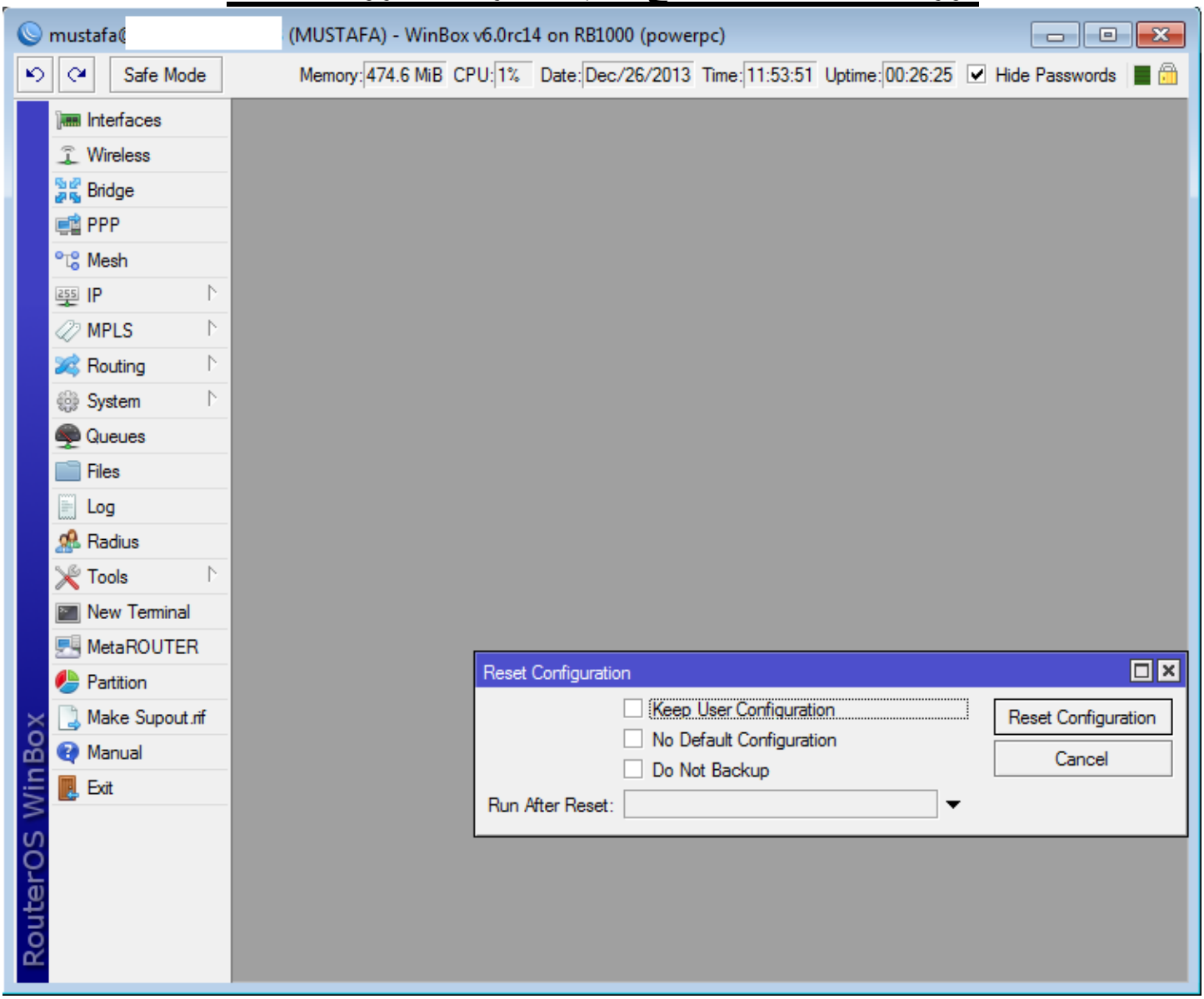
وتنقسم الاستجابة الى عدة اقسام:

١- (disk) وتعني خزن الحدث في قرص تابع للجهاز او السيرفر المرتبط به.
٢- (echo) وتعني ارسال رد فعل او رسالة استجابة للحدث.
٣- (memory) وتعني حفظ الحدث في الذاكرة.
٤- (remote) وتعني تبليغ حاسبة بعيدة بالحدث وارسال اشعار لها بذلك ويتم ادخال عنوان (IP) تلك الحاسبة من تبويب (actions).

والان للاطلاع على مجمل احداث الجهاز والفعاليات التي جرت فيه منذ تشغيله ننقر على (log) لتظهر النافذة التالية:



واخيراً لإعادة ضبط الجهاز على اعدادات المصنع نذهب الى (system) ثم (reset configuration) لتظهر النافذة التالية:



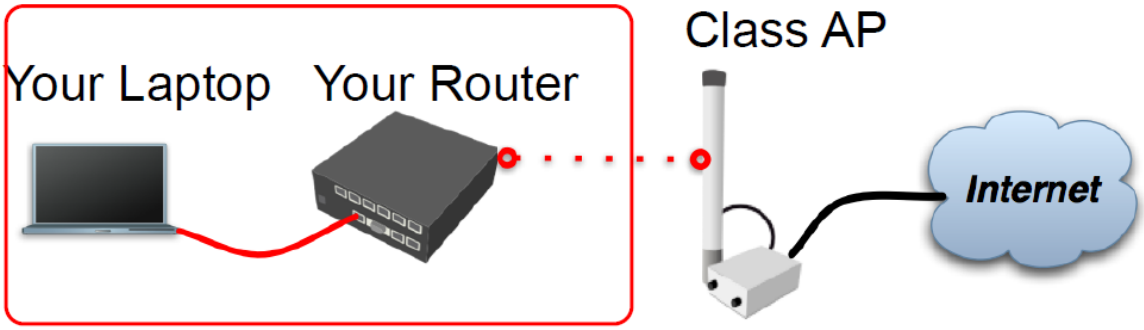
وهنا يطلب منك اختيار الحفظ لإعدادات المستخدم (keep user configurations) او لا وغيرها واخيراً وبعد اتخاذ القرار الحاسم ننقر على (Reset configuration) ويفضل ان نكون قد خزننا نسخة من الاعدادات في ال (backup) قبل الاقدام على محو كل تغييرات قمنا بها.

اتمنى ان يكون الشرح وافياً ومفهوماً وان شاء الله تستمر الدورة في شرح الاساسيات حتى نصل الى مرحلة قوية تمكننا من رسم شبكة افتراضية في مخيلتنا او طبقاً لحاجة فعلية والبدء بضبط اعداداتها.

دورة اساسيات التعامل مع منتجات شركة مايكروتك ٣٠

السيناريو العملي ١

في هذا الدرس احبتي سنتطرق الى الجزء الاهم من عمل مدير الشبكة وهو سيناريو الشبكة وطريقة ربط مكوناتها وهو القرار الاهم الذي يعتمد عليه كل العمل اللاحق له ويتوقف اختيار السيناريو المناسب على طبيعة الاجهزة المتوفرة او التي في النية شرائها وكذلك قيود السعر ونوعية الخدمة المطلوبة وعدد المستخدمين وامنية الشبكة وغيرها من الاعتبارات الاخرى الامر الذي يضع مدير الشبكة امام حيز لانهائي من السيناريوهات المحتملة ولنأخذ احد ابسطها ونرى خطوات ضبط مكوناته ونكرر الامر مع عدة سيناريوهات حتى نصل الى فهم كامل والمام بالخطوات الضرورية لكل شبكة ويبقى الباقي للمدير الشاطر للتجربة والخطأ والتعلم من الاخطاء والتوسع في البحث عن مصادر تعلم اوسع واكثر حتى يصل الى مرحلة مدير شبكة حقيقي والان لنرى السيناريو المقترح:

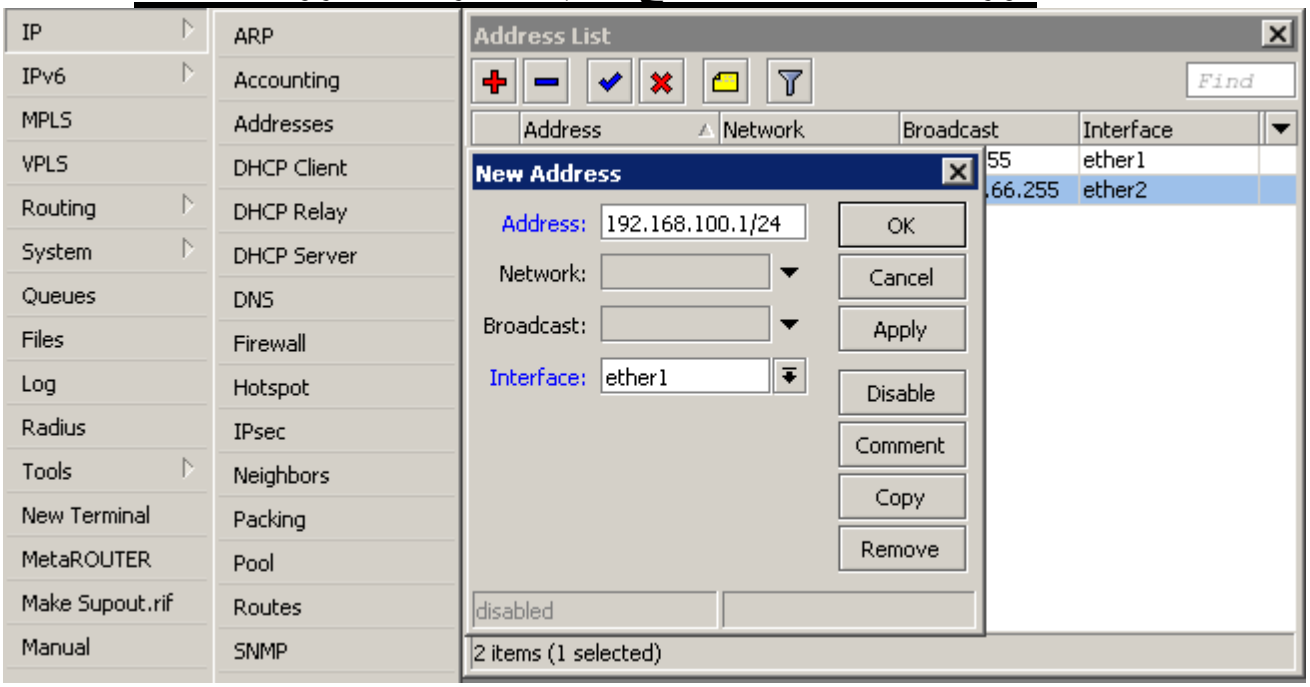


الان يمكن ان تلاحظ اخي القاري الكريم ان السيناريو يتضمن مصدر خدمة وهو غيمة الانترنت ونقطة وصول لاسلكية (wireless access point) وموجه (mikrotik router) ذو طرفين سلكي ولاسلكي وحاسبة طرفية واحدة اي مستخدم واحد وهذا هو الوضع الاولي وحال اكمال الاعدادات نستطيع استبدال اللابتوب بسويتش (switch) ومنه الى الحاسبات السلكية او اللاسلكية والان لنرى خطوات اعداد الشبكة:

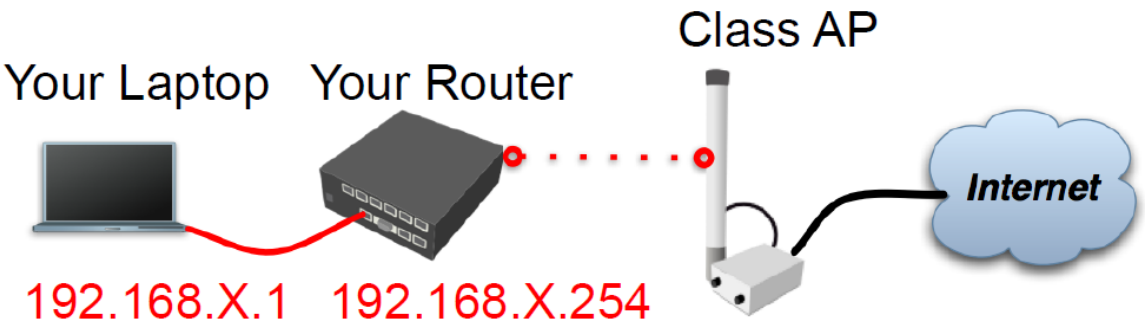
١- من اللابتوب الى الراوتر.
٢- من الراوتر الى نقطة الوصول.

- بداية لضبط اعدادات الموجه واللابتوب نقوم بأيقاف اي واجهات لاسلكية (wireless interfaces) في اللابتوب ونضبط عنوان اللابتوب ليكون (192.168.100.1) وقناع الشبكة ليكون (255.255.255.0) وعنوان بوابة الشبكة (default gateway) ليكون (192.168.100.254).

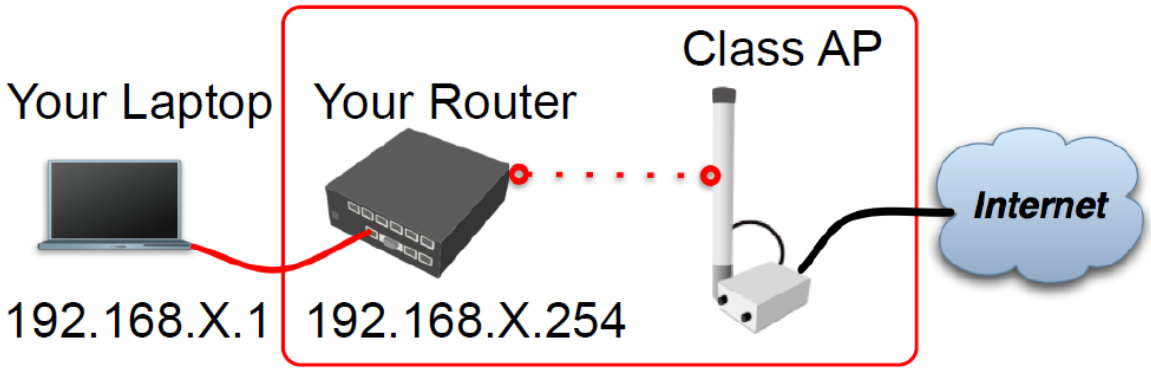
- نربط الحاسبة الشخصية بالراوتر بسلك كروس اوفر كما تم شرحه سابقاً وننصب ال (Winbox) او في الحقيقة نقوم بتنزيله من موقع الشركة وكما تم شرحه ايضاً سابقاً وندخل الى الراوتر عن طريق ال (mac address) ونضيف له عنوان الى المنفذ المرتبط باللابتوب مباشرة ليساوي عنوان بوابة الشبكة التي تم اسنادها قبل قليل (192.168.100.254) وكما في النافذة التالية:



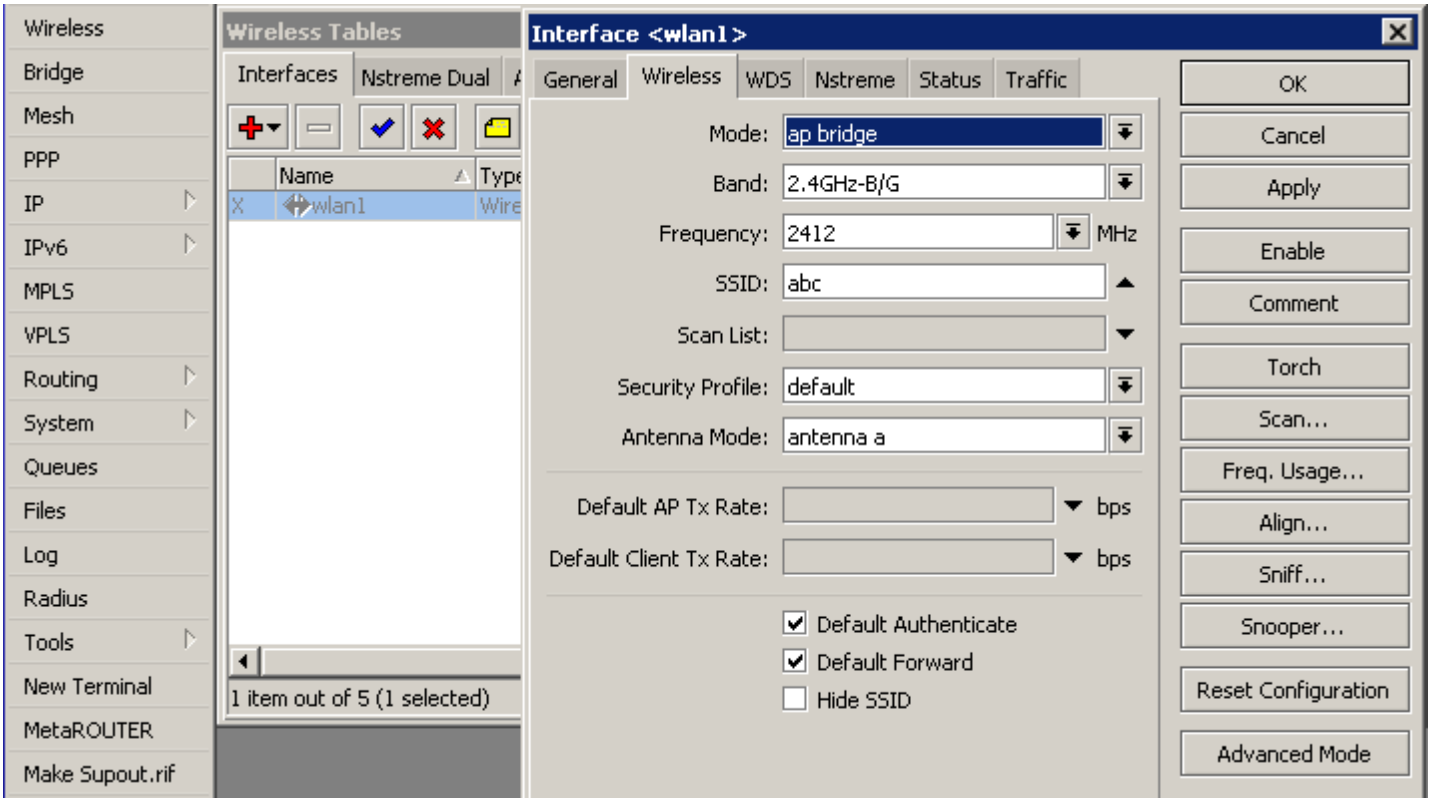
الان نقوم بأغلاق برنامج ال(Winbox) ونعيد فتحه بأستخدام عنوان (IP) حيث لا يجب الاتصال عن طريق ال (MAC) الا اذا كان لا يوجد (IP) والان تكون نتيجة الاعدادات كالاتي:



والان ننتقل الى الخطو التالية وهي ضبط اعدادات الاتصال بين الراوتر والانترنت او (access point) وكما في النافذة ادناه:



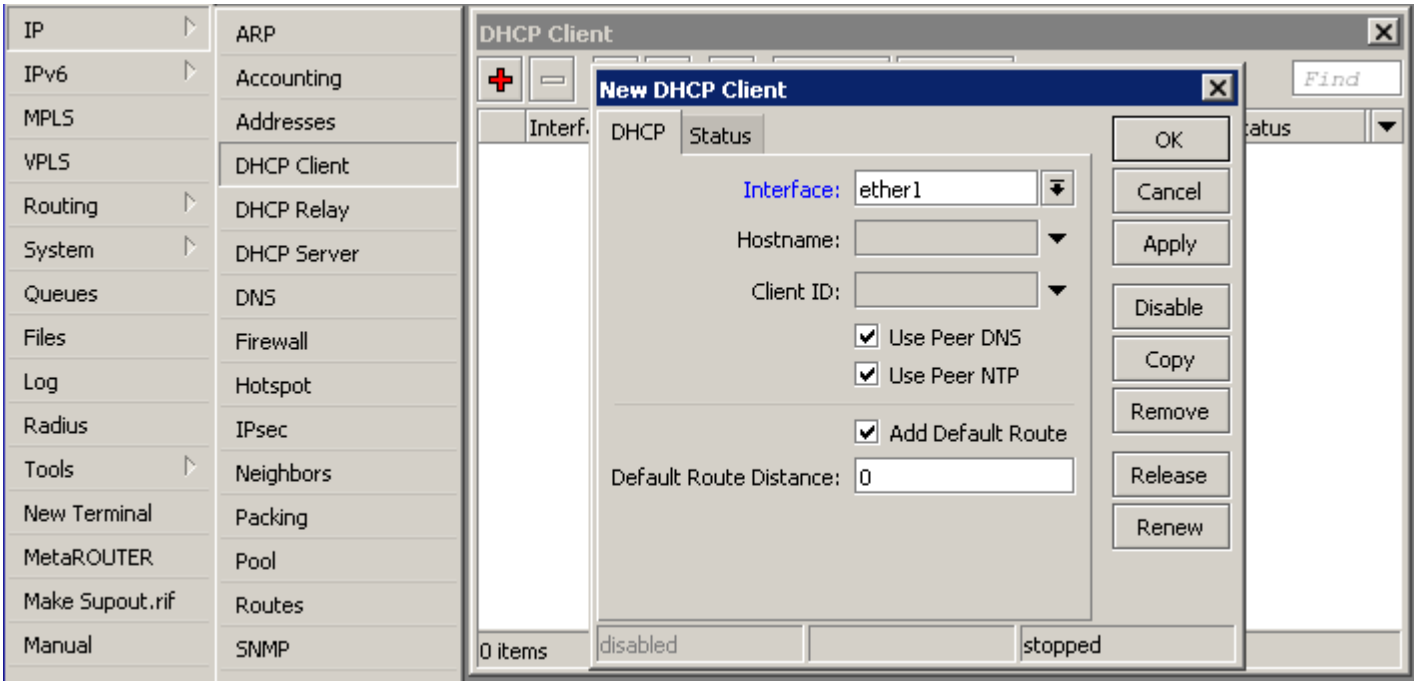
نقطة الوصول في حالتنا هذه يمكن ان تكون اي جهاز ذو قابلية ارسال واستقبال لاسلكي ولما كانت الكثير من منتجات مايكروتك تدعم هذه الخواص وباسعار مناسبة وخصائص مميزة وامكانيات بسيطة الاعداد فيفضل استخدام احد منتجات مايكروتك لتكون نقطة الوصول خاصتنا ولتكون قابلة لأستلام اشارات لاسلكية من القمر الصناعي او من نقطة بث اخرى نضبها لتكون بطور (access point AP) اما الموجه المرتبط بها لاسلكياً فلأنه سيكون محطة الاستلام شبه النهائية للأشارة اللاسلكية فيجب ان يكون بطور (Station) ولضبط اعدادات منفذ الوايرلس ننقر على تبويب (wireless) وكما في النافذة التالية:



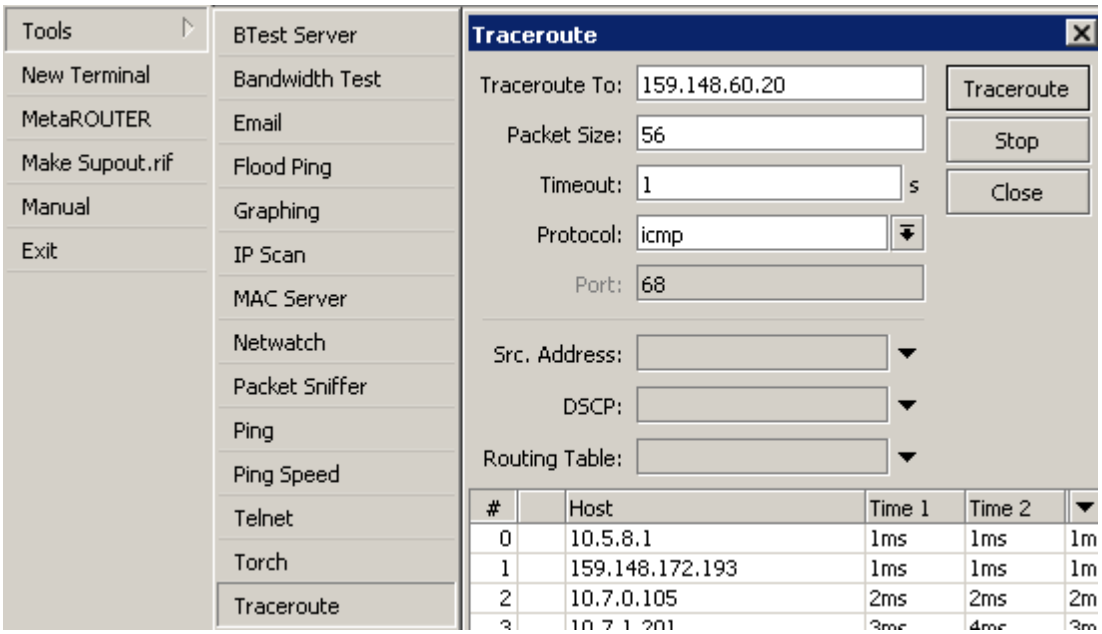
وبعد ضبط اعدادات نقطة الوصول اللاسلكية واسناد اسم للشبكة التي تبثها ولتكن (my net) نذهب الان الى الموجه خاصتنا ونقوم بالنقر على تبويب (wireless) ثم الذهاب الى زر (scan) للبحث عن الشبكات اللاسلكية وحين نعثر على شبكتنا (my net) نقوم بالنقر على اتصال (connect) والان نحن متصلين بنقطة الوصول اللاسلكية.

ملاحظة لابد من اخذها بعين الاعتبار وهي ان المنفذ اللاسلكي للموجه يحتاج الى عنوان (IP) ايضاً ولما كان يجب ان يتصل بنقطة الوصول فيجب ان نجعله يحصل على عنوانه منها حيث ان كل نقاط الوصول اللاسلكية (Wireless access points) توفر قابلية اسناد عناوين (IP) ديناميكية ولكن فقط بشرط تفعيل خيار (DHCP client) في جهاز الراوتر خاصتنا وكما يلي:

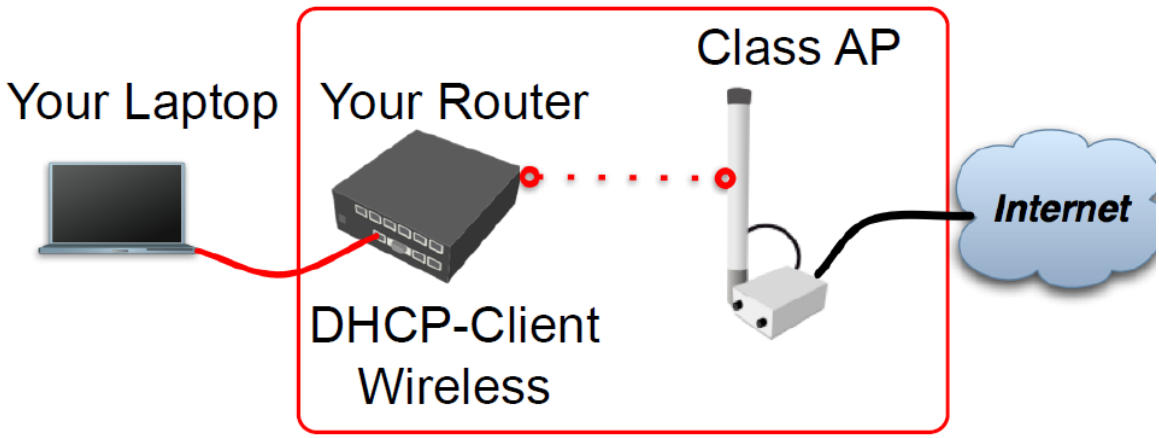
نذهب الى تبويب (DHCP client) ثم ننقر على علامة (+) ونختار المنفذ الذي نريد له ان يحصل على عنوان (IP) من ال (Access Point) وكما في النافذة التالية:



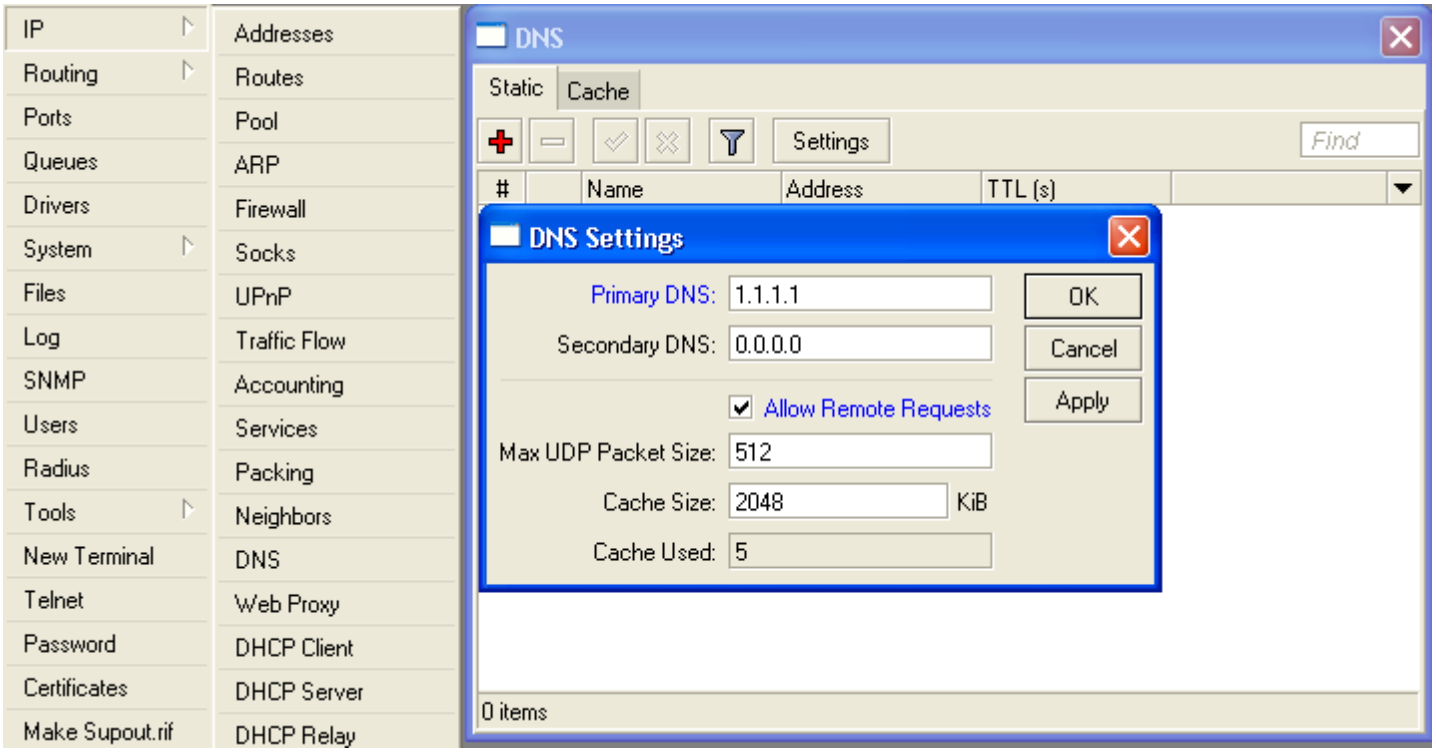
والان اكتملت اعدادات الاتصال بالانترنت وكل ما علينا فعله هو التأكد من الاتصال بالانترنت ويتم ذلك بالذهاب الى تبويب (tools) ومنها الى (tracert or ping) ونكتب عنوان الموقع المراد اختبار الاتصال به وكما في النافذة التالية:



والان شبكتنا مكتملة الاتصال بالانترنت ويفترض ان يكون سيناريو ارتباطها كما في الصورة التالية:

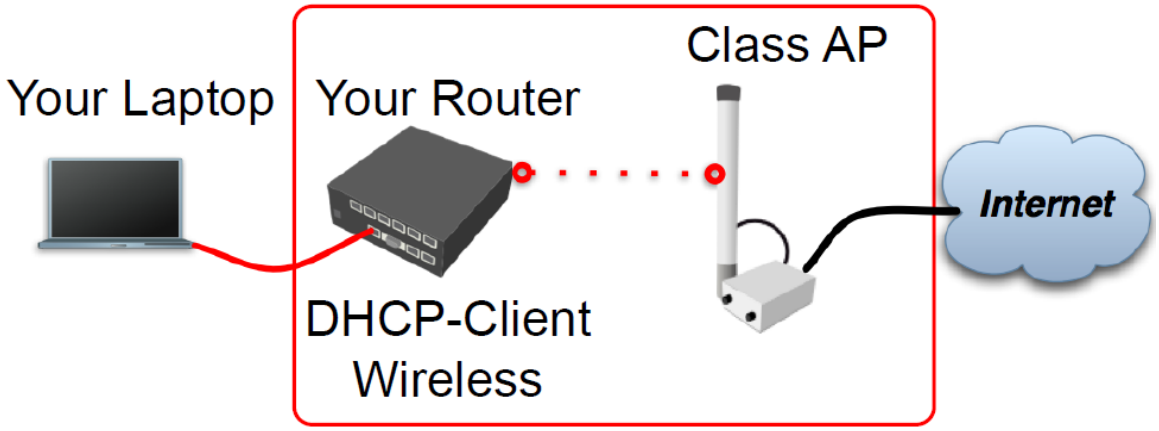


والان لتستطيع الحاسبات المتصلة بالراوتر مباشرة او عبر سويتش او هب او غيرها الدخول الى مواقع الانترنت المختلفة فأنها يجب ان تتصل بخادم نظام مجال الاسماء (Domain Name System DNS) والذي يقوم بتحويل العناوين الى اسماء والعكس بالعكس وكما قلنا فان منتجات المايكروتك متعددة الخصائص وتوفر قابلية العمل كخادم DNS ويتم ذلك بالذهاب الى تبويب (IP) ومنه نختار (DNS) لتظهر نافذة نختار منها اضافة خادم DNS جديد بالنقر على (+) وندخل عناوين (primary DNS and secondary DNS) مع ملاحظة ضرورة اختيار خيار السماح بطلبات عن بعد (allow remote requests) وكما في الصورة التالية:

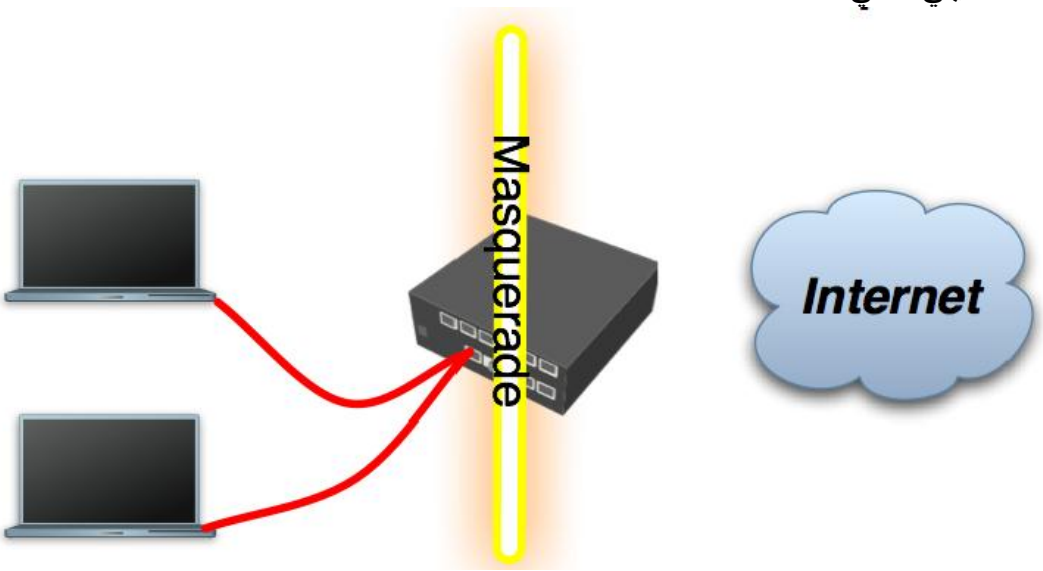


والان لنخبر اللابتوب او اي جهاز اخر متصل بالروتر بأن يستخدم الروتر كخادم DNS نقوم بأدخال عنوان (router IP) في حقل ال (DNS server) ضمن اعدادات اللابتوب وهكذا نكون قد اكملنا اجراءات الاتصال وستكون الشبكة جاهزة للبدء بالعمل بعد عدة خطوات سنقوم بشرحها ان شاء الله في الدرس القادم.

الدرس الخامس من دورة المايكروتك
بعد ان قمنا برسم سيناريو تجريبي لأبسط نوع من انواع الشبكات التي يمكن استخدام منتجات المايكروتك فيها نكمل مسيرتنا في تهيئة الشبكة لتكون جاهزة للاستخدام وكما يلي:
للتذكير فقط بشبكتنا من الدرس السابق فأننا وصلنا الى تعريف الحاسوب الشخصي على سيرفر ال DNS واصبحت الشبكة بالشكل التالي:



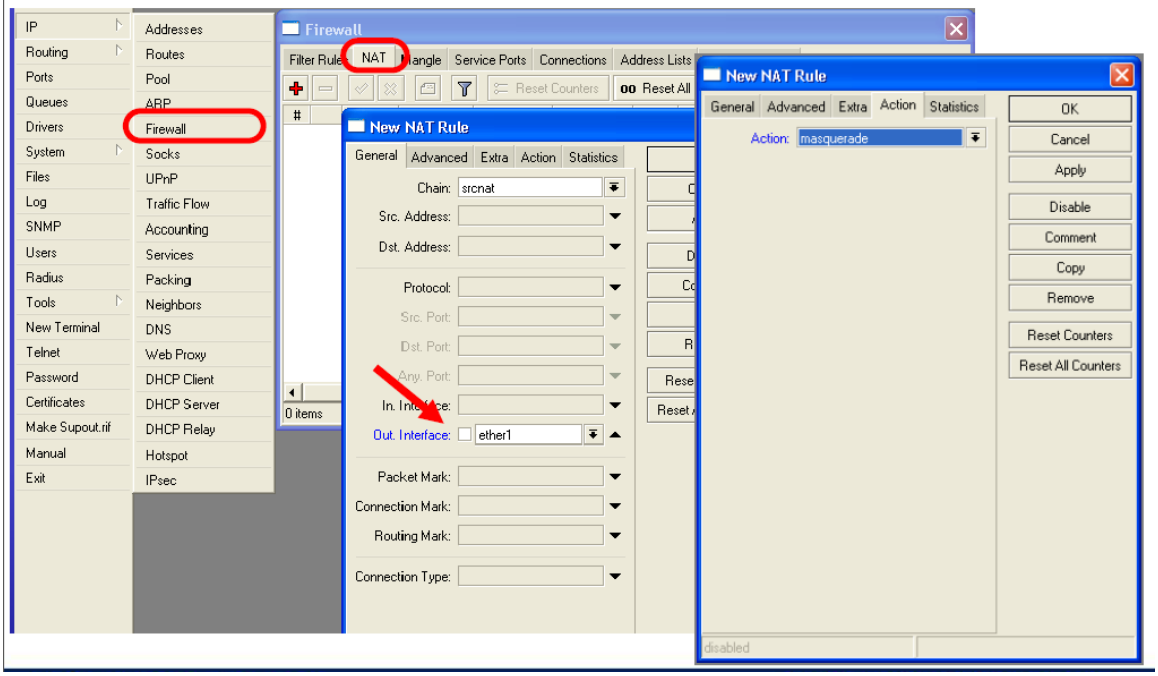
والان ولمنع اي حاسوب اخر من الاتصال بالشبكة اللاسلكية نقوم بإخفاء اسمها باستخدام تقنية ال (Masquerade) وكما في الشكل التخيلي التالي:



ويستخدم هذا التنكر (masquerade) في الشبكات التي يمكن ان يصل اليها العامة (with public access) حين تكون هناك عناوين خاصة في الشبكة (private addresses) وادناه جدول العناوين الخاصة المتاحة في عناوين الجيل القديم (IPV4):

Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0-192.168.255.255

ويكمن اضافة التنكر بأتباع الخطوات المبينة في الخطوات ادناه:



الى هذه المرحلة يفترض ان تعمل الشبكة بشكل صحيح ولكن قد تحصل عدة اخطاء يمكن تلخيصها في النقاط التالية:

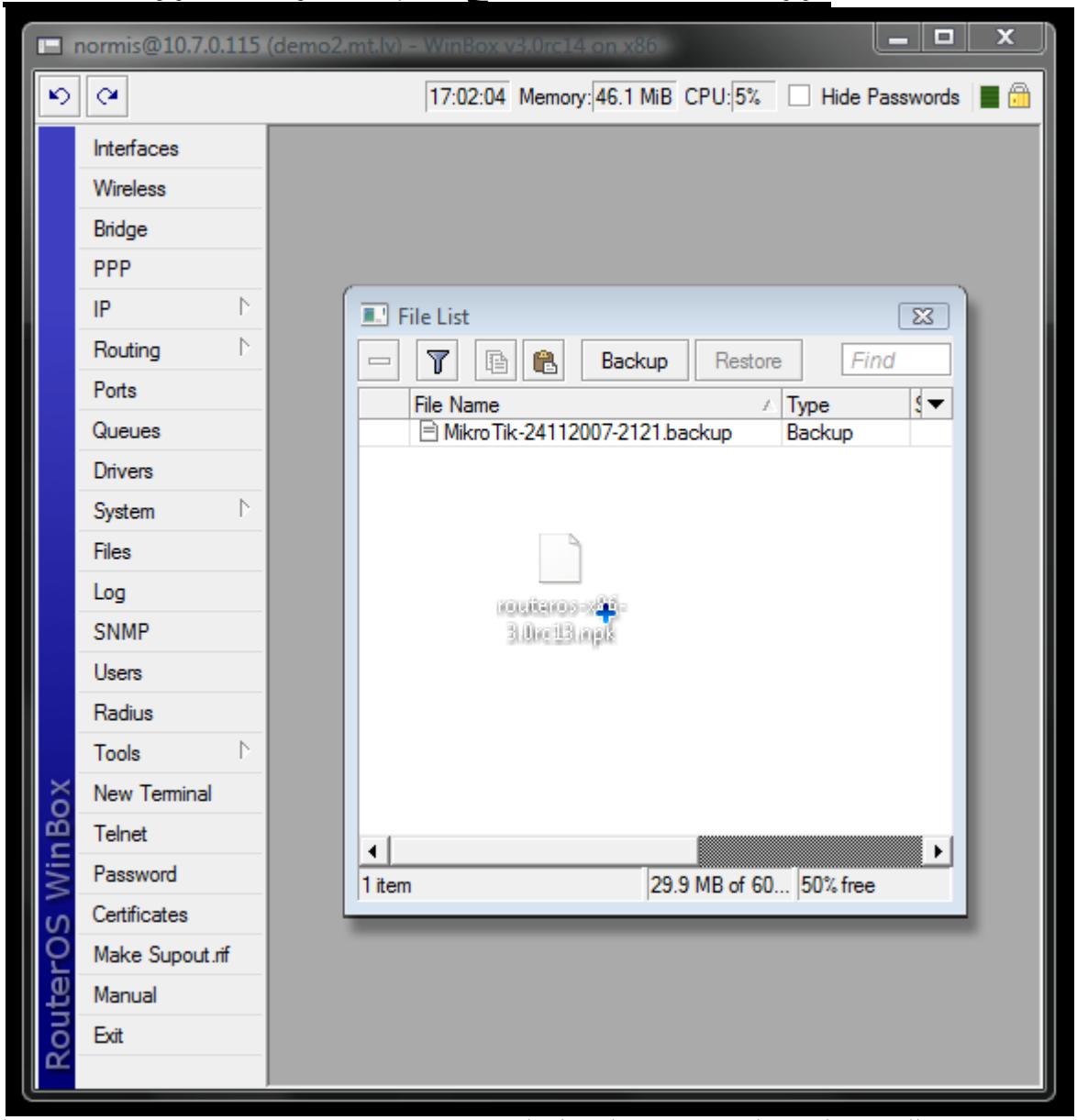
١- الراوتر لا يمكنه الوصول الى ما بعد نقطة الوصول (AP).
٢- الراوتر لا يمكنه تحويل الاسماء الى عناوين او العكس.
٣- الحاسوب لا يمكنه الوصول الى الراوتر.
٤- الحاسوب لا يمكنه تحليل وتحويل العناوين والاسماء.

ولحل هذه المشاكل نتأكد من التالي:

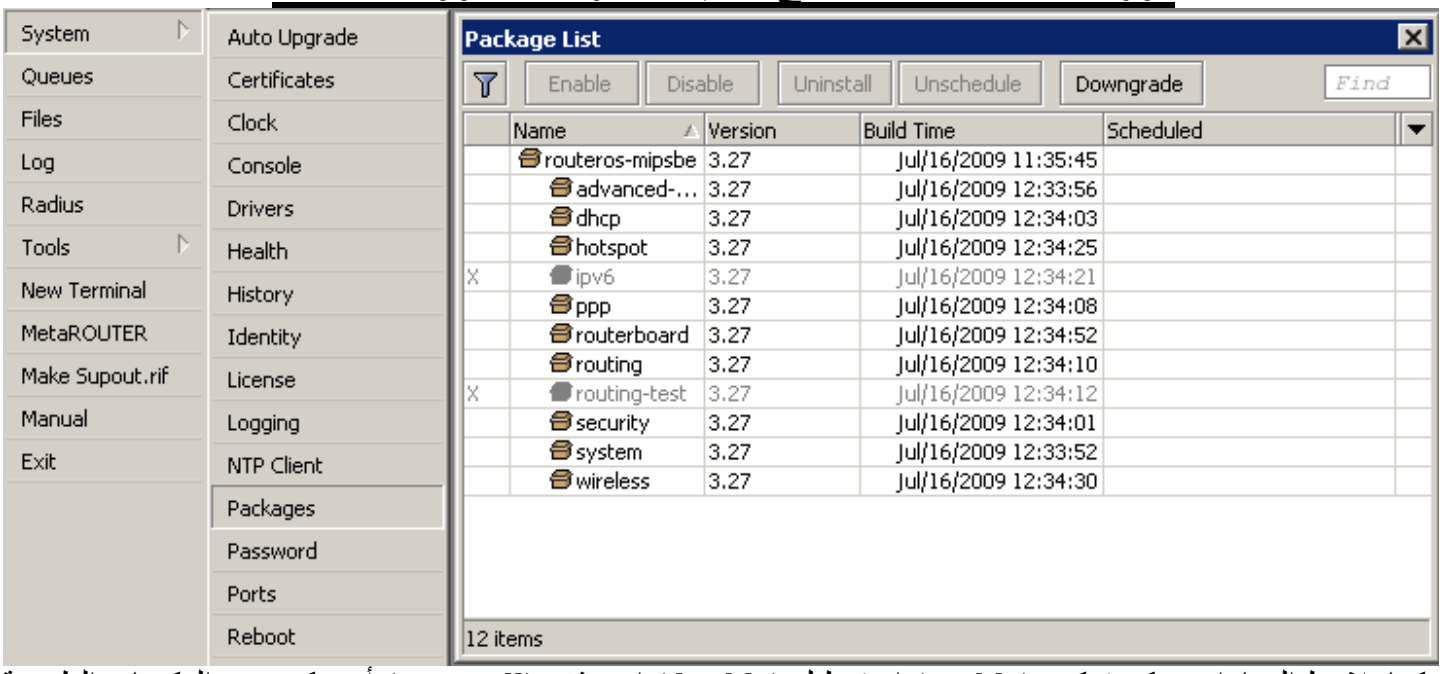
١- هل يعمل التنكر او لا؟
٢- هل يستخدم الحاسوب الراوتر كسيرفر (DNS) وبوابة شبكة (default gateway)؟

والان ننتقل الى كيفية تطوير (upgrade) نظام تشغيل الراوتر وذلك بأتباع الخطوات التالية:

١- نقوم بالدخول الى موقع شركة مايكروتك (www.mikrotik.com) والذهاب الى تبويب (downloads) ومنه نقوم بتنزيل النسخ الاحدث والاكثر تطوراً من نظام تشغيل الراوتر او ببساطة ندخل الى العنوان (ftp://192.168.200.254) ومنه نقوم بتنزيل التطوير.
٢- نقوم برفع الملف المحمل الى الراوتر عن طريق برنامج ال (winbox) بالذهاب الى تبويب ملفات (files) ونقوم بسحب وافلات الملف الى النافذة كما في الصورة التالية:



٣- والان للتحكم بالحزم المتاحة نقوم بالدخول الى تبويب (system) ثم (packages) وكما في الصورة التالية:

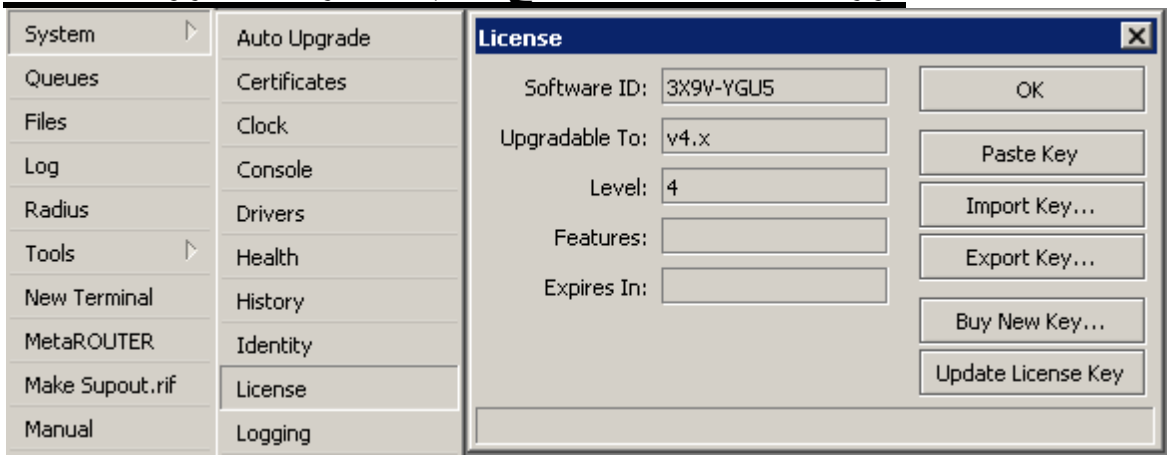


وكما نلاحظ الخيارات يمكن تمكين (enable) او تعطيل (disable) او حذف (uninstall) أي مكون من المكونات الطبيعية لنظام تشغيل الراوتر والتي تتضح في الجدول التالي:

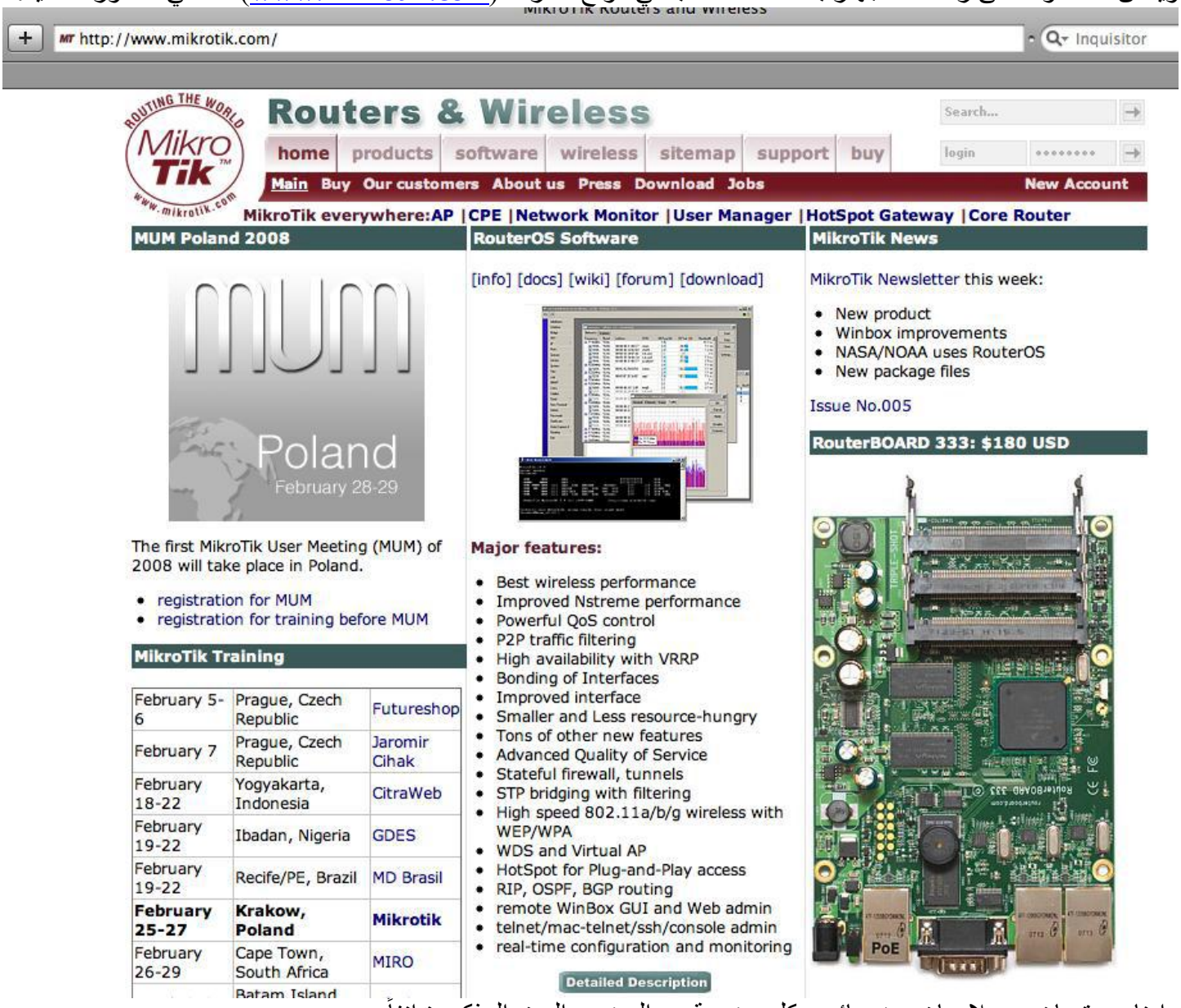
Name	Functions
advanced-tools	Email client, ping, netwatch
dhcp	DHCP Server and Client
hotspot	HotSpot Gateway
ntp	NTP server
ppp	PPP, PPTP, L2TP, PPPoE
routerboard	RouterBOARD specific functions
routing	RIP, OSPF, BGP
security	Secure Winbox, SSH, IPSec
wireless	Wireless 802.11a/b/g
user-manager	User-Manager management system
ipv6	IPv6

والان نصل الى الحديث عن رخصة استخدام الراوترات من شركة سيسكو حيث يتم بيع كل جهاز مع رخصة من مستوى معين وتتراوح تلك المستويات من (١-٦) بحيث يكون المستوى الاول الاقل صلاحيات والثاني اكثر وهكذا حتى نصل الى المستوى السادس والذي يمتلك صلاحيات مطلقة كما سنرى بعد قليل في جدول يفصل صلاحيات ومميزات كل مستوى رخصة.

يمكن الاطلاع على مستوى رخصة الجهاز الحالي من تبويب (system→ license) كما في الصورة التالية:



ويمكن الحصول على رخصة للجهاز بعد انشاء حساب في موقع الشركة (www.mikrotik.com) كما في الصورة التالية:



وادناه مستويات وصلاحيات وخصائص كل رخصة من الرخص الست المذكورة انفاً:

Level number	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Upgradable To	-	no upgrades	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes(*)	yes	yes	yes
EoIP tunnels	24h limit	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200	200	500	unlimited
PPTP tunnels	24h limit	1	200	200	500	unlimited
L2TP tunnels	24h limit	1	200	200	500	unlimited
OVPN tunnels	24h limit	1	200	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
Synchronous interfaces	24h limit	-	-	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited

الحلقة السادسة من سلسلة شرح سيرفر المايكروتك – ضبط اعدادات PPPOE Server

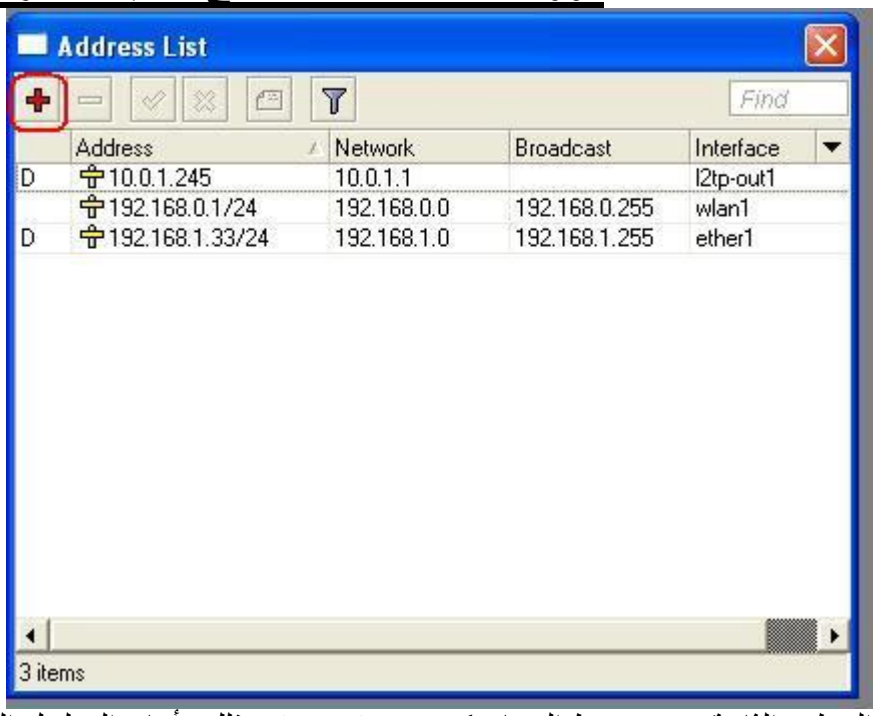
سيكون موضوع درسنا اليوم هو الحلقة الاهم من سلسلة حلقات متصلة في ضبط اعدادات اجهزة شركة مايكروتك لإيصال خدمة الانترنت الى الزبائن ولما كانت هناك الكثير من الوسائل لفعل ذلك وباستخدام المميزات المتعددة التي توفرها الشركة والتي كانت الى حد قريب تفضل العمل على (hotspot) الا ان العمل الحالي يتركز على تقنية الارسال والاستقبال من نقطة الى نقطة او ما يسمى (point to point protocol over Ethernet PPPOE) والتي ستكون محور درسنا اليوم فأبقوا معنا:

خطوات اعداد الاتصال من نوع (PPPOE):

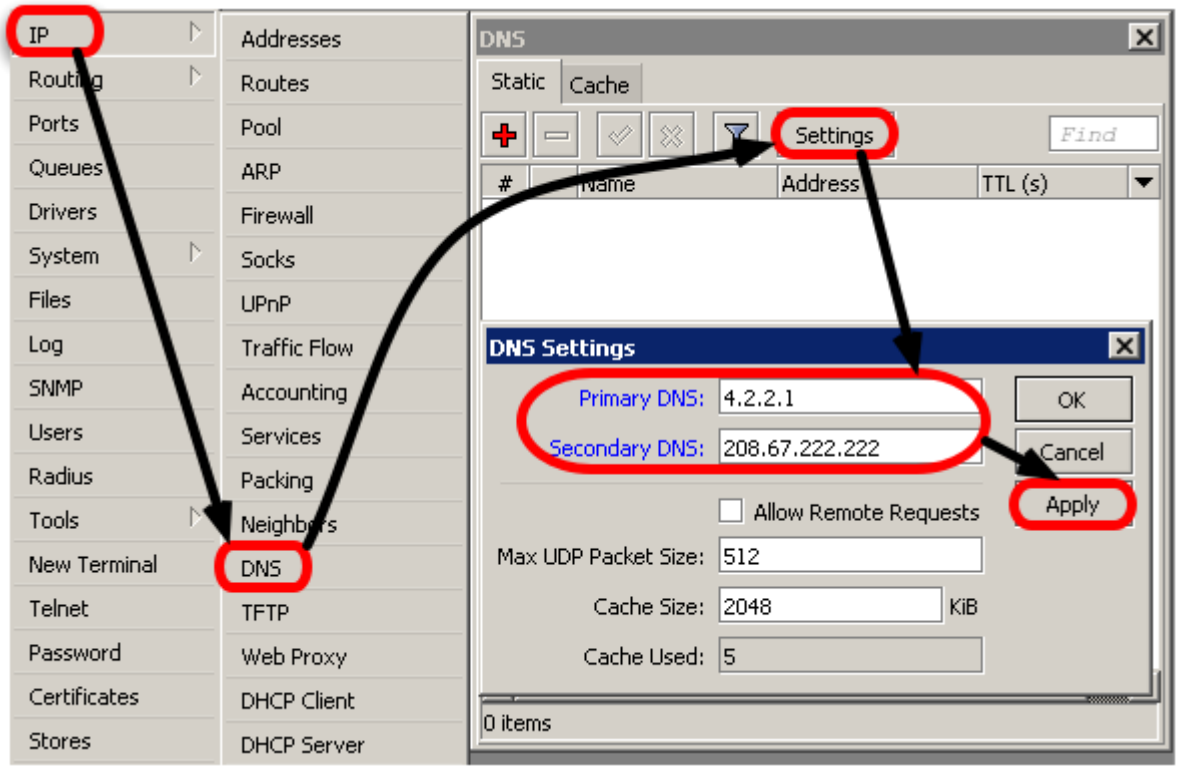
١- ضبط عناوين منفذي اللان والوان (LAN and WAN IP address configuration).
٢- ضبط المايكروتك كخادم نظام اسماء المجال (DNS Server).
٣- ضبط المايكروتك كخادم اسناد العناوين الديناميكية (DHCP server).
٤- خلق حوض عناوين منطقية لأسنادها ديناميكياً (IP pool to be assigned automatically).
٥- ضبط اعدادات خادم ال (PPPOE).
٦- خلق ملفات تنظيمية (profiles) للسيرفر لتستخدم عناوين من الحوض المكون مسبقاً.
٧- ضبط قواعد الجدار الناري وحسب الحاجة.
٨- خلق مسار افتراضي لمرور الانترنت.

والان نبدأ على بركة الله:

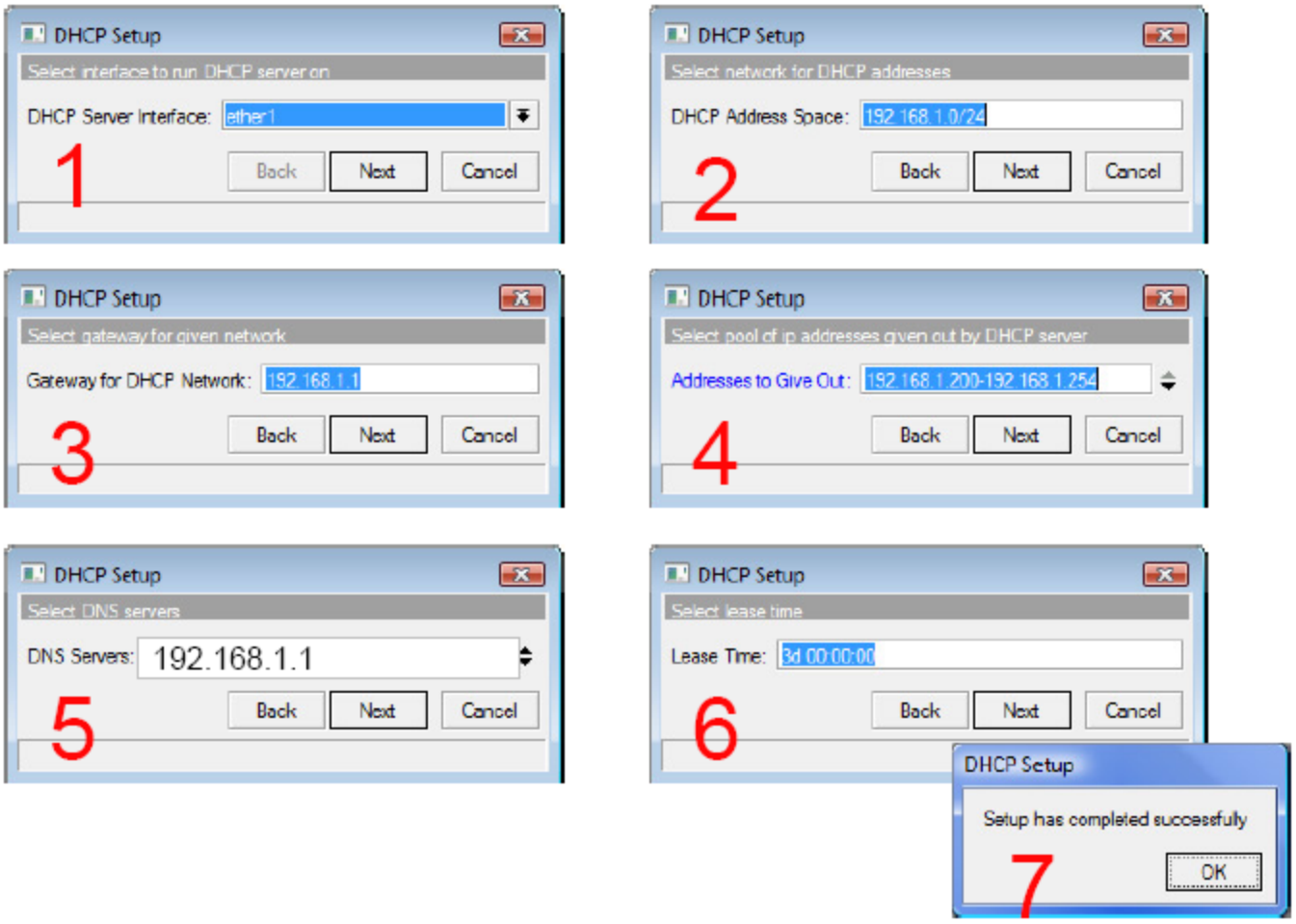
الخطوة الاولى وهي اضافة عناوين للمنافذ السلكية واللاسلكية وحسب نوع الجهاز وسبق ان تم شرحها حيث نذهب الى تبويب (IP) ثم الى (addresses) وننقر على اشارة (+) ونضيف عناوين المنفذ المحلي (للشبكة المحلية LAN) والمنفذ العالمي (للشبكة الخارجية اي لمصدر الانترنت WAN) وكما في الصورة التالية:



الخطوة الثانية وهي ضبط الجهاز كسيرفر (DNS) وذلك بأتباع التسلسل الطبيعي بالذهاب الى تبويب (IP) ثم الى (DNS server) ثم (setting) او اشارة (+) ونضيف العناوين والتي يفضل ان تكون (primary DNS=8.8.8.8) و (secondary DNS=8.8.4.4) او غيرها وحسب الخبرة ولا ننسى وضع علامة صح امام خيار (Allow remote requests) وكما في الصورة التالية:



الخطوة الثالثة هي ضبط اعدادات الجهاز ليكون خادم اسناد عناوين منطقية ديناميكية بشكل اوتوماتيكي (DHCP server) وذلك بالذهاب الى (IP) ثم (DHCP server) ثم (DHCP) ثم (DHCP setup) اتباع الخطوات التالية:



وادناه شرح الخطوات حسب ارقامها:

١- نحدد المنفذ المحلي (LAN port) والذي سيكون هو المكان الذي تسند من خلاله العناوين بشكل اوتوماتيكي للحواسيب في الشبكة.

٢- هنا نحدد عنوان الشبكة التي يعمل ضمنها سيرفر ال (DHCP) ويفترض ان يكون من نفس كلاس الشبكة المحلية التي سبق ان ضبطنا عناوينها في الخطوة الاولى.

٣- نحدد عنوان بوابة الشبكة وهو نفس عنوان المنفذ المحلي (LAN port) وهو نفس عنوان ال (DNS server).

٤- هنا نحدد حوض العناوين اي من اين الى اين نسند العناوين وهنا في الصورة المثال يقول اننا سنقوم بالسماح لسيرفر ال (DHCP) بأسناد عناوين من (192.168.1.200) ولغاية (192.168.1.254) وكما تلاحظون هي نفسها من نفس كلاس الشبكة المحلية ويتم اسناد هذه العناوين بشكل ديناميكي متغير مع الوقت. ملاحظة لا بد منها وهي ان العدد الكلي للعناوين هنا هو ٥٤ عنوان وهو العدد الاقصى من الحواسيب التي يمكن ان تتصل بالشبكة في وقت واحد ولذا ان كنا نعلم ان الشبكة تضم حواسيب اكثر فيجب ان نزيد من حجم حوض العناوين ليضم عدد اكبر.

٥- هنا نضع عنوان ال (DNS server).

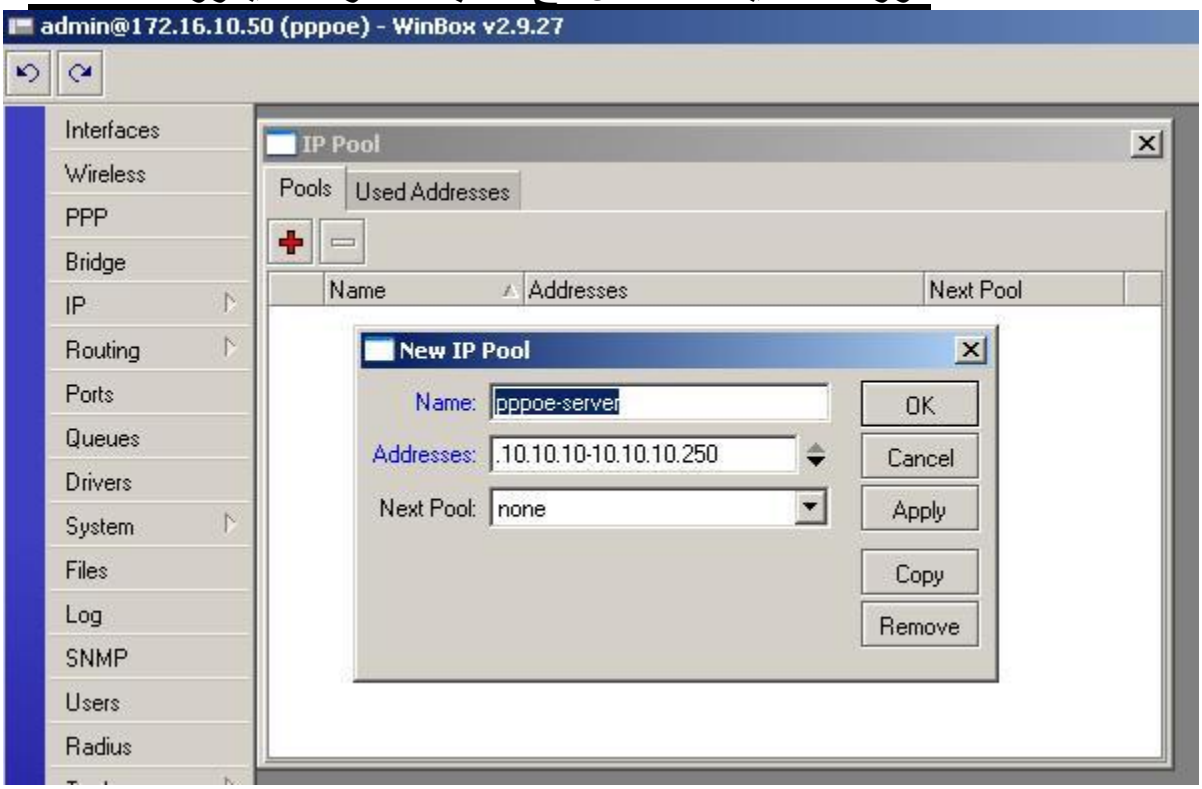
٦- هنا نضع ما يسمى (lease time) وهو زمن الاستئجار او زمن بقاء العنوان الواحد مسنداً الى كل حاسوب قبل تغييره اوتوماتيكياً من قبل سيرفر ال(DHCP) وهنا يفضل ان يكون الزمن قصيراً للشبكة اللاسلكية وطويلاً نسبياً للشبكة السلكية.

٧- وهنا يقول لنا ان الضبط تم بنجاح.

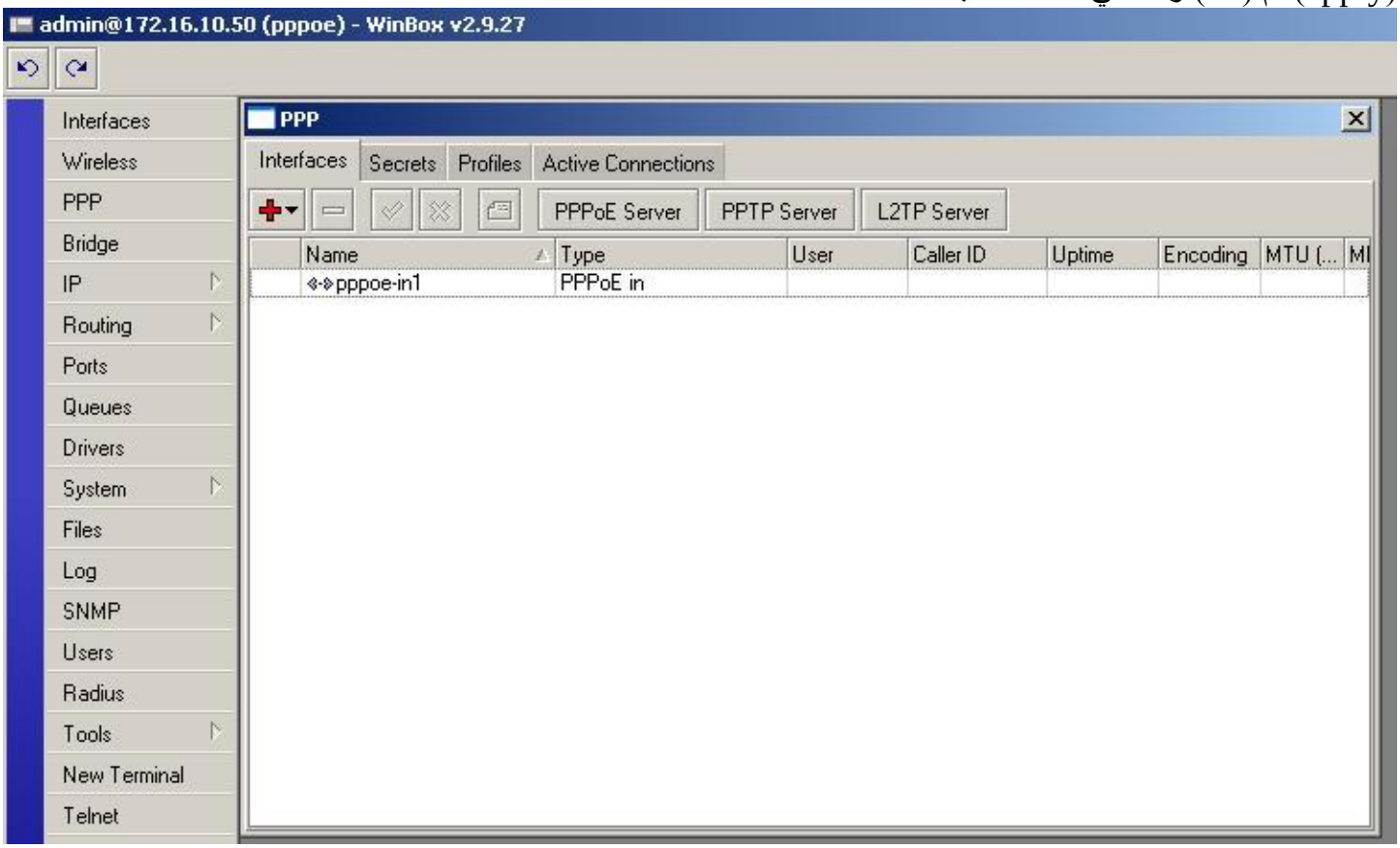
الخطوة الرابعة تمت ضمنياً مع الخطوة السابقة وكما في النقطة ٤ اعلاه.

الان نضبط اعدادات ال (PPPOE server) وكما يلي:

اول خطوة هي بالذهاب الى (IP) ثم (pool) ثم نضغط على علامة (+) ونخلق حوض العناوين الذي سيستخدم من قبل سيرفر ال (PPPOE) ونحدد حيز العناوين وكما في الصورة التالية:

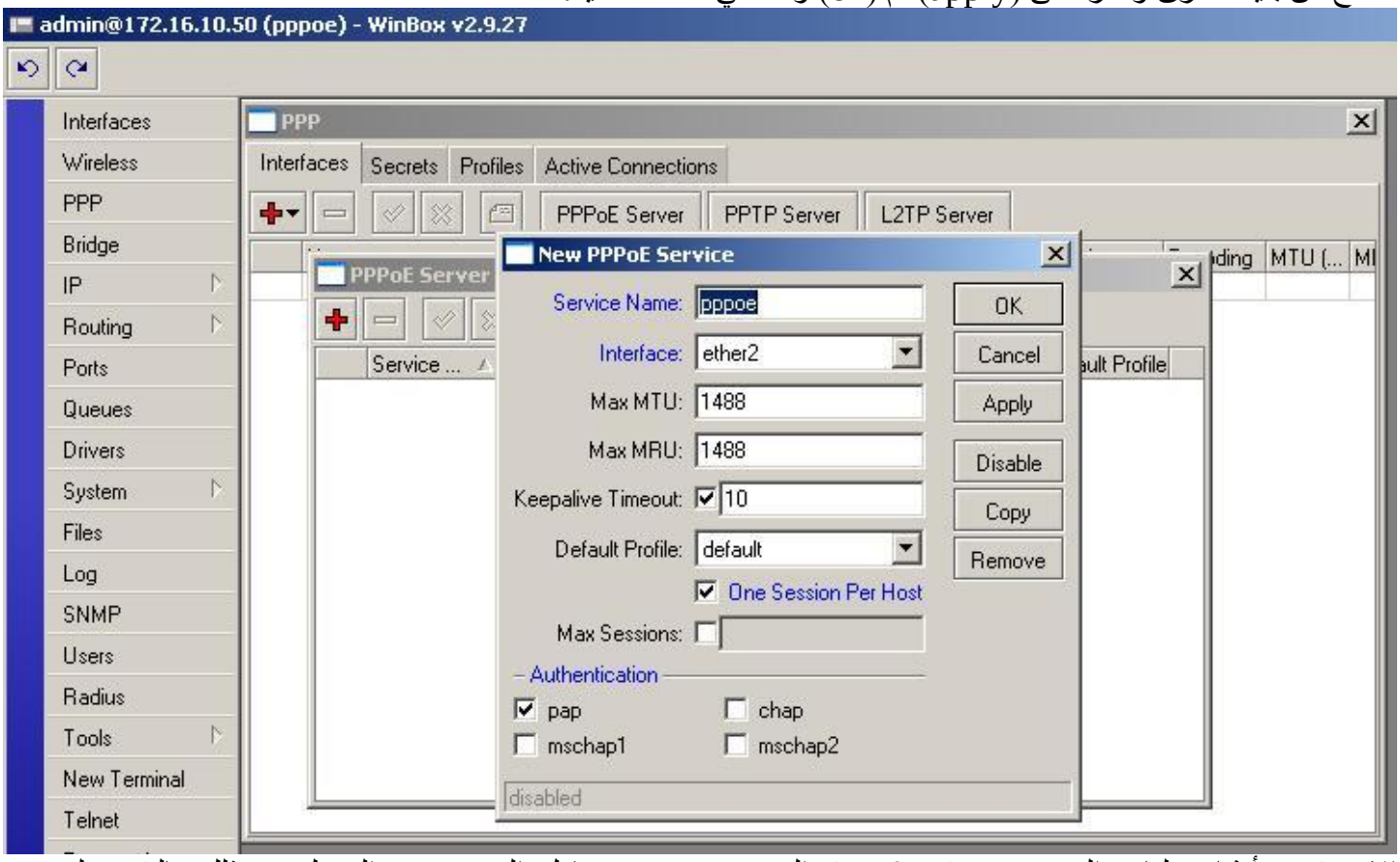


والان نخلق سيرفر ال (PPPOE) بالذهاب الى تبويب (PPP) ثم النقر على اشارة (+) فتظهر نافذة صغيرة فننقر على (apply) ثم (ok) وكما في النافذة التالية:

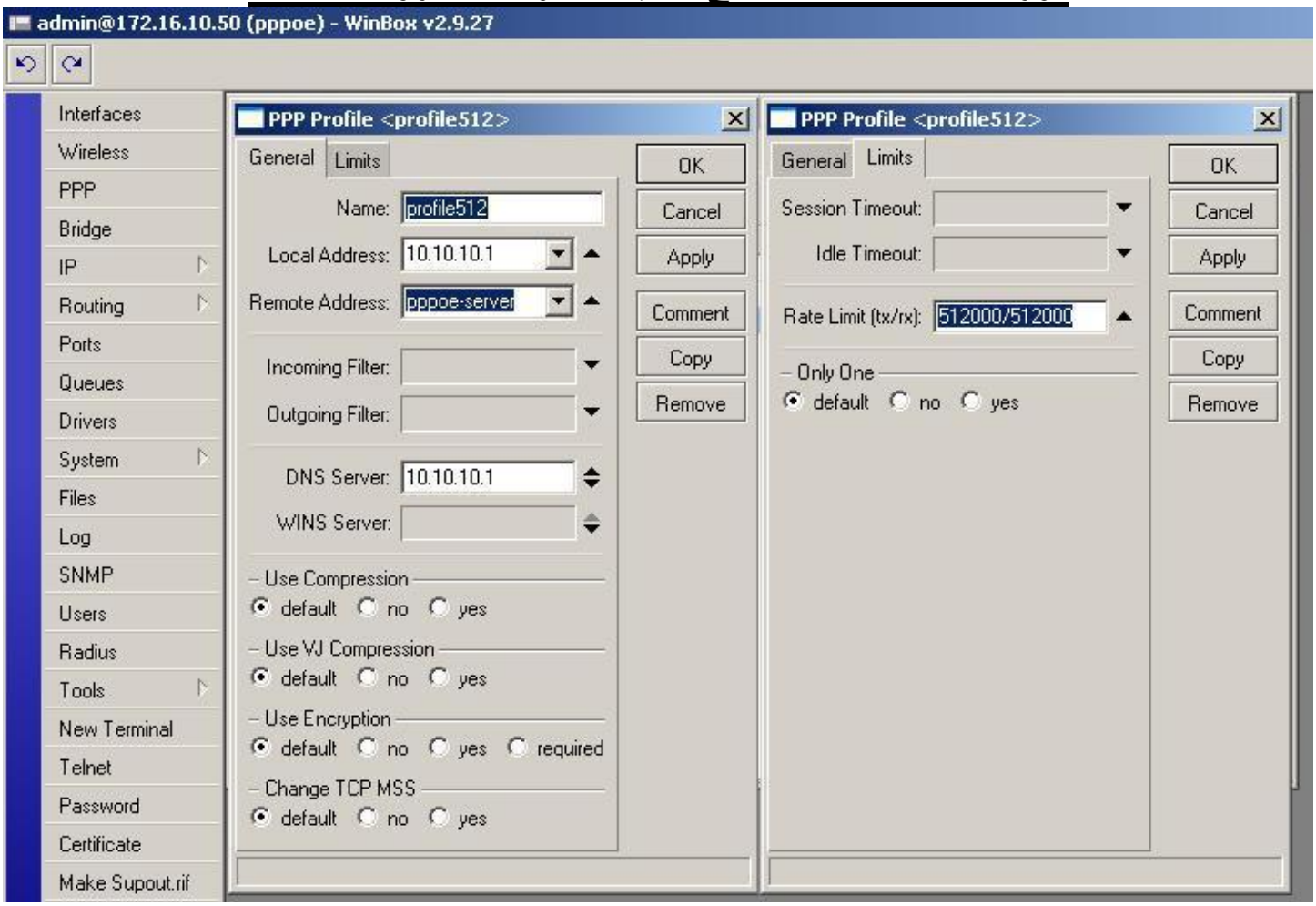


الان سنقوم بخلق السيرفر الرئيسي بالنقر على زر (PPPOE Server) من النافذة اعلاه لتظهر نافذة جديدة ننقر فيها على علامة ال(+) ونحدد اسم السيرفر ليكون مثلاً (PPPOE-server) او اي اسم اخر ثم نختار المنفذ المتصل بالشبكة المحلية (LAN port) وهو في مثالنا هنا (ether2) ولا تقم بتغيير قيم (Maximum Transmission Unit MTU) وتعني قيمة

اكبر وحدة ارسال ولا قيمة (Maximum Receive Unit MRU) وتني قيمة اكبر وحدة استلام ونزيل علامة الصح من امام (keep alive time out) ونضع علامة صح امام (one session per host) ومن اسفل النافذة نجد طرق التخويل ونختار منها (PAP) ويعني بروتوكول التخويل بكلمة المرور (Password Authentication Protocol) ونزيل علامة الصح من بقية الطرق وننقر على (apply) ثم (ok) وكما في النافذة التالية:



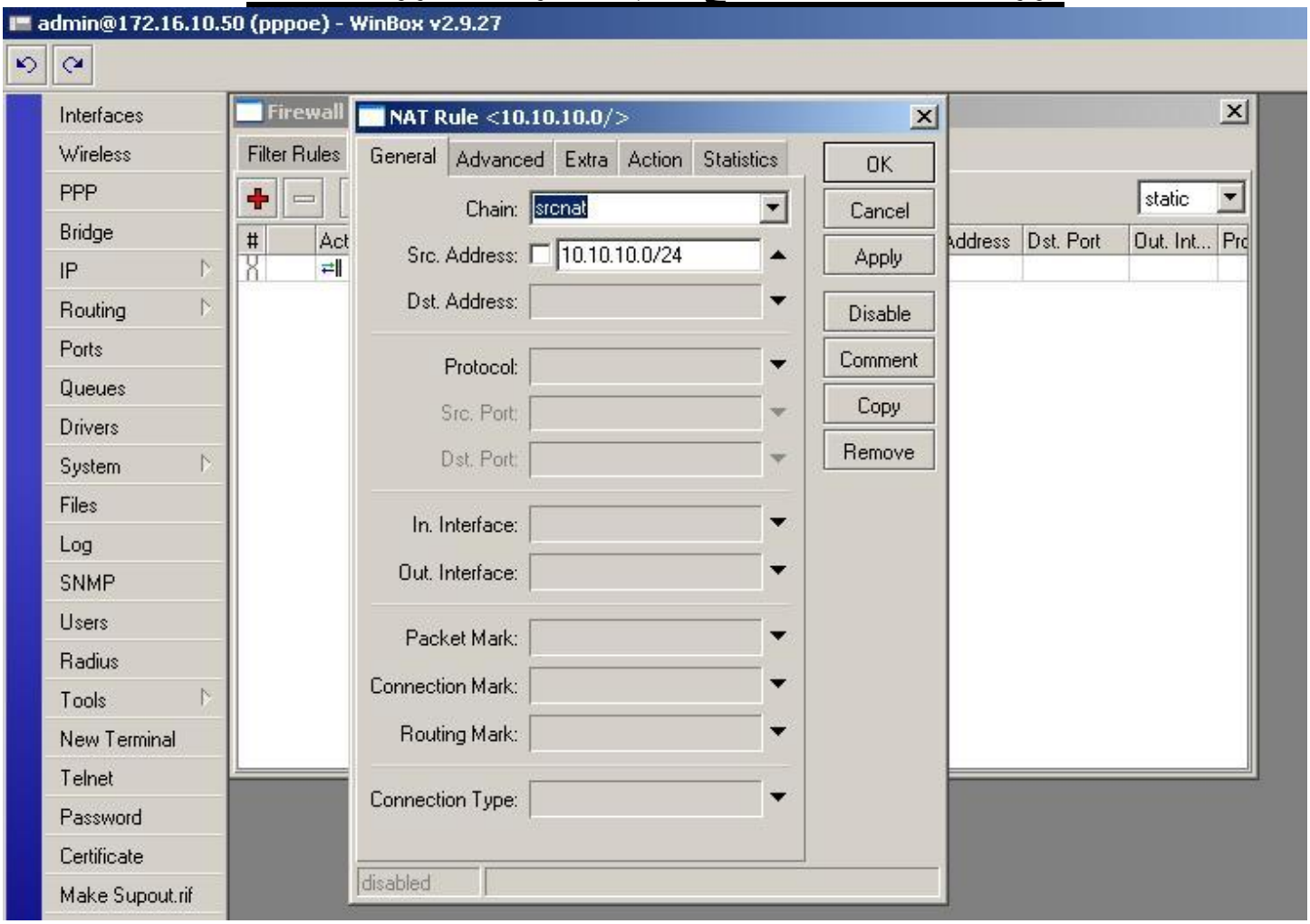
الان نقوم بأنشاء ملفات التخصيص (profiles) التي ستستخدم من قبل المستخدمين المختلفين وذلك بالنقر على زر (profiles) من نافذة ال (PPP) لتظهر نافذة كما في ادناه ونجد فيها نموذجين تلقائيين (two default profiles) ولا نقوم بالتلاعب بها وانما نقوم بخلق واحد جديد بالنقر على علامة الزائد لتظهر نافذة نحدد فيها اسم البروفايل الجديد وليكن اي اسم معبر وهو في المثال (profile512) ويكون العنوان المحلي (local address) هو عنوان المنفذ المحلي للسيرفر او عنوان منفذ ال (LAN) واما عنوان ال (Remote address) فهو لحوض العناوين الذي خلقناه في الخوة الاولى من اعدادات ال (PPPOE) والذي سميناه (PPPOE-server) ونستطيع اختياره بالنقر على السهم المثلث او كتابة الاسم باليد اما عنوان ال (DNS server) فهو نفس العنوان الذي ضبطناه سابقاً ثم ننقر على تبويب (limits) كما في الصورة ادناه ونحدد الحد الاعلى للأرسال والاستقبال (tx/rx) وليكن (512 KB) كما في الصورة وحسب عرض نطاق الشبكة الكلية وعدد المستخدمين:



والان نصل الى مرحلة خلق المستخدمين وذلك بالذهاب الى تبويب (secrets) ثم النقر على علامة الزائد (+) لأضافة مستخدم جديد وفي حقل (name) نضع اسم معرف للمستخدم وهنا سميناه (test) وهو اسم المستخدم في الطرف الاخر من الشبكة واما كلمة المرور (password) فهي في هذه الحالة (test) ايضاً وهما المعلومتان التان يجب اعطائهما للمستخدم ليقوم بخلق اتصال من نوع (broadband) في حاسبته المتصلة بالشبكة سلكياً او لاسلكياً. وفي خانة الخدمة (service) نضع (PPPOE) وهو نوعية الخدمة التي ننوي تقديمها لهذا المستخدم وفي حقل البروفايل نختار البروفايل الذي خلقناه قبل قليل (profile512) ولا نغير اي شيء اخر ثم ننقر على (apply) ثم (ok) وكما في النافذة التالية:

والان انتهينا من اعداد سيرفر ال(PPPOE) ولكن حتى هذه اللحظة لن يستطيع اي مستخدم الوصول الى الانترنت ما لم نضبط اعدادات المسار الافتراضي (default route) و تحويل عناوين الانترنت (network address translation NAT) وكما يلي:

بالنسبة للنات نذهب الى (IP) ثم (Firewall) ثم من تبويب (NAT) نختار اضافة (net firewall rule) بالضغط على علامة الزائد وبالاعدادات التالية: (chain=srcnat , src.address=10.10.10.0/24) ثم نذهب الى تبويب (action) من نفس النافذة ونختار (action=masquerade) لأخفاء اسم الشبكة وعدم القدرة على الارتباط بها الا من قبل الروتروات من نوع مايكروتك في الطرف الاخر وحسب اعداداتنا التي نعرفها لوحدنا لمنع الاختراق ثم (Apply) ثم (ok).

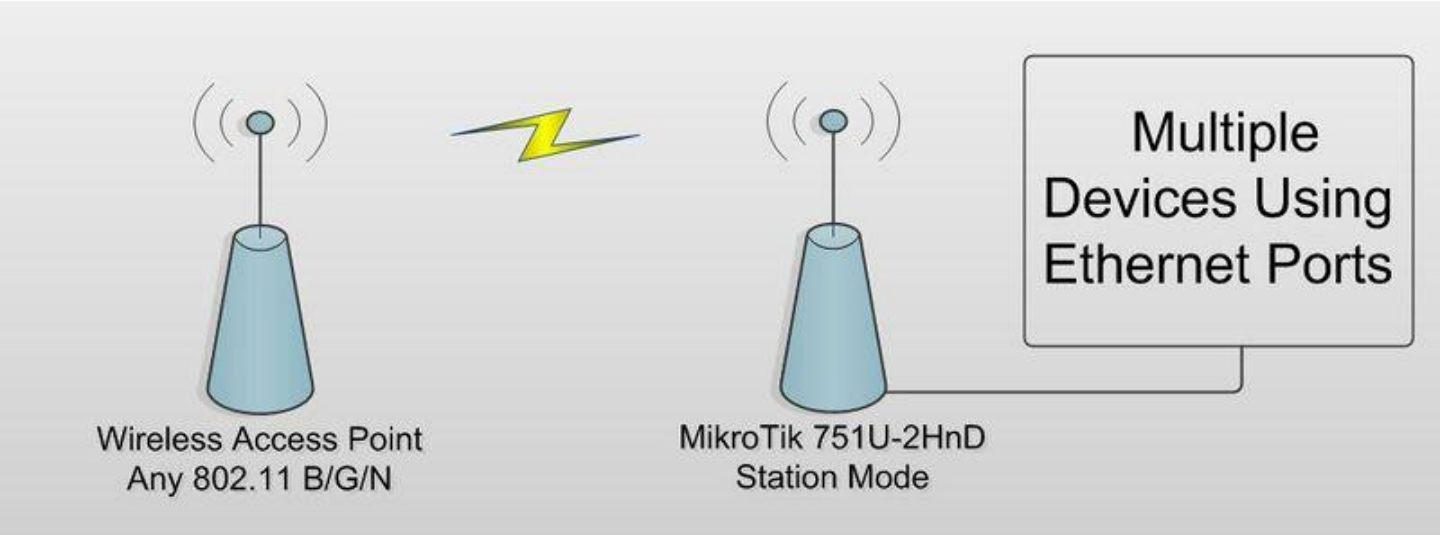


والان ننتقل الى الخطوة الاخيرة وهي ضبط المسار الافتراضي للبيانات (default route) وذلك بالذهاب الى تبويب (IP) ثم (routes) ثم ننقر على علامة الزائد لأضافة مسار ثابت (static route) ويكون عنوان الهدف له (0.0.0.0) ويكون عنوان بوابة الشبكة (gateway) هو نفس عنوان منفذ ال (WAN) وهو نفس المنفذ المتصل بمصدر الانترنت ثم (apply) ثم (ok) وكما في الصورة التالية:

الى هنا نصل الى نهاية درسنا على امل اللقاء بكم في دروس اخرى بعون الله تعالى

الجزء السابع من دورة المايكروتك (PPPOE setting- client side)

في الدرس السابق تطرقنا الى اعدادات جهة السيرفر من المايكروتك في حالة العمل بخدمة ال (PPPOE) اي في الجانب الايسر من السيناريو التالي:



والان في الجانب الاخر من الشبكة وتحديداً في جهة المستخدم لابد ايضاً من نصب جهاز مايكروتك يعمل لأستلام البث للأنترنت وايصاله الى المستخدم وهو المتمثل في الجهة اليمنى من الصورة اعلاه وفي هذا الدرس سنركز على هذا الجانب وهو كيفية الارتباط بشبكة لاسلكية متاحة:

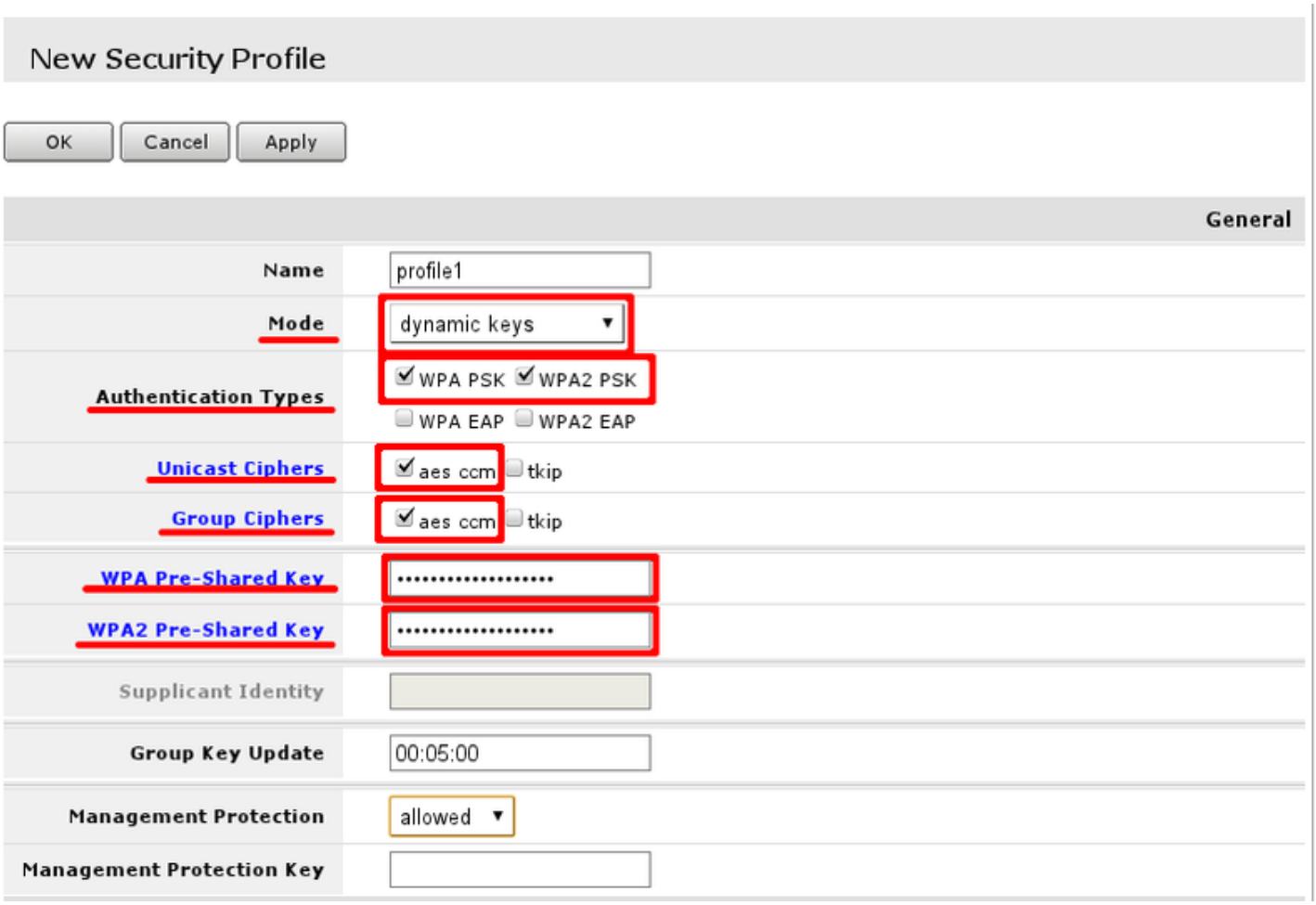
المتطلبات:

جهاز مايكروتك يدعم منفذ سلكي ولاسلكي حيث يكون المنفذ السلكي هو المنفذ للشبكة المحلية للمستخدم والمنفذ اللاسلكي هو الواسطة الى الشبكة اللاسلكية.

اسم مستخدم وكلمة مرور يقوم صاحب الشبكة بمنحها الى المستخدم.

الخطوة الاولى: انشاء اعدادات الامن

ننقر على تبويب (Wireless) في برنامج ال(Winbox) في طرف المستخدم والذي نرتبط به بنفس الطرق المشرروحة في الدروس السابقة ثم نذهب الى (Security profiles) ثم ننقر على اشارة الزائد (+) لأضافة ملف امن جديد لتظهر النافذة التالية:

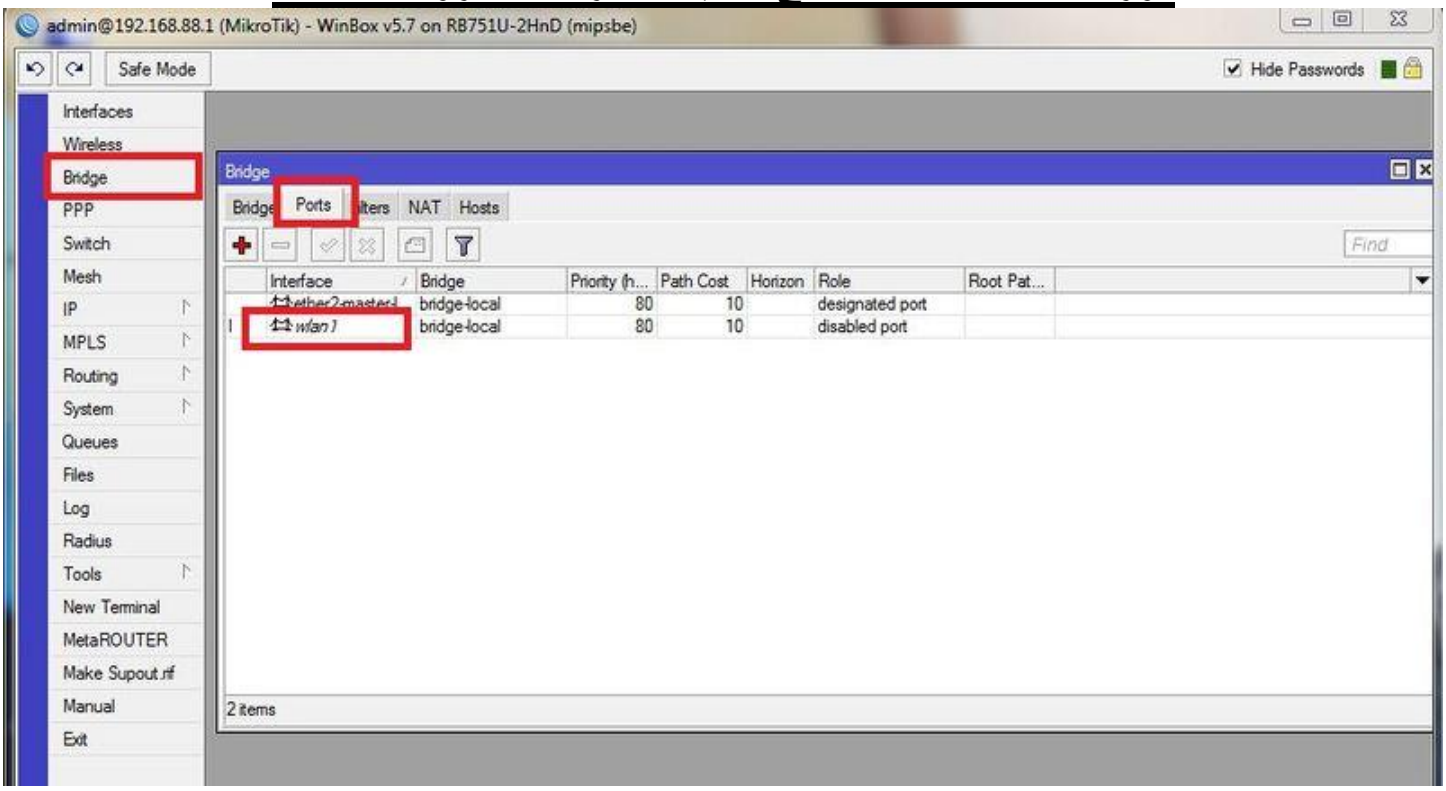


حيث ان (mode) هو نوع الامن ويفضل اختيار المفاتيح الديناميكية.

واما (Authentication types) فهو انواع تخويل الدخول وهناك الكثير من الانواع الان ان افضلها هو ما تم اختياره في الصورة ويتضمن نوعين من كلمات المرور.

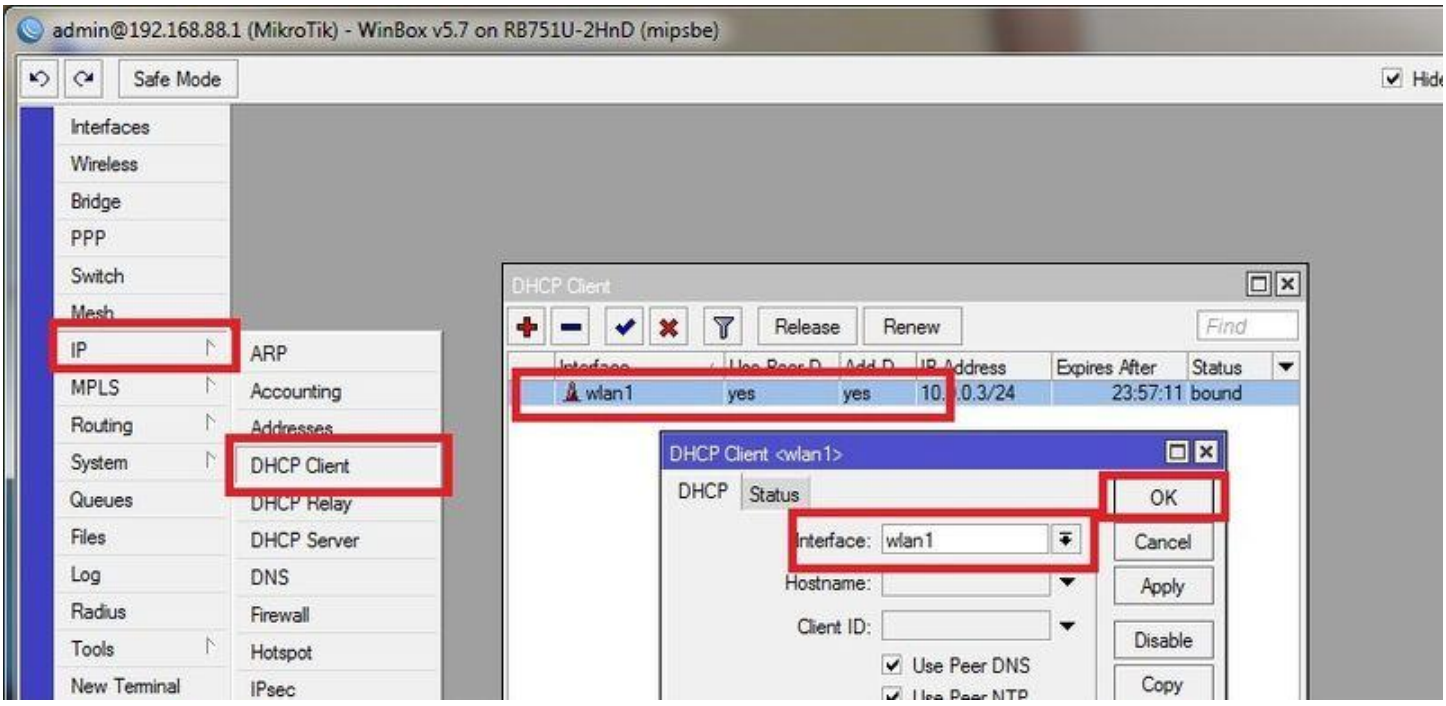
اما ال (unicast) و (group) فهي نوعية التشفير ويفضل اختيار (aes ccm) كما موضح واخيراً فأن (WPA) و (WPA2) فهي كلمات مرور الشبكة المشتركة بين الخادم والزبون.

الخطوة الثانية: حذف ال (wan1 bridge)



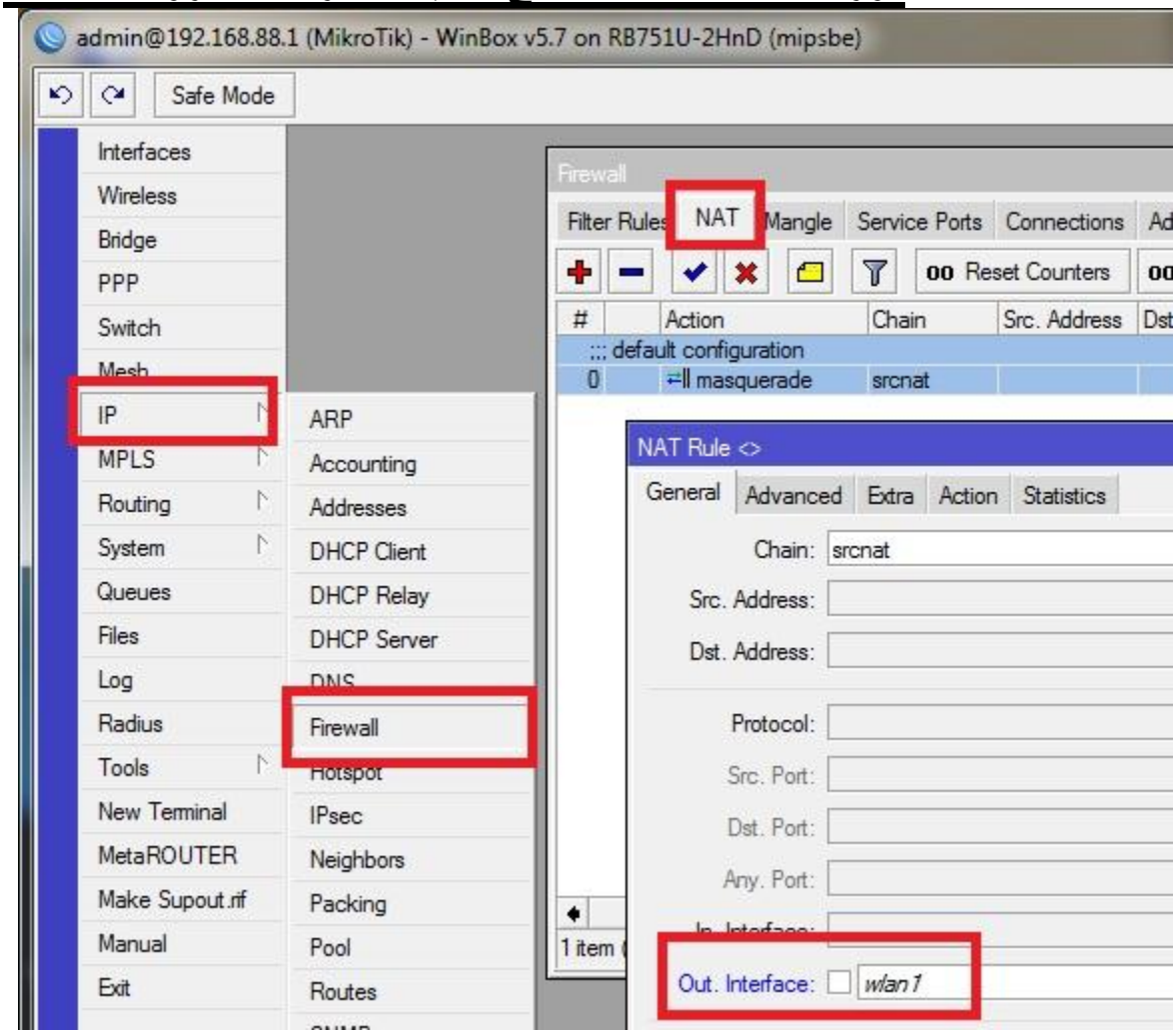
ننقر على تبويب (bridge) ثم (ports) ثم ننقر نقرة يمين على منفذ (wan1) ونختار (remove)

الخطوة الثالثة: تشغيل خدمة (DHCP client) لل (Wan1)



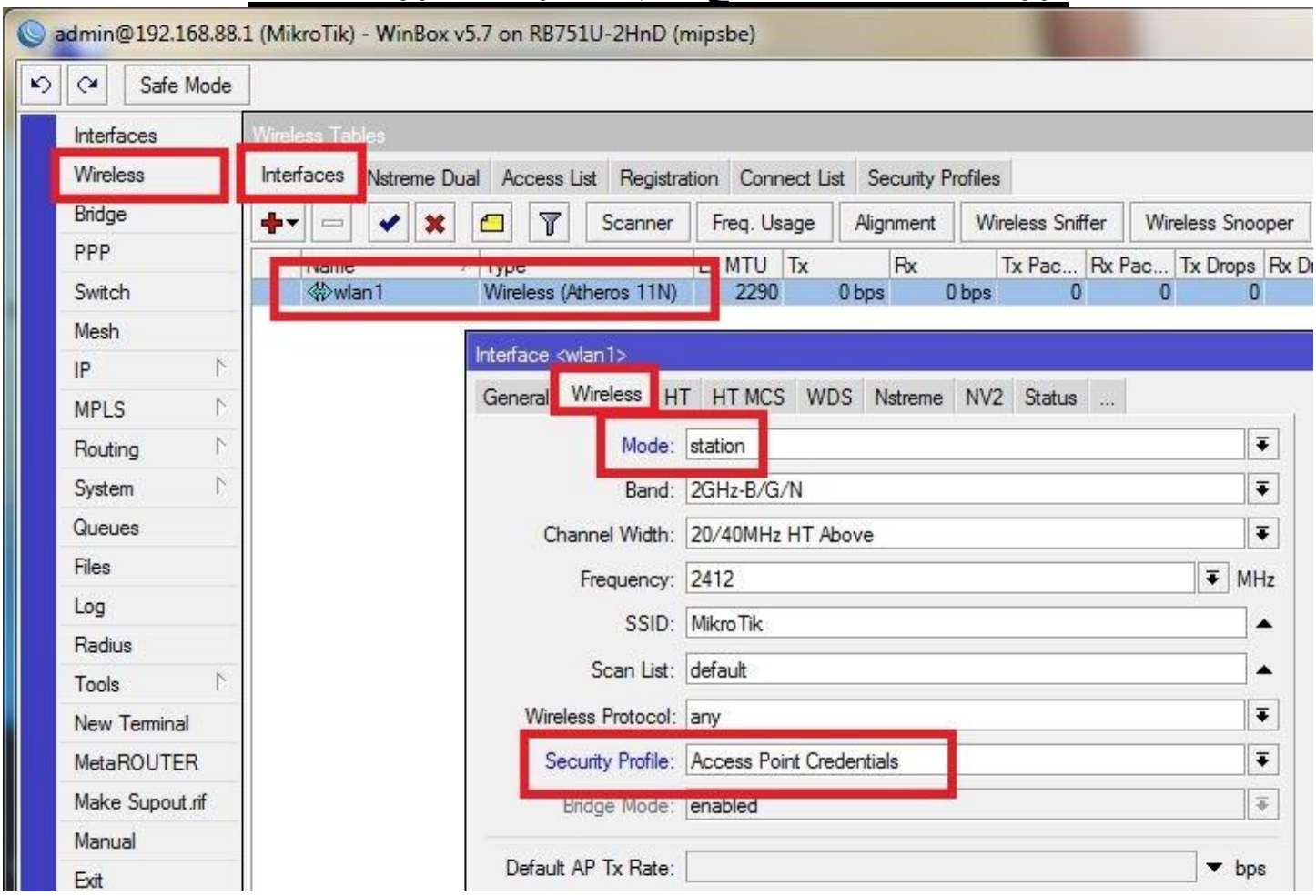
وكما في الصورة ننقر على تبويب (IP) ثم (DHCP client) ثم ننقر نقرتين على (Wan1) ونضيفه الى (interface) ثم (ok).

الخطوة الرابعة: تغيير منفذ خروج ال (NAT)

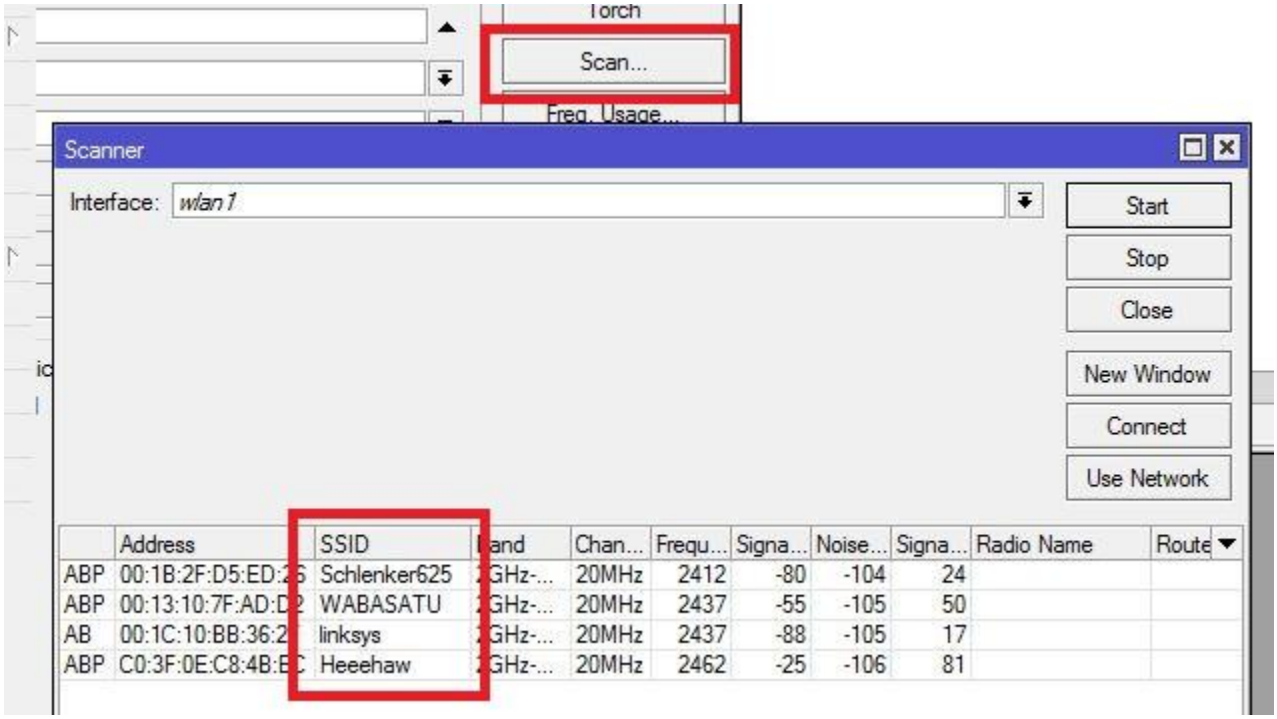


الشرح واضح من الصورة وحسب تسلسل الخطوات من اليسار الى اليمين.

الخطوة الخامسة: تغيير طور عمل المايكروتك للزبون الى (Station):



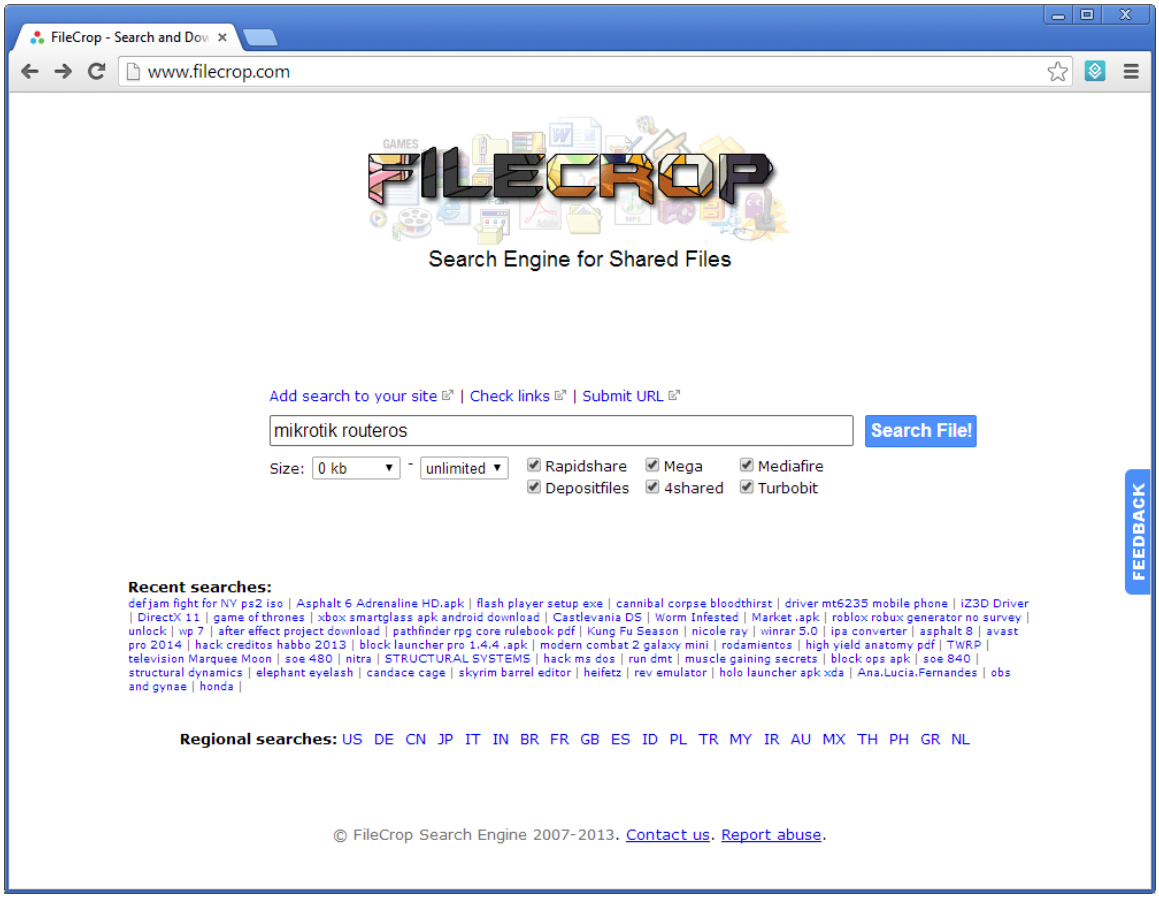
الخطوة الاخيرة: والان وبعد ضبط الاعدادات اعلاه نبدأ المرحلة الاخيرة وهي البحث (scan) من نفس النافذة اعلاه في الجانب الايمن نجد زر (scan) لتظهر لنا الشبكات المتاحة ونختار منها شبكتنا التي ضبطنا اعداداتها في جهة السيرفر وكما يلي:



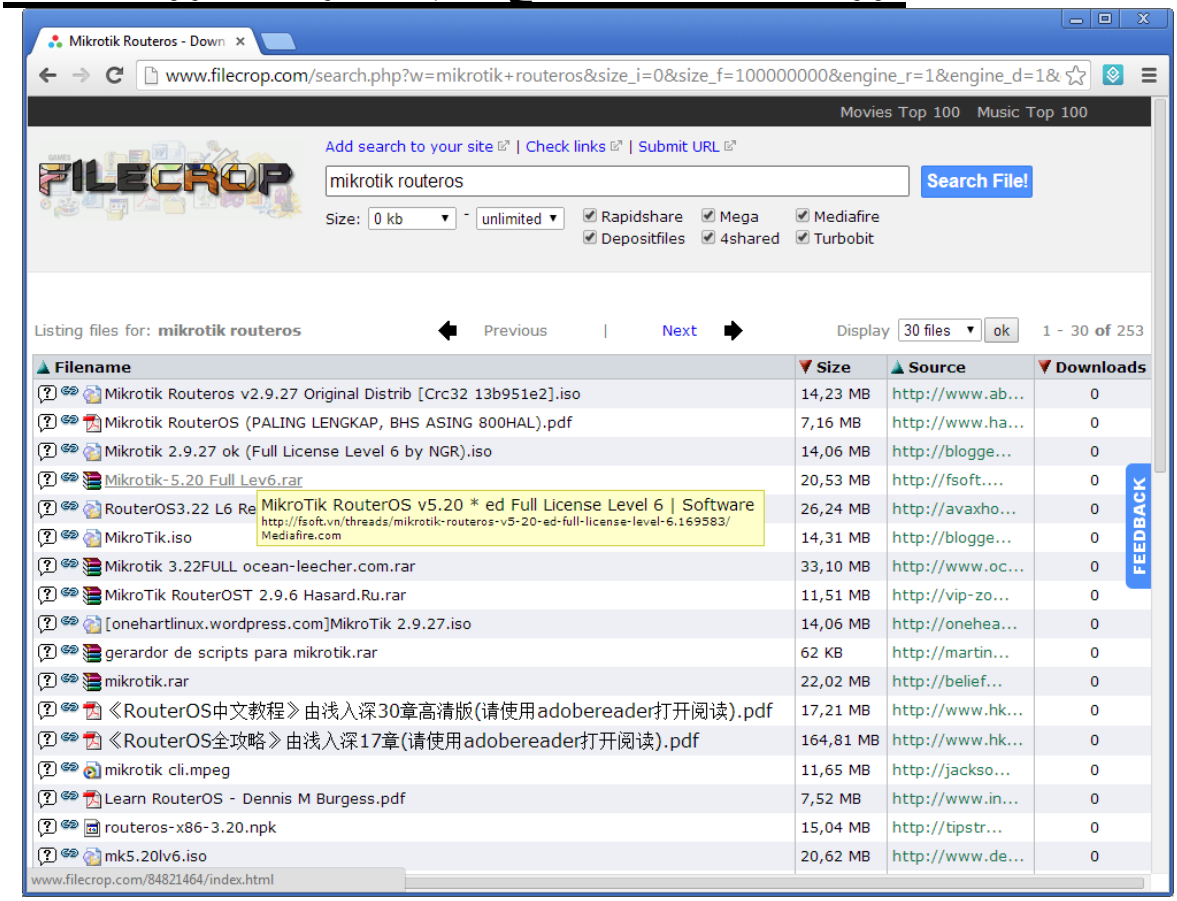
وبعد البحث واختيار الشبكة المطلوبة ننقر على (ok) وهنا يفترض ان الجهازين في جهة المصدر (Server) وجهة المستخدمين (clients) قد اتصلا وبالنسبة للجهاز في طرف المستخدم فهو يحتوي منفذ (Ethernet) او منفذ وايرلس اخر ينقل من خلاله اشارته الى سويتش سلكي او نقطة وصول (Access Point) لاسلكية للتوزيع على المستخدمين.
ولجعل المستخدمين يستطيعون الاتصال نقوم بعمل اتصال من نوع (broad band) في كل حاسبة مطلوب جعلها تستفيد من خدمة الانترنت وبأستخدام اسم المستخدم (user name) وكلمة المرور (password) التي قمنا بخلقها في جهة السيرفر في الدرس السابق والتي كانت كمثال (test, test)

الدرس الثامن من دورة المايكروتك

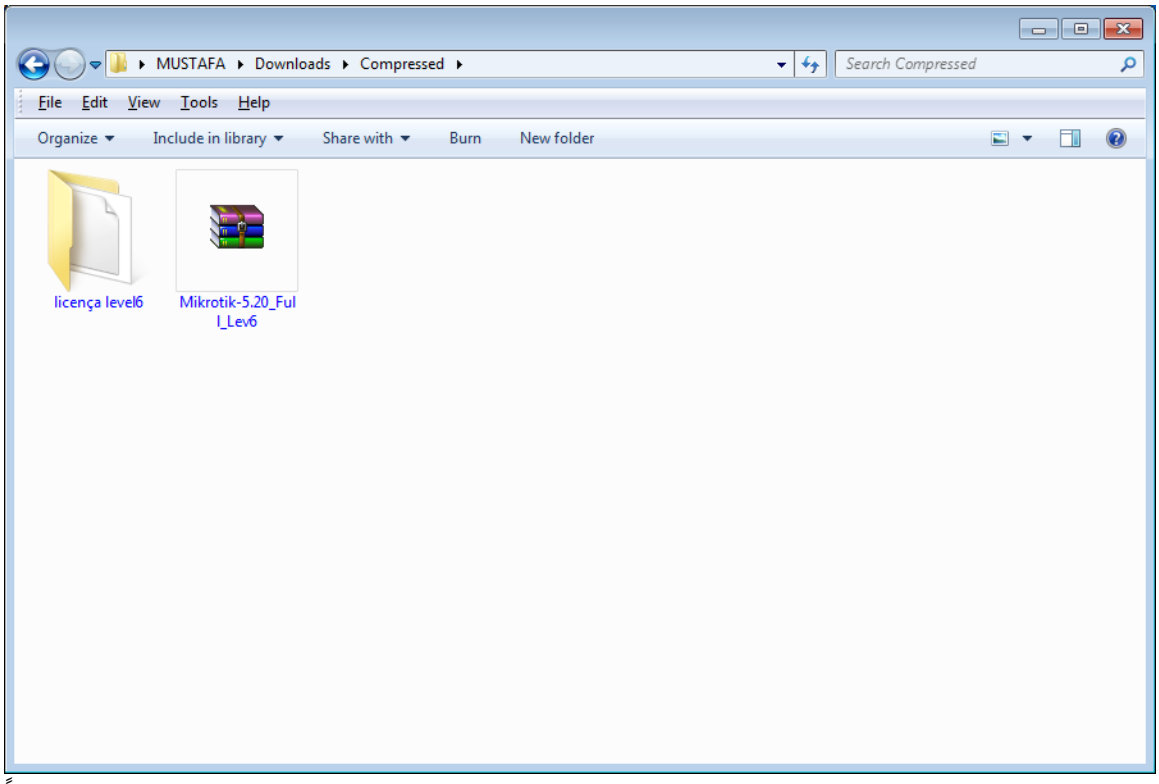
رغم تأخر الامر قليلاً وبناءاً على طلب بعض الاخوة من متابعي هذه السلسلة من الدروس وبسبب صعوبة شراء اجهزة مايكروتك حقيقية على البعض واكتفائهم بالعمل على نسخة افتراضية من نظام تشغيل المايكروتك (RouterOS) سنقوم بشرح تنزيل نسخة النظام على الحاسوب وتنصيبه على برنامج الماكنة الافتراضية (VMware Workstation) ليتسنى للجميع الاستفادة منه من لديهم جهاز مايكروتك حقيقي ومن يعملون في مختبر افتراضي ونبدأ على بركة الله:
يمكننا الذهاب الى الموقع الرسمي للشركة (www.mikrotik.com) والنقر على تبويب (downloads) لتنزيل نسخة من النظام ولكنه لن يكون مجاني وحتى النسخة التي يتم تنزيلها ستحتوي الكثير من المشاكل حتى يتم شرائها او كسر حمايتها وبدلاً من ذلك يمكن الذهاب الى الموقع الرهيب (www.filecrop.com) والذي له الواجهة التالية:



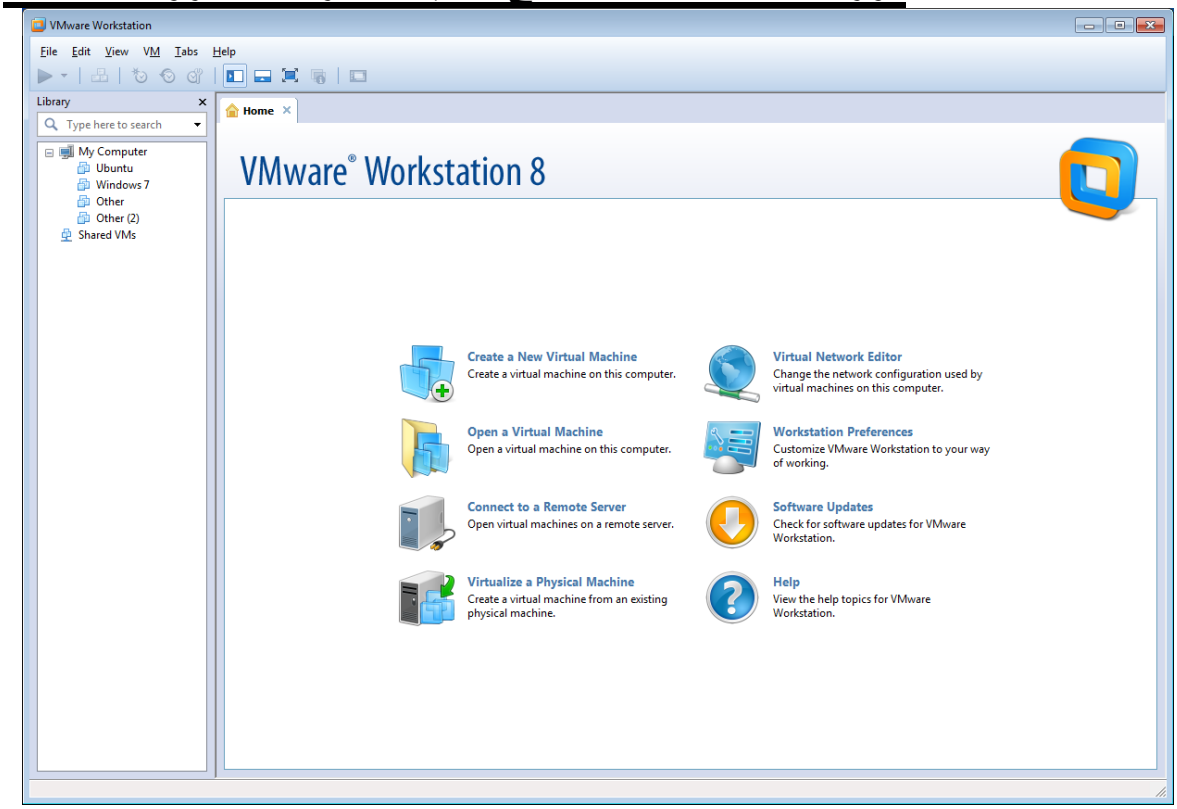
فنقوم بكتابة كلمة البحث كما في النافذة اعلاه لتظهر لنا النتائج التالية:



فنختار منها الخيار الرابع والذي يحتوي نسخة كاملة للنظام مع رخصة العمل عليه وبعد اكتمال تنزيلها نقوم بفك الضغط ليظهر لدينا ملفين كما في النافذة التالية:

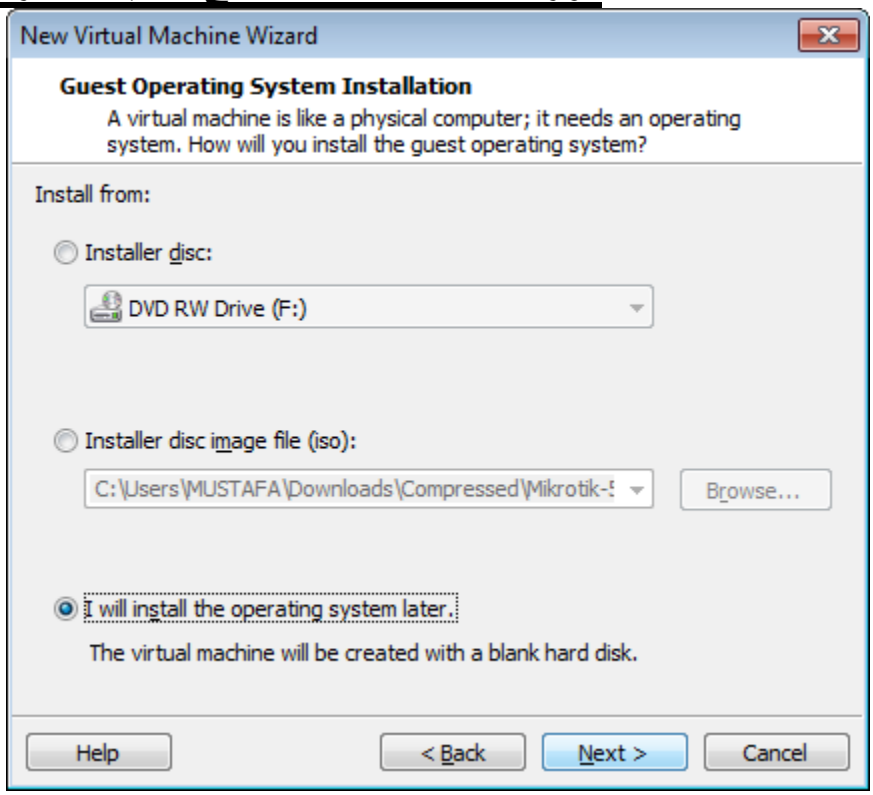


والان نذهب الى برنامج ال (VMware Workstation) والذي يفترض اننا قمنا بتنصيبه مسبقاً وعند فتحه تظهر النافذة التالية:

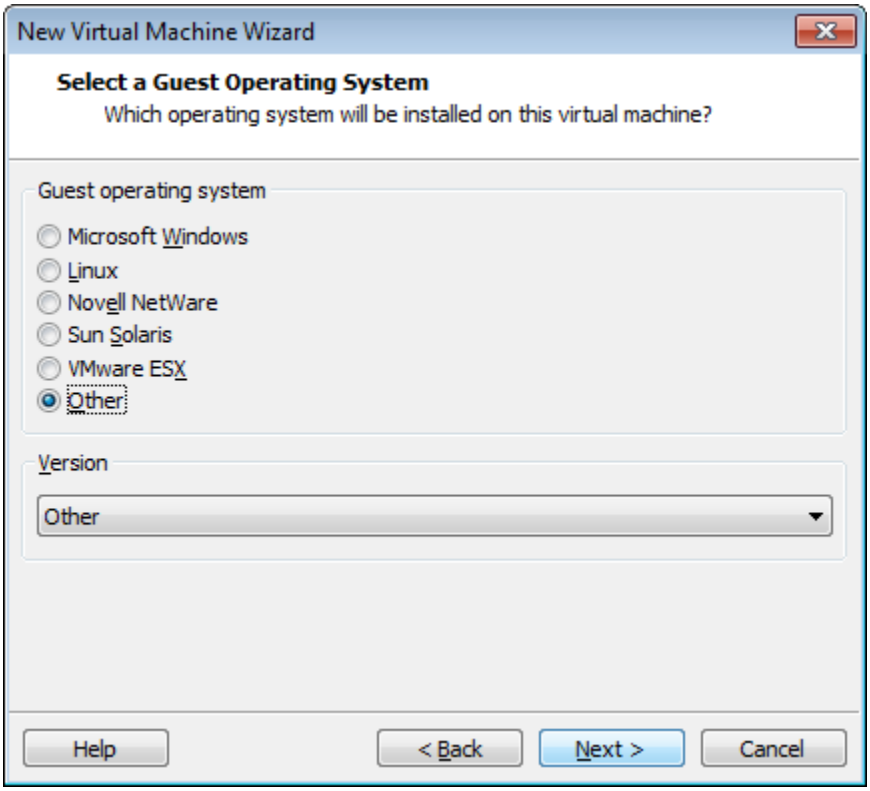


والان نقوم بالنقر على (create new virtual machine) لتظهر النافذة التالية:

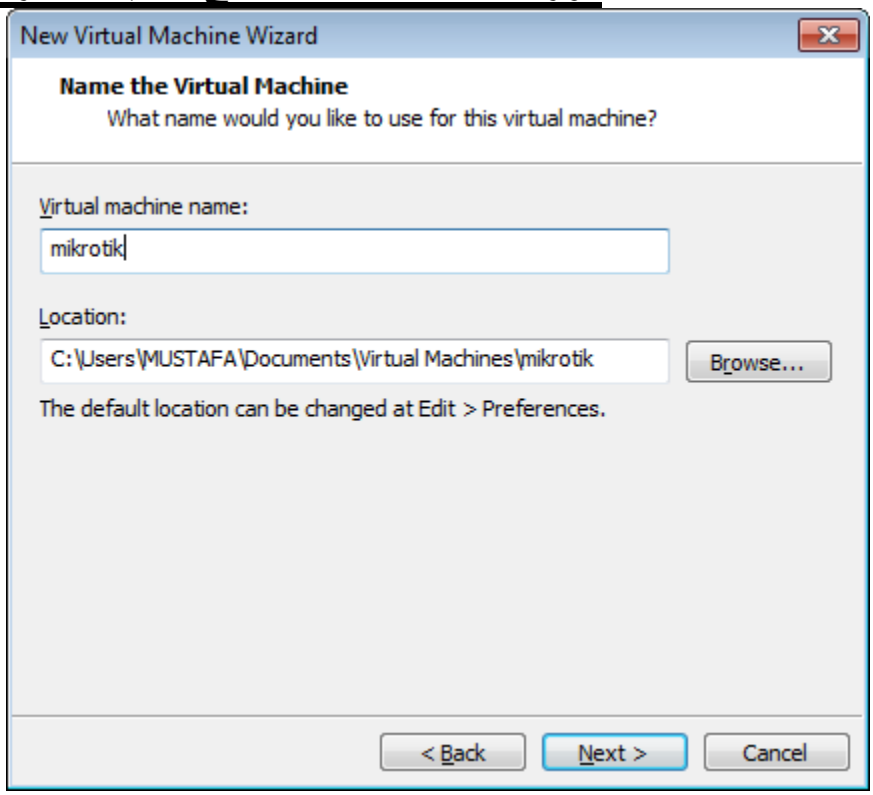
نختار (typical) وننقر على (next) لتظهر النافذة التالية:



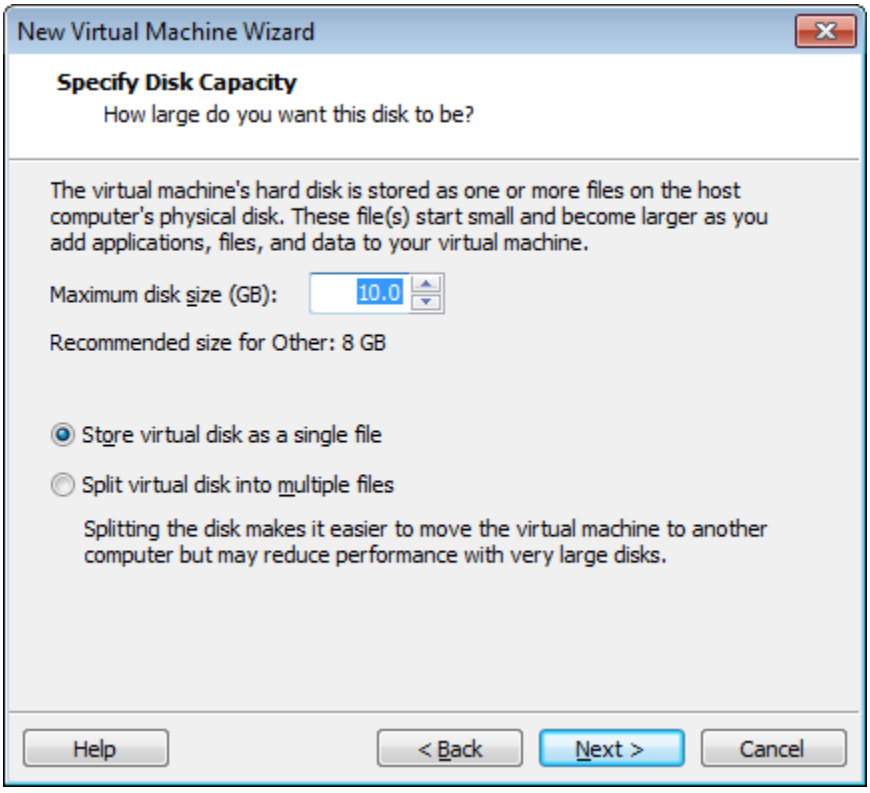
نقوم بأختيار تنصيب نظام التشغيل لاحقاً وهو الخيار الثالث كما في النافذة اعلاه ثم ننقر على (next) لتظهر النافذة التالية:



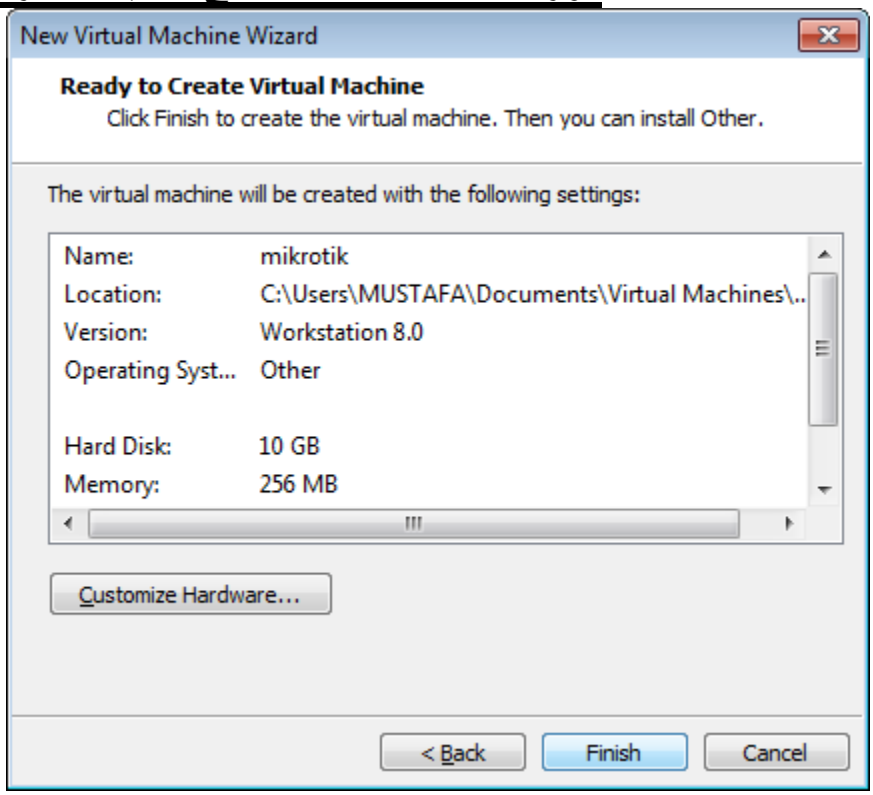
نختار (other) والنسخة (version) ايضاً (other) ثم ننقر على (next) لتظهر النافذة التالية:



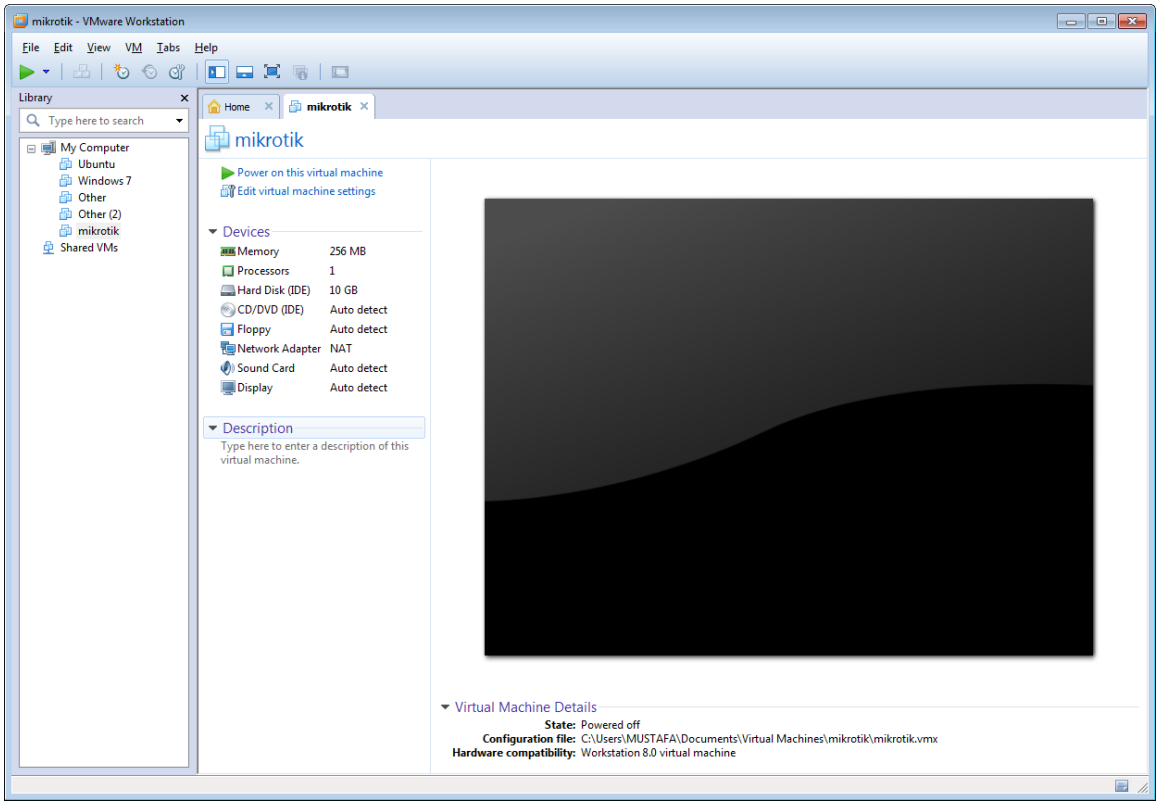
نسمي الماكنة الافتراضية بأسم (mikrotik) او اي اسم اخر ونحدد مكان خزنها وليكن كما في المسار المحدد في (location) او غيره وننقر على (next) لتظهر النافذة التالية:



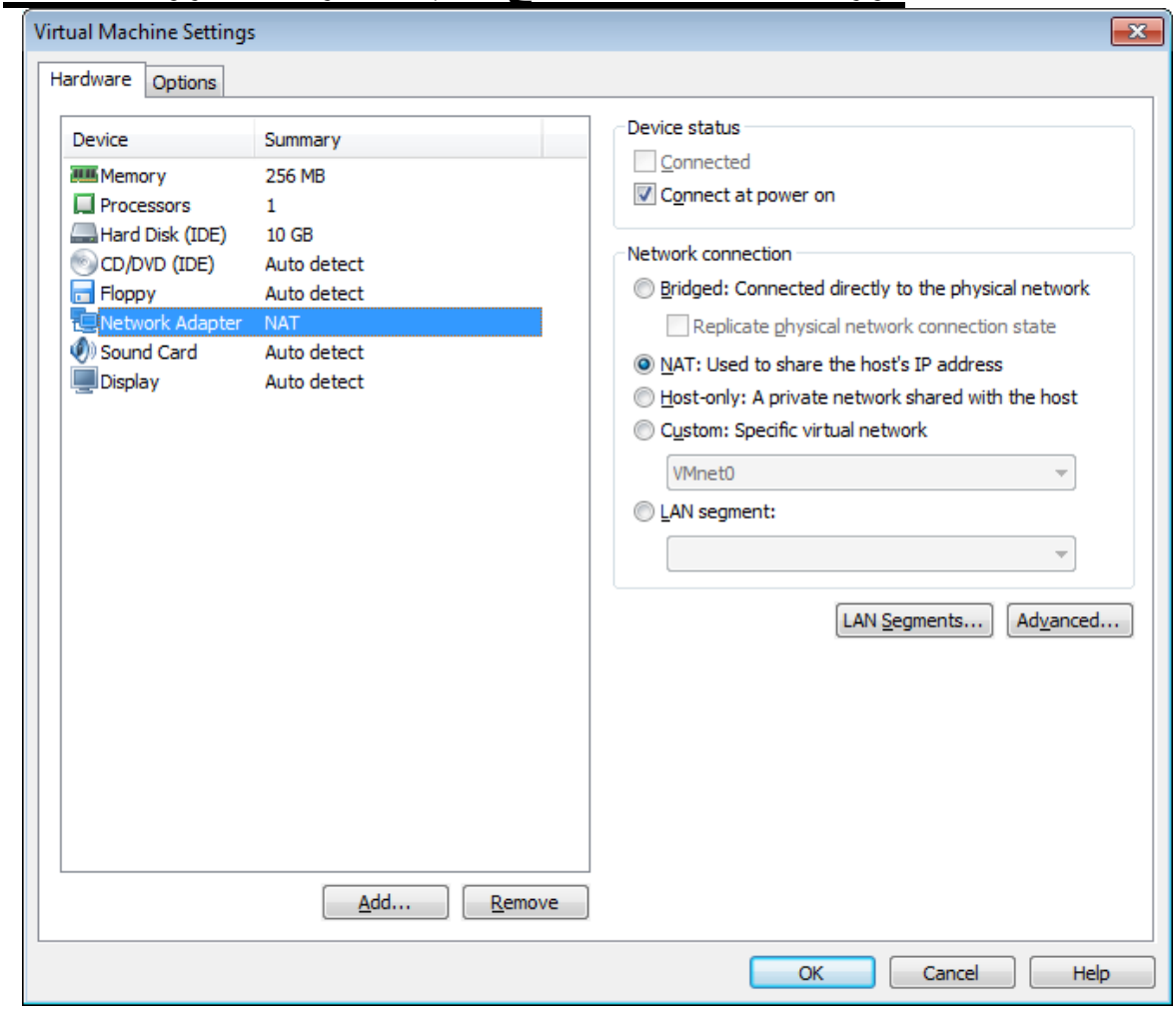
نحدد حجم الهارد المخصص لنظامنا او لجهازنا الافتراضي ويفضل ان لا يقل عن ١٠ غيغابايت ونختار خزن القرص الافتراضي كملف واحد (store virtual disk as a single file) كما في النافذة اعلاه وننقر على (next) لتظهر النافذة التالية:



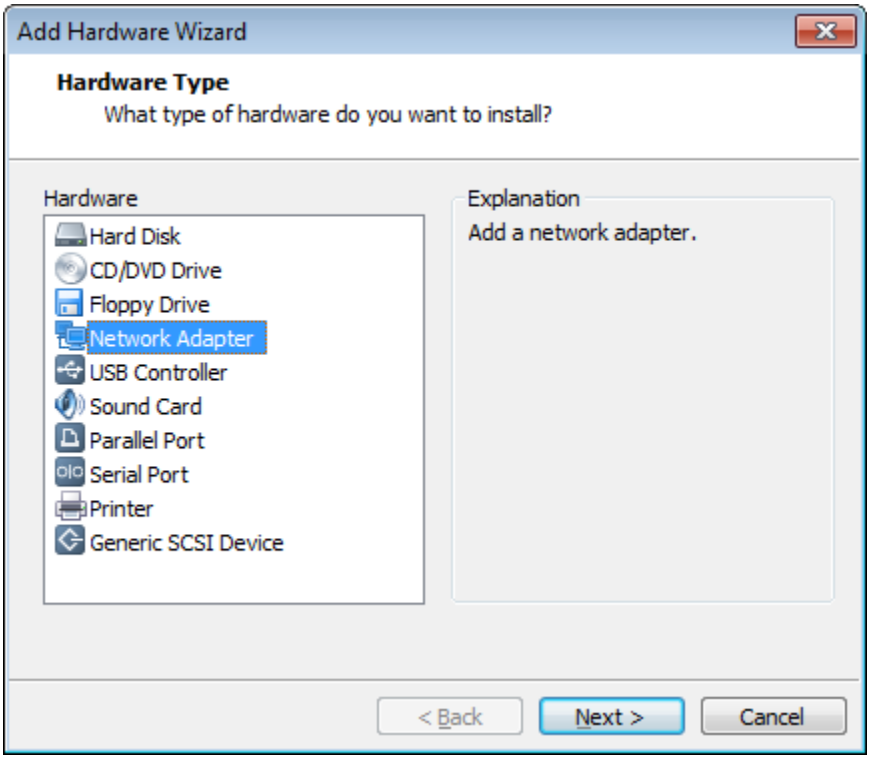
ننقر على (finish) لتصبح واجهة البرنامج كما في الصورة التالية:



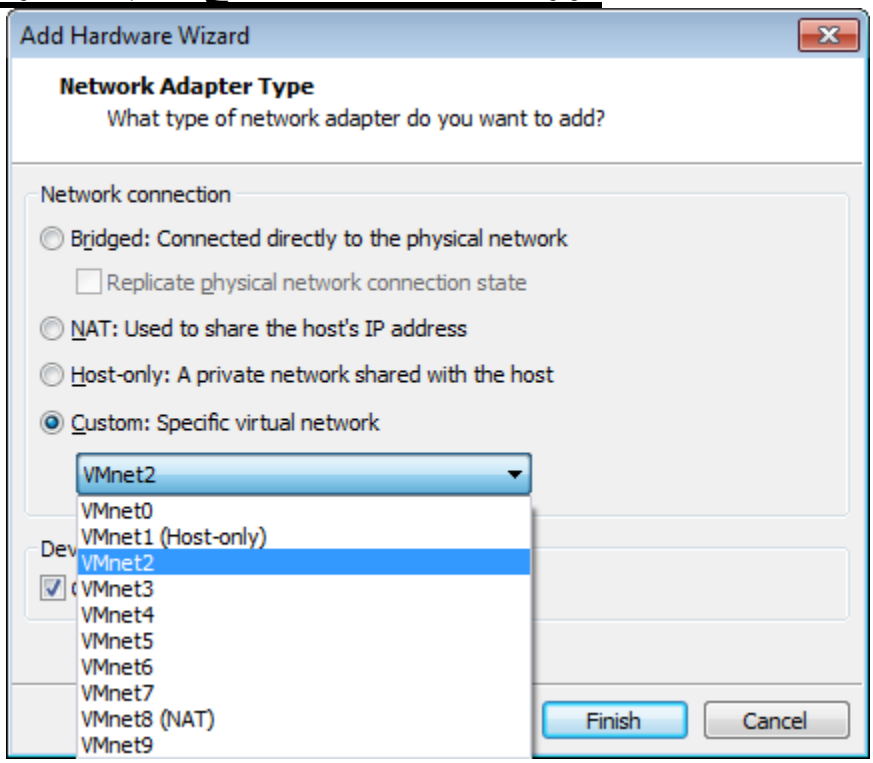
الان وقبل تنصيب نظام التشغيل نقوم بأضافة كرت شبكة اخر (ثاني) الى الجهاز حتى نحوله الى روتر مستقبلاً بحيث يصبح احد الكروت (LAN card) والاخر (WAN card) وذلك بالنقر على (network adapter) في منتصف النافذة تقريباً نقرة مزدوجة لتظهر النافذة التالية:



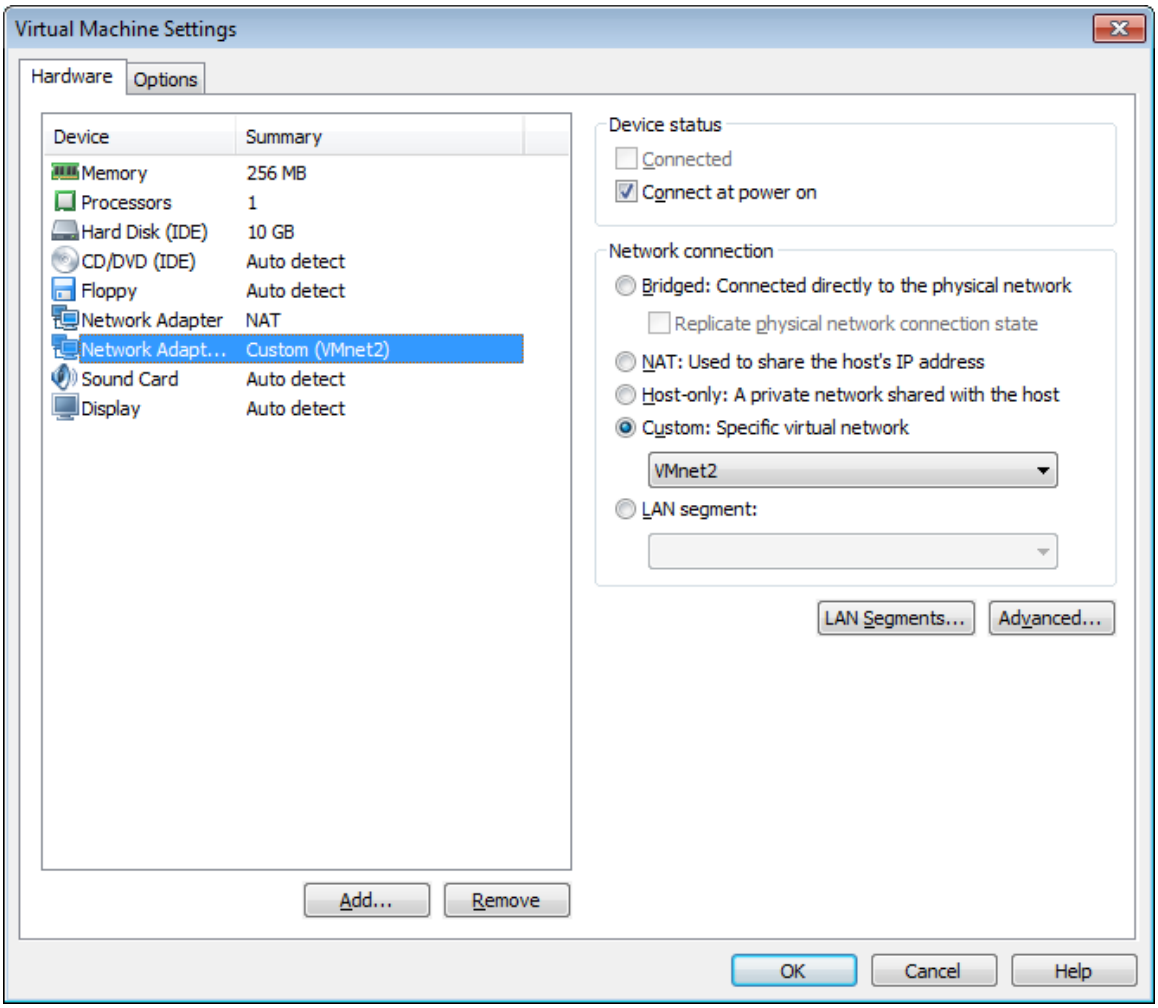
ننقر على (add) لتظهر النافذة التالية:



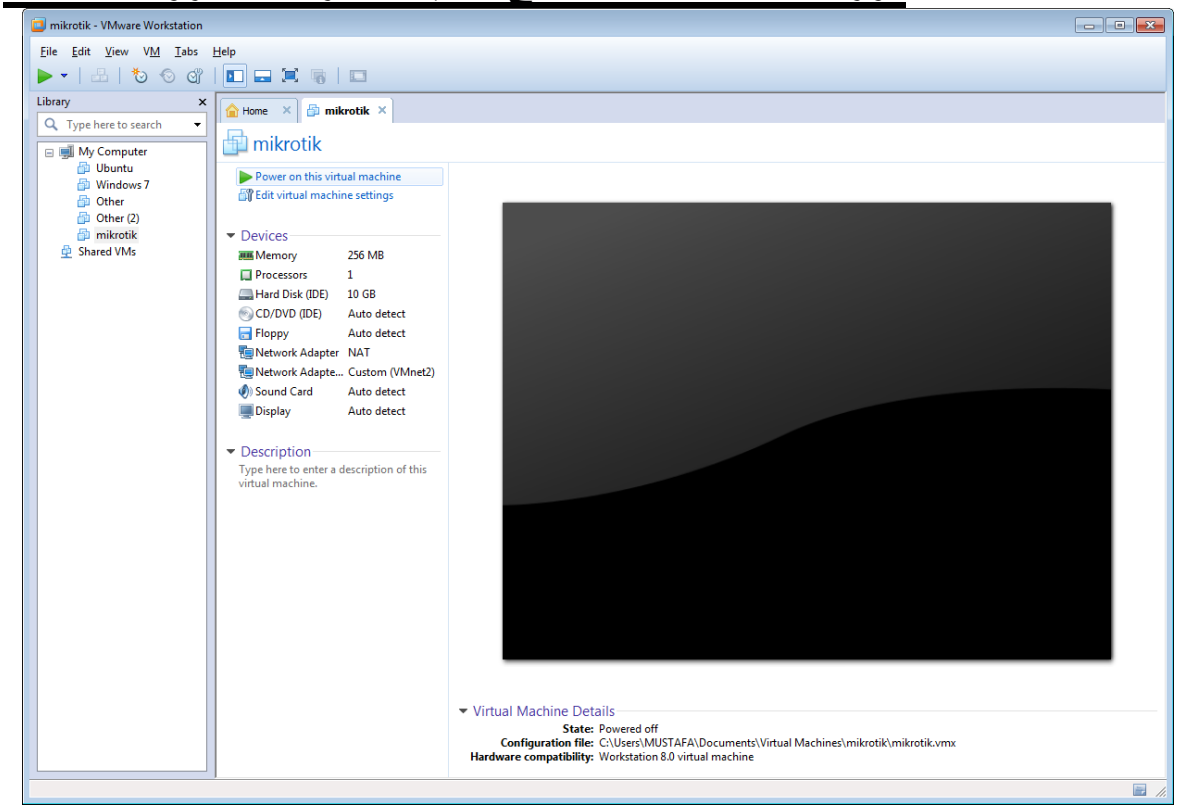
ننقر على (next) لتظهر النافذة التالية ونختار منها تسمية الكرت الثاني وكما مؤشر ادناه:



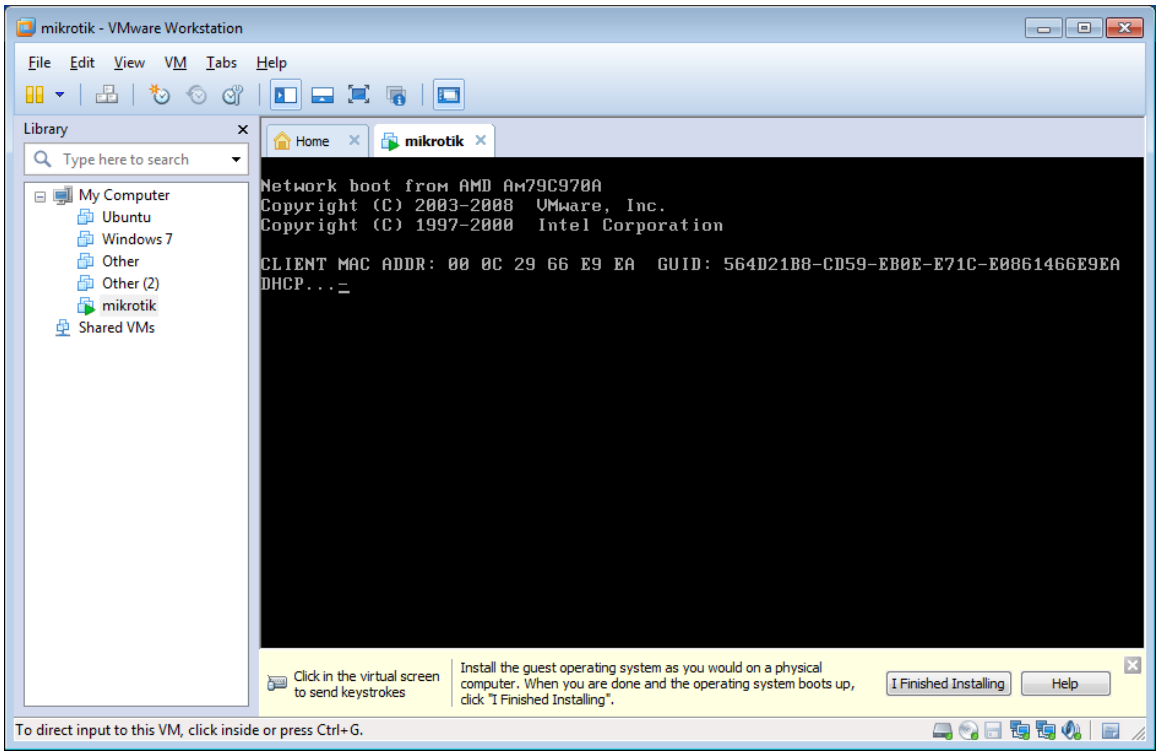
واخيراً ننقر على (finish) لتظهر النافذة التالية:



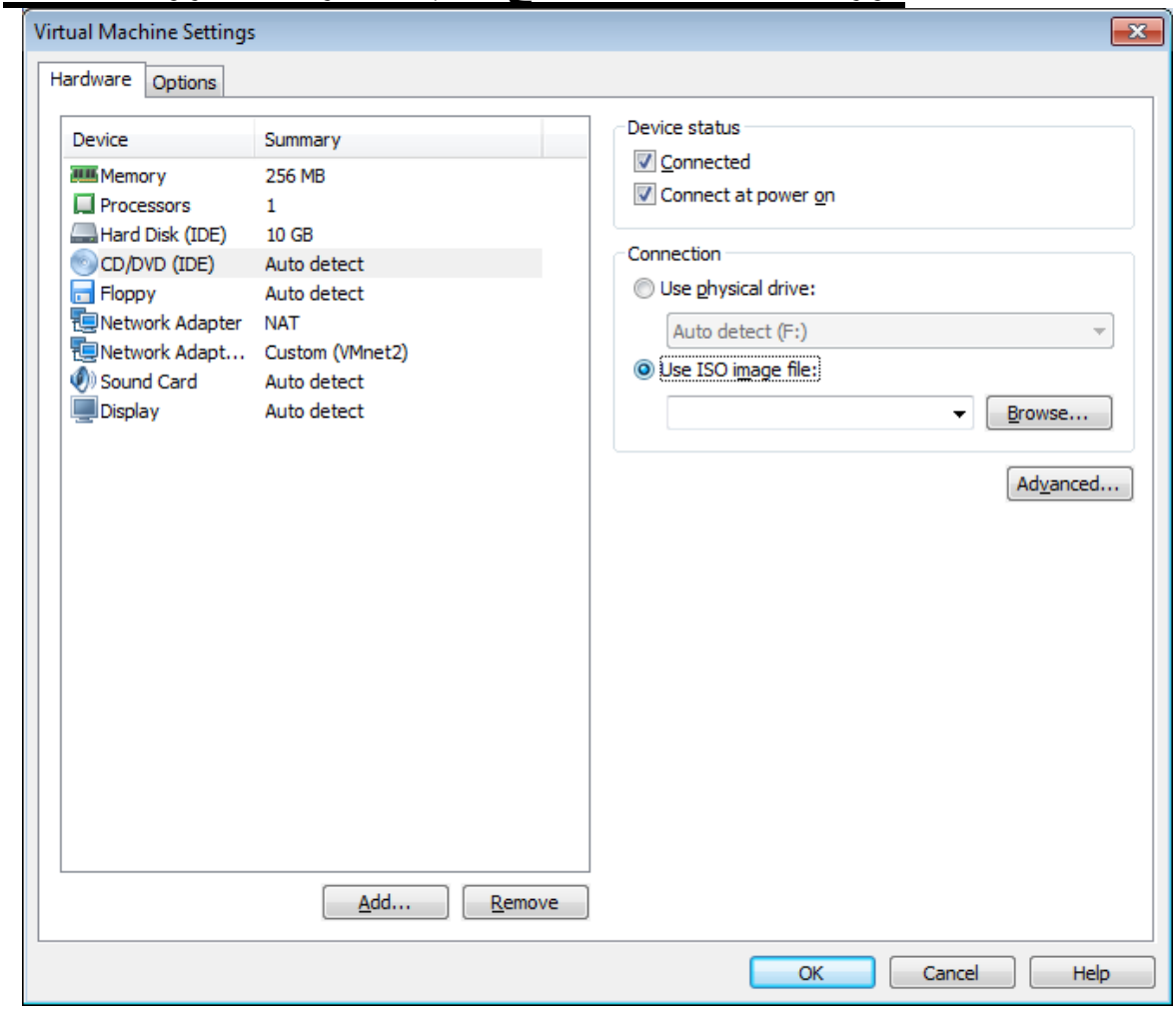
نغلق النافة اعلاه بالنقر على (ok) والان نشغل الماكنة الافتراضية بالنقر على (power on) كما في الصورة ادناه:



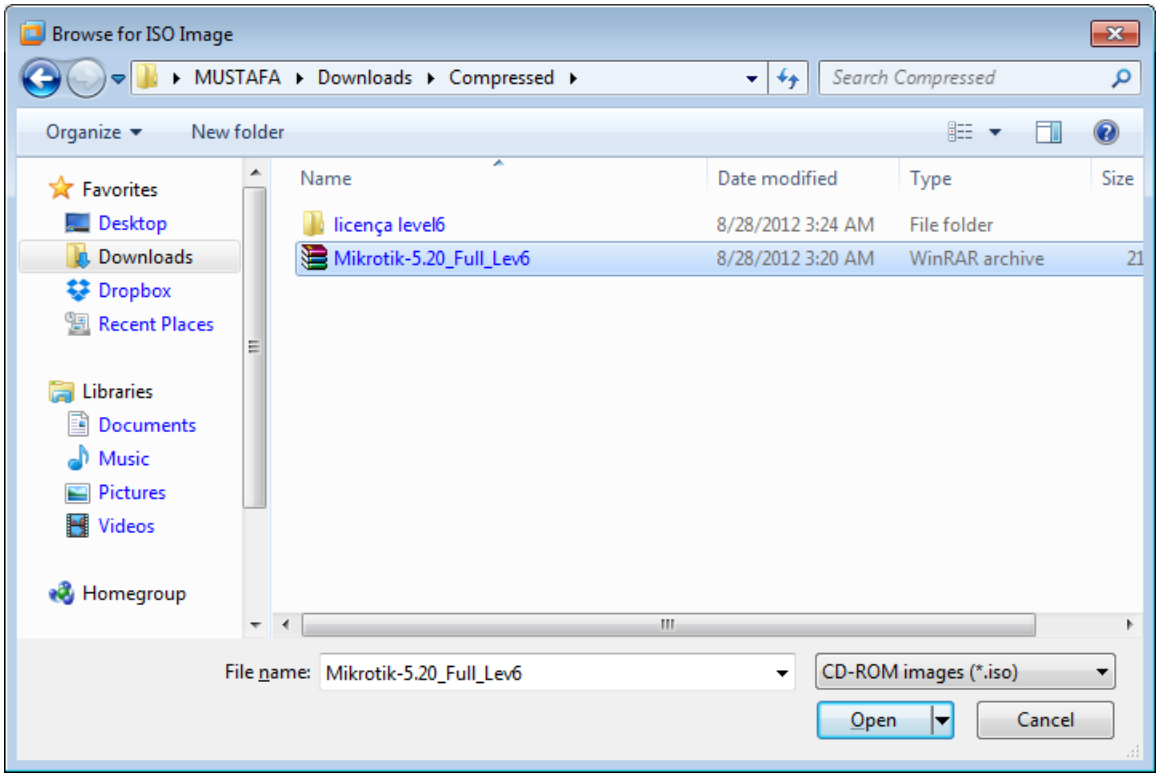
والان نذهب الى اسفل النافذة في الجهة اليمنى لنجد ايقونة تشبه قرص ال (CD) فننقر عليها كما في النافذة التالية:



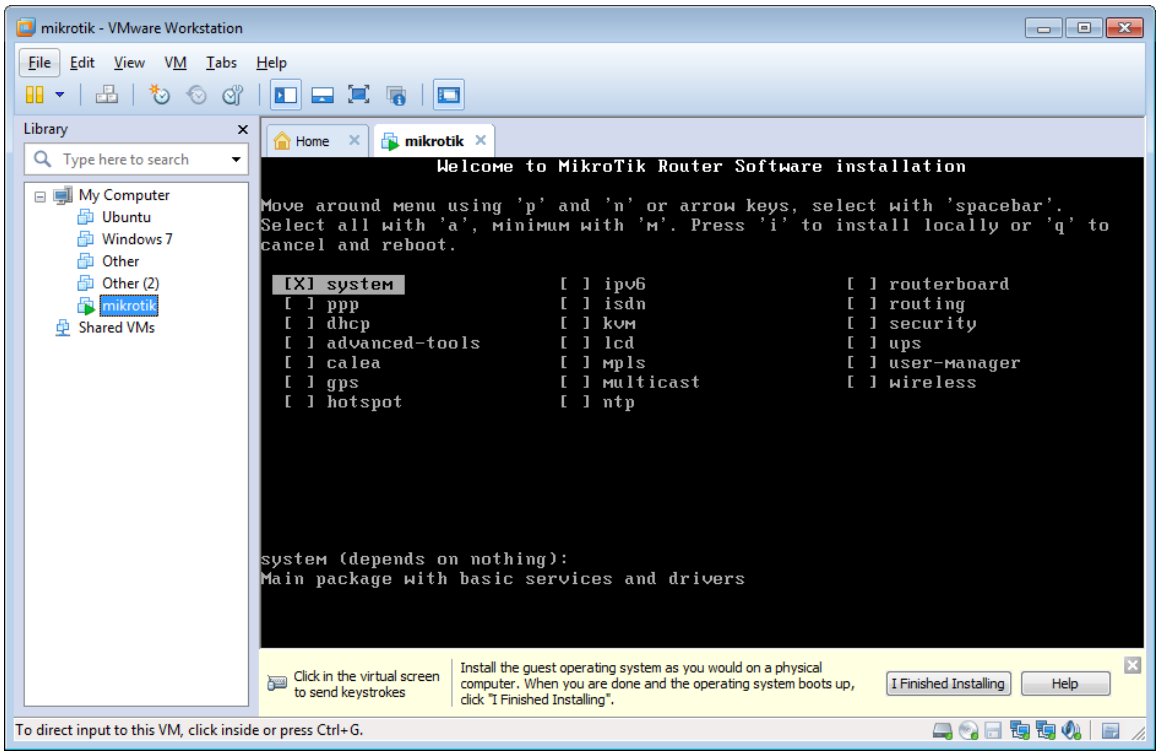
وبعد النقر عليها تظهر النافذة التالية ونختار منها (Use ISO image file) وننقر بعدها على (browse) :



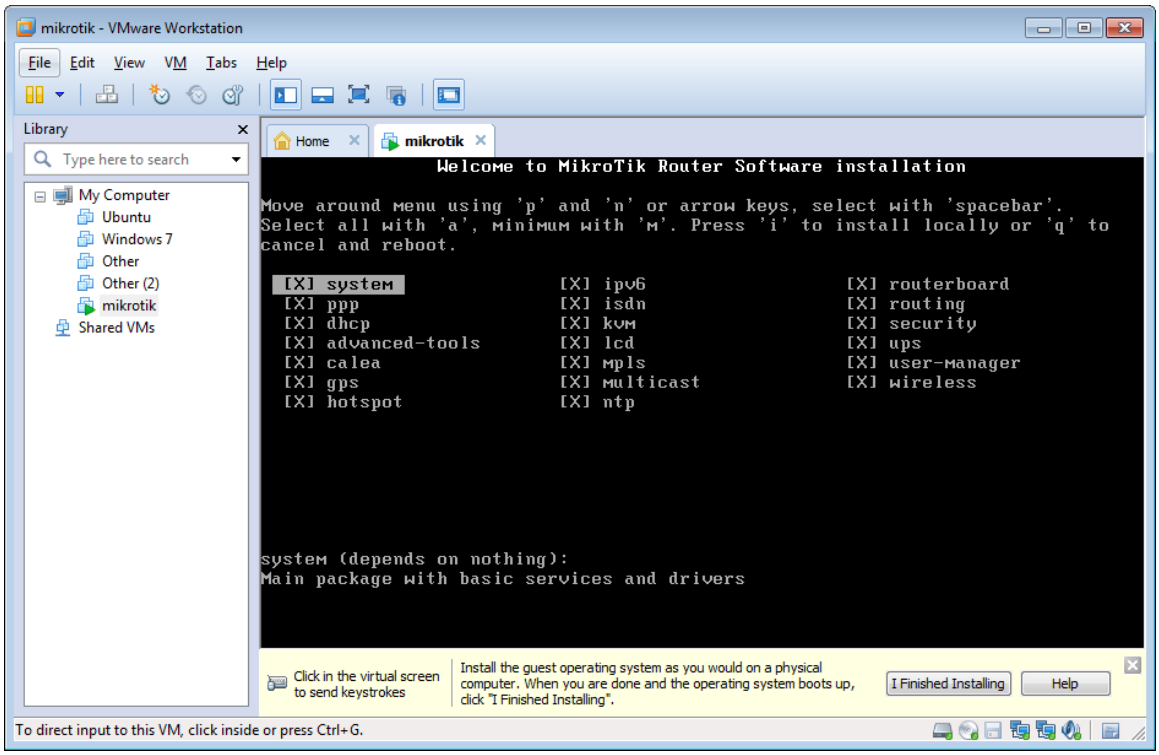
تظهر بعددها النافذة التالية التي نحدد فيها مكان الملف الذي قمنا بتنزيله :



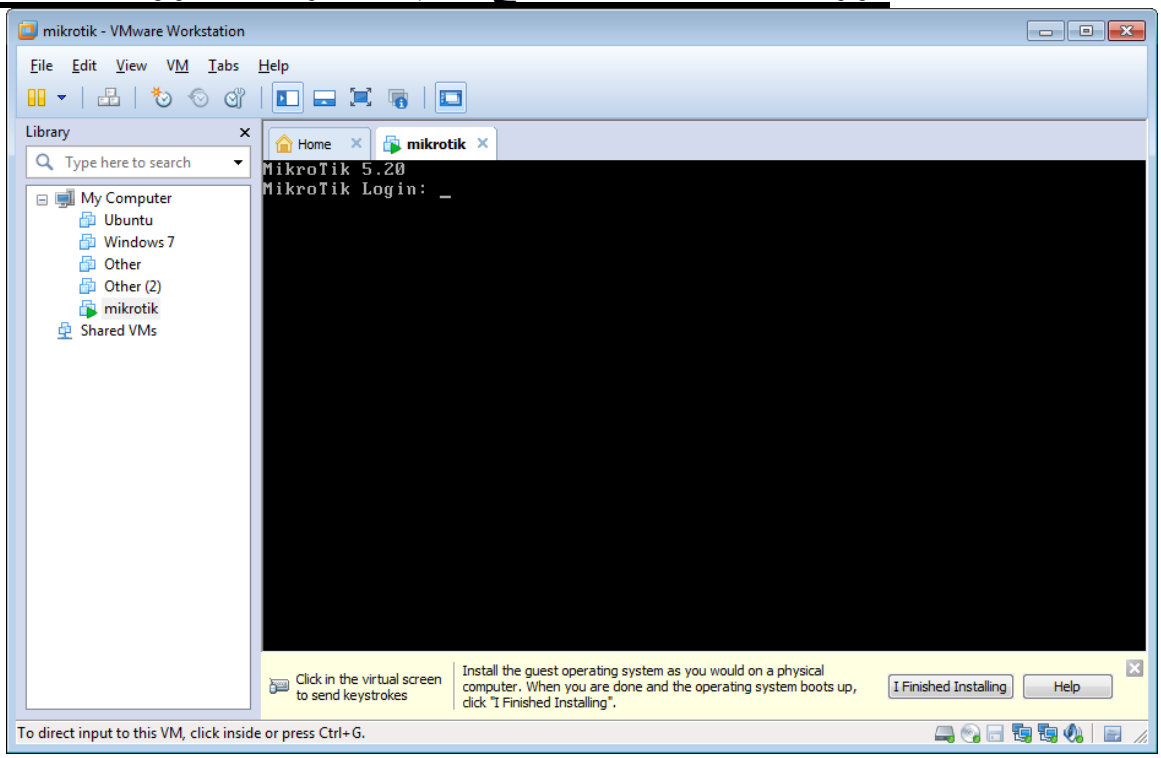
الان نعيد تشغيل الجهاز الافتراضي بالنقر على ايقونة اسم الجهاز (mikrotik) نقرة يمين ثم الذهاب الى (power) ثم (reset) وعند اعادة التشغيل سيبدأ تنصيب المايكروتك وكما في النافذة ادناه:



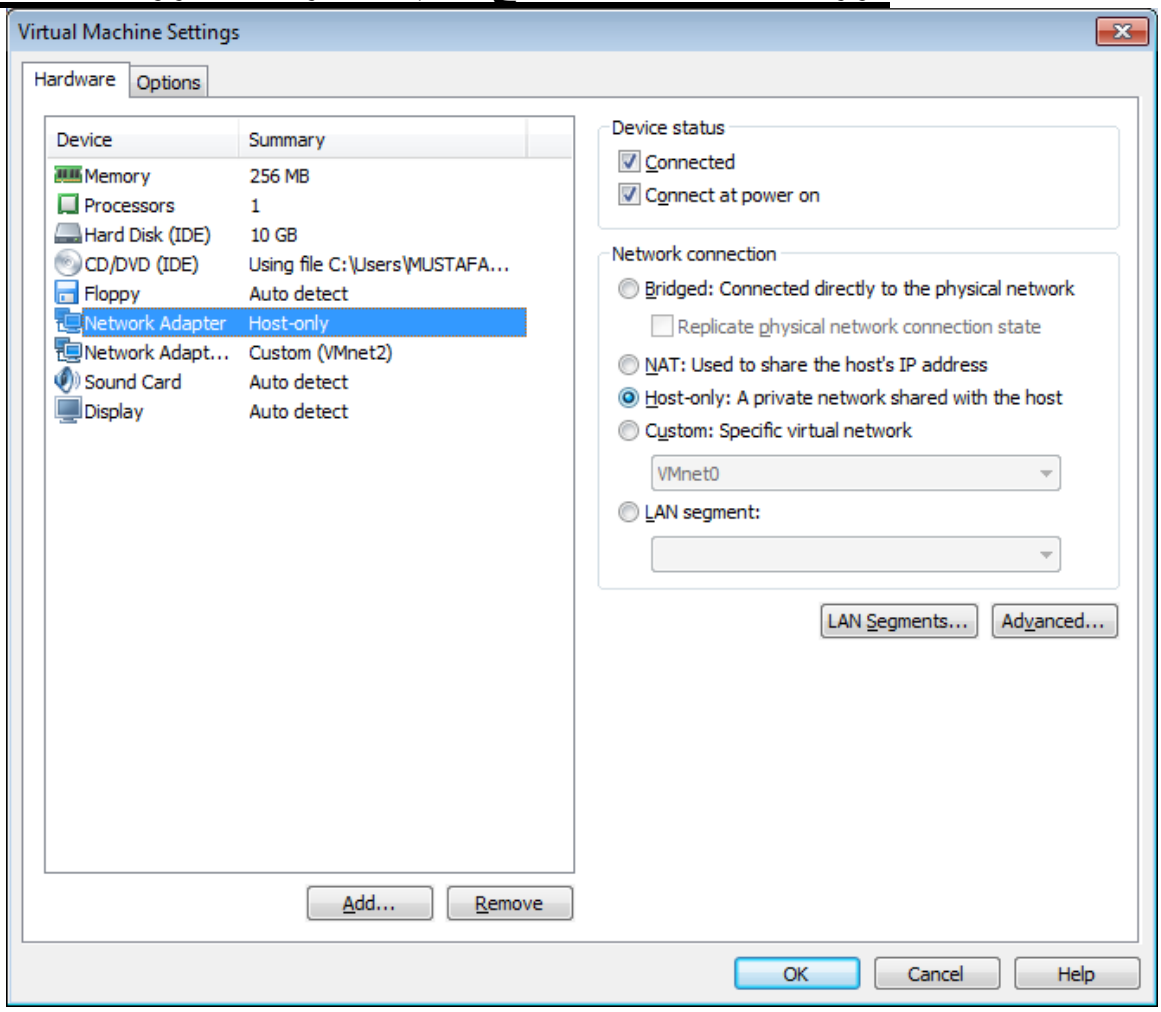
الان ننقر على زر (a) لأختيار الكل فتتحول النافذة الى الشكل التالي:



والان ننقر على زر (I) للتنصيب ثم ننقر على (n) ثم (y) ليبدأ التنصيب وبعد قليل وعند انتهاء التنصيب ننقر على (enter) لأعادة التشغيل وبعد ان يتم اعادة التشغيل تظهر النافذة التالية:



والان نقوم بالخطوة الاخيرة لجعل جهازنا الافتراضي قابل للوصول اليه من قبل حاسوبنا الحقيقي فنذهب الى الجزء الاسفل الايمن من نافذة النظام الافتراضي وننقر على ايقونة كرت الشبكة الاول الاصلي ونذهب الى (Setting) ثم تظهر نافذة كالاتي:

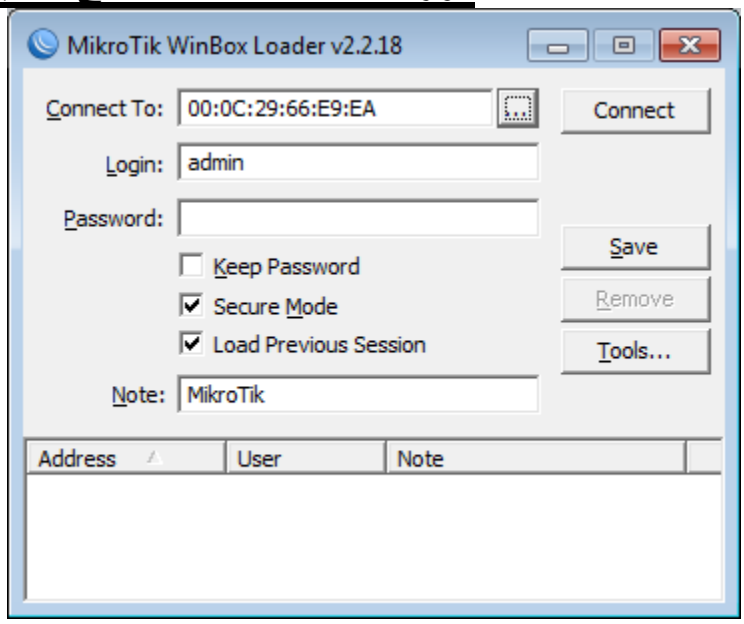


فنختار نوع ارتباط بالشبكة من نوع (host only) كما في النافذة اعلاه.

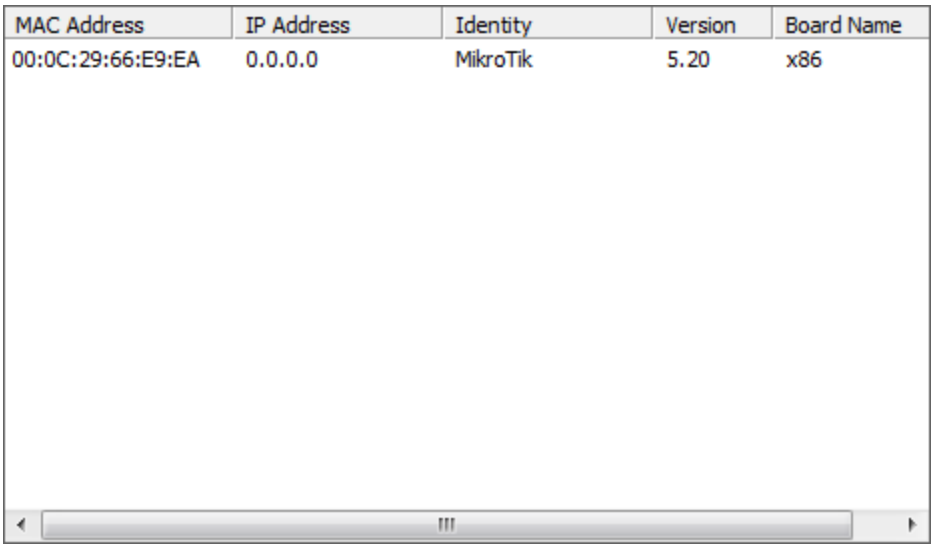
والان نستطيع ترك هذه النافذة والذهاب الى سطح المكتب خاصتنا (الحقيقي) وننصب برنامج ال (winbox) او في الحقيقة ننزله من موقع الشركة ومن الرابط التالي:

http://www.mikrotik.com/download

وعند النقر على ايقونة البرنامج تفتح النافذة التالية:



فننقر على زر (connect) لتظهر النافذة التالية وننقر على ال (MAC address) للأتصال بالروتر الافتراضي ونبدأ من هنا تطبيق الدروس من (١-٧) التي تم نشرها سابقاً:



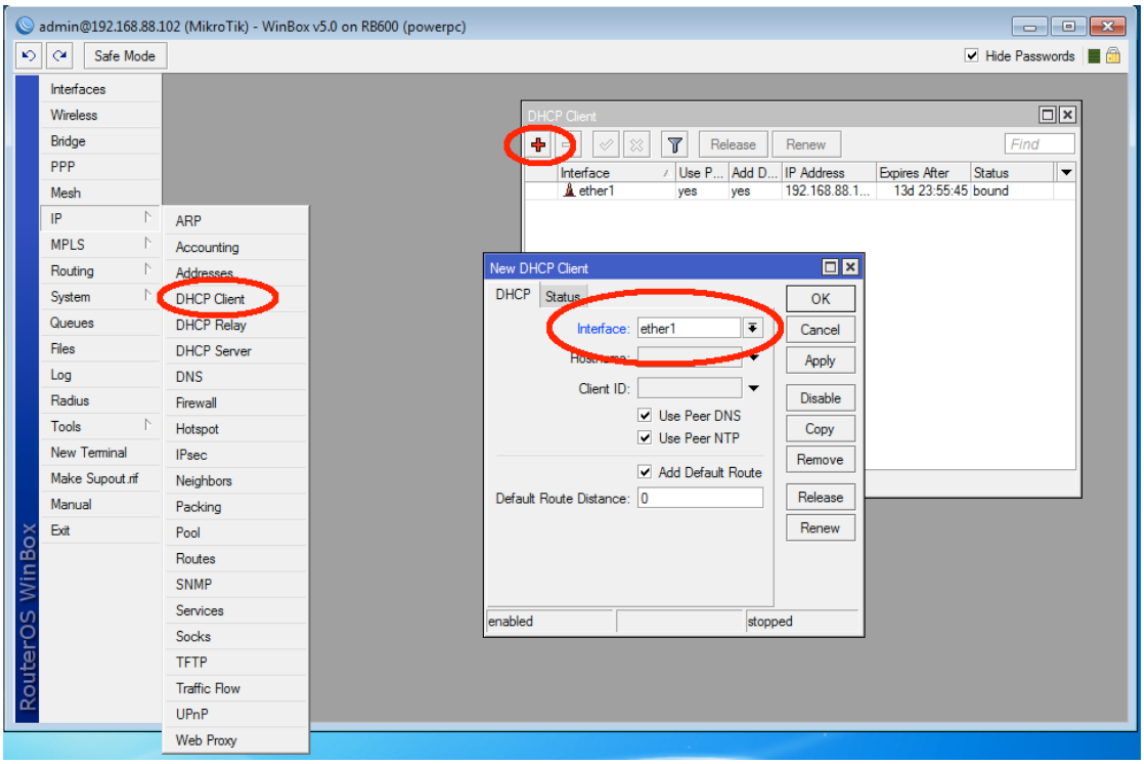
الدرس التاسع من سلسلة دروس شرح سيرفر المايكروتك

انشاء وادارة (MikroTik hotspot):

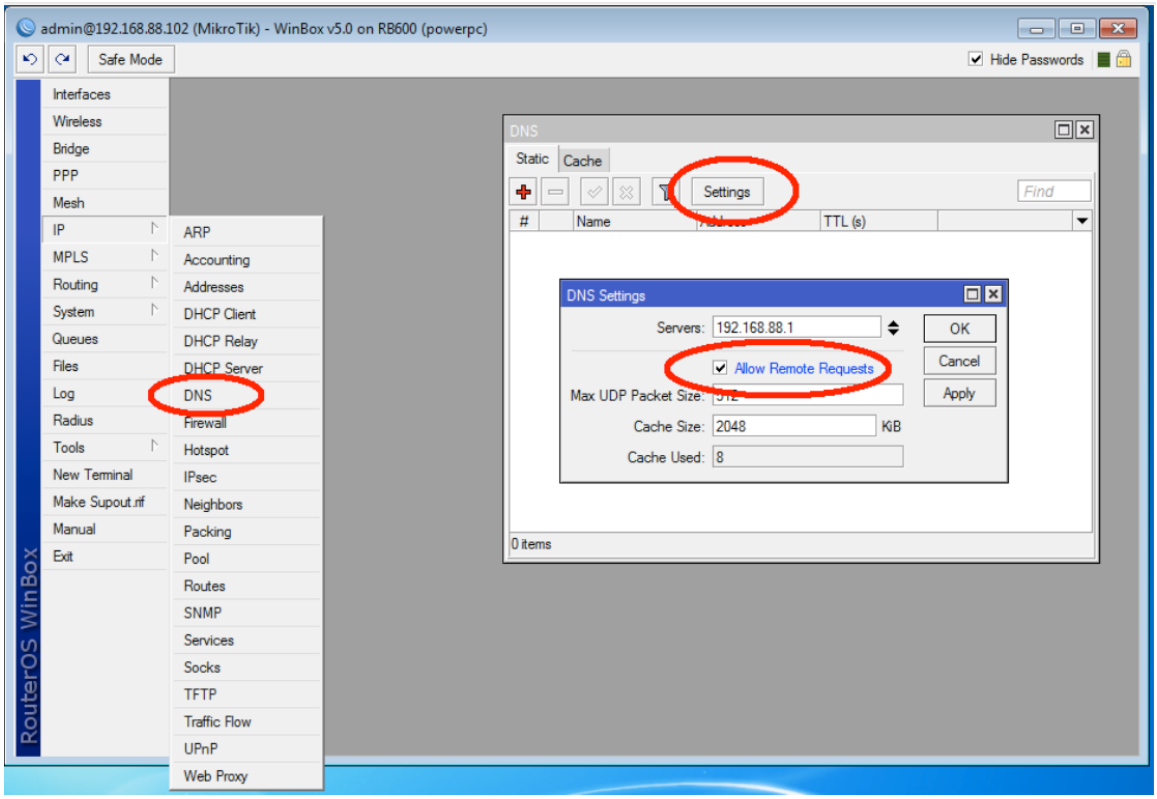
الهوت سبوت هو احد الطرق الكثيرة التي يوفرها راوتر المايكروتك لتسهيل امكانية الوصول اللاسلكي الى الانترنت عبر سيرفرات المايكروتك عن تسهيل استخدام واجهة الدخول بكلمة مرور واسم مستخدم. هذه الطريقة تعطي لمالك الشبكة او مدير الشبكة سيطرة تامة على محددات التنزيل وادارة السرعة وعرض النطاق وكيفية الدفع وتحديد وقت توفير الخدمة ووقت قطعها. وتعتبر هذه الطريقة هي الطريقة الانسب للفنادق والمطاعم والمقاهي ومراكز المؤتمرات والاجتماعات لتوفير خدمة الانترنت بشكل ديناميكي ومسيطر عليه بشكل جيد.

في البدء يجب التأكد من ان الراوتر الذي سنعمل عليه مضبوط على اعدادات المصنع اي انه ليس هناك اي اعدادات مستخدم مسبقة قد تتضارب مع اعداداتنا الحالية والمستقبلية وان يتوفر فيه المنافذ المطلوبة ولتكن منفذين سلكيين ومنفذ لا سلكي على الاقل (2-LAN Card and 1-Wireless LAN card).

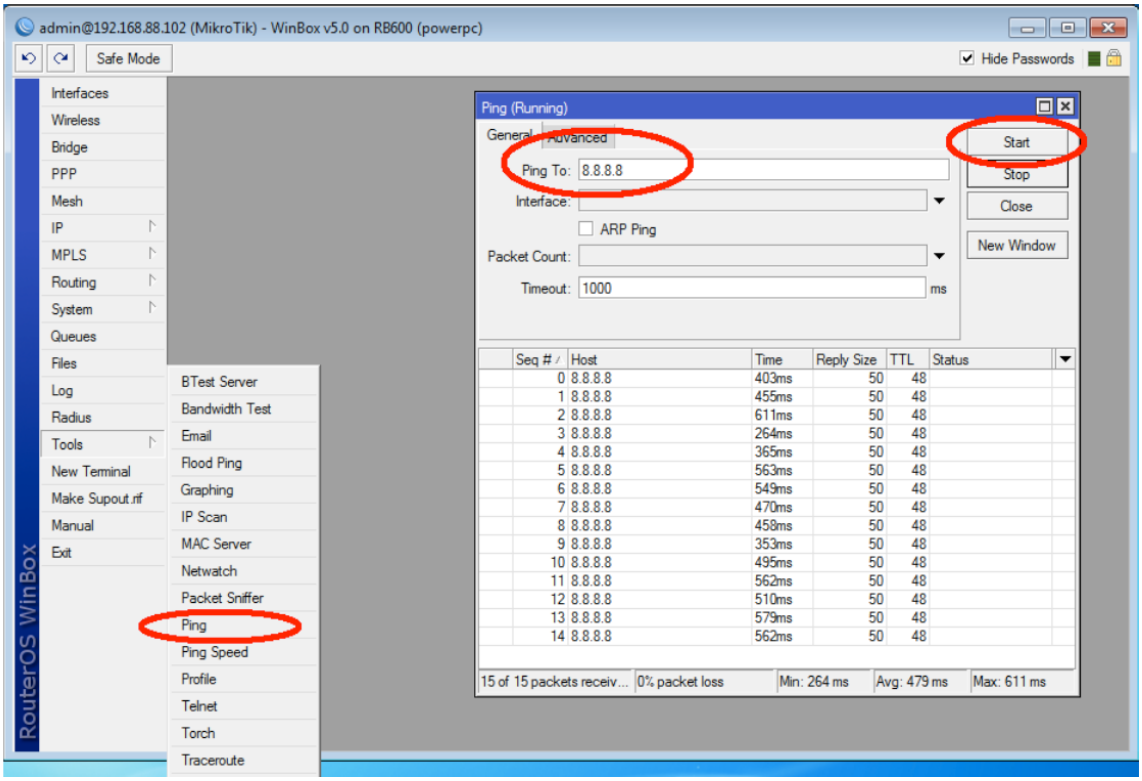
اول خطوة في ضبط الهوت سبوت هو توفير اتصال بالانترنت للرواتر من احد منفذي الشبكة المحلية (LAN card) ويتم ايصال خدمة الانترنت الى راوتر المايكروتك من اي رواتر اخر وليكن (ADSL modem) ويفترض ان تكون خاصية (DHCP server) مفعلة في ذلك المودم لكي نفعل خاصية ال (DHCP client) في راوتر المايكروتك خاصتنا وكما في الصورة ادناه:



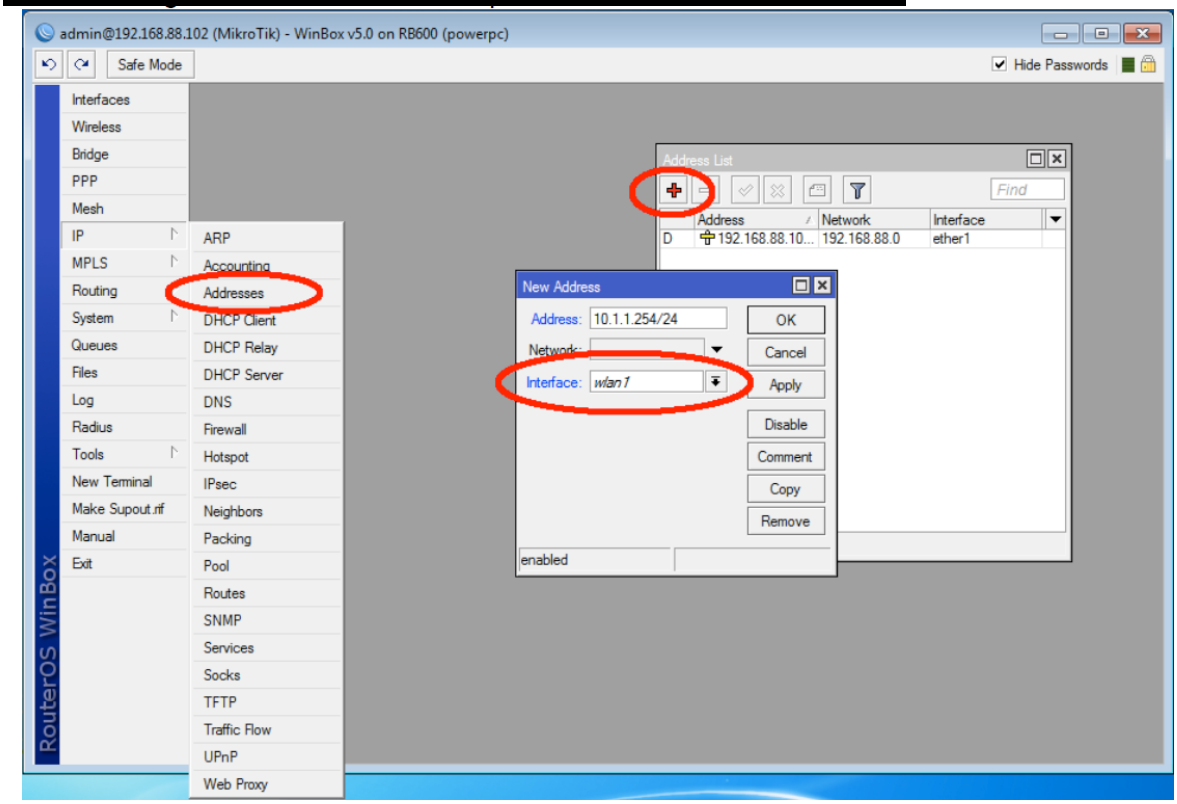
الخطوة الثانية في اعدادات الهوت سبوت هي التأكد من ان الراوتر خاصتنا يستطيع استلام طلبات ال (DNS) استناداً الى اعدادات ال (DHCP server) وكما في ادناه:



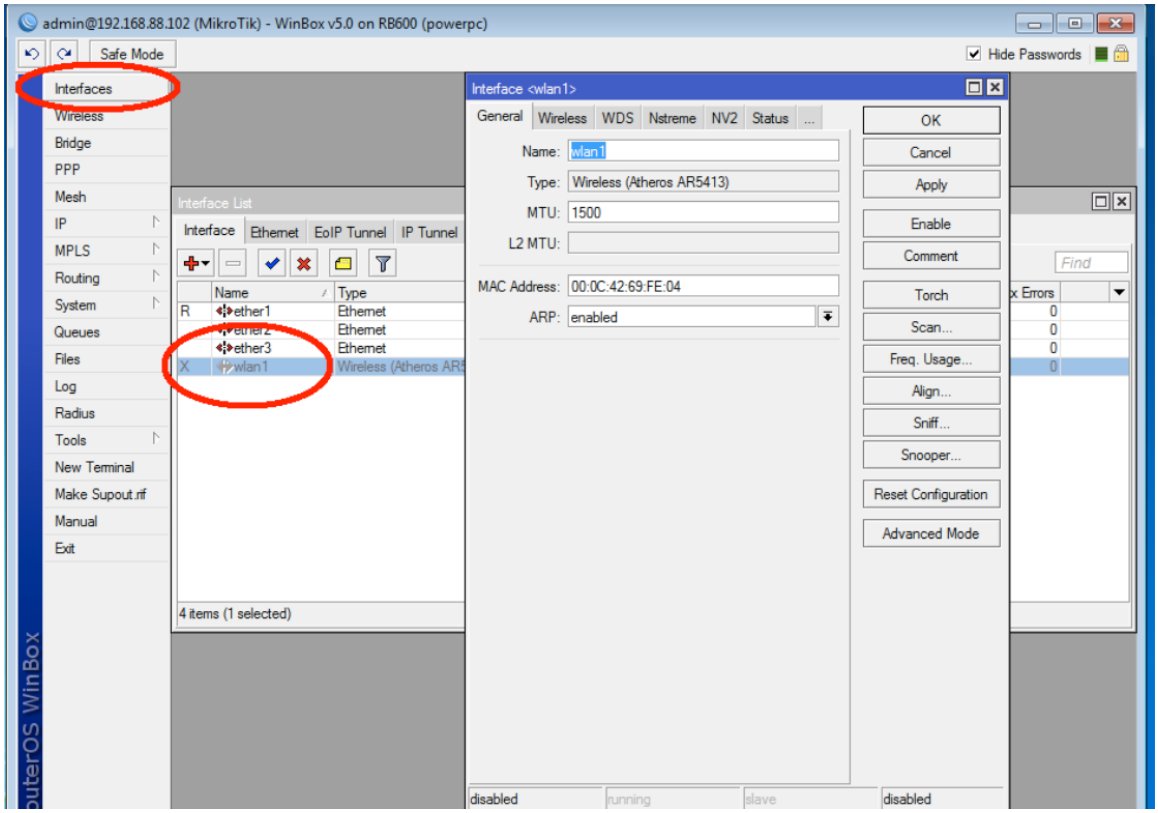
الخطوة الثالثة هي ضبط اعدادات اتصال الانترنت بأرسال رسالة فحص الى سيرفر الكوكل على العنوان (8.8.8.8) وهو سيرفر ال(DNS) الخاص بالكوكل وكما يلي:



والان نصل الى ضبط اعدادات المنفذ اللاسلكي الذي سيكون مسؤول عن توزيع الخدمة للزبائن وتكون اول خطوة في اسناد عنوان (IP address) الى المنفذ اللاسلكي ويمكن استخدام اي عنوان هنا شرط ان يختلف عن حيز عناوين ال (DHCP server) وتذكر ان تكتب الرقم الخاص بقناع الشبكة الفرعية (subnet mask /8 or/16 or /24) وحسب نوع العنوان المستخدم وكما في ادناه:

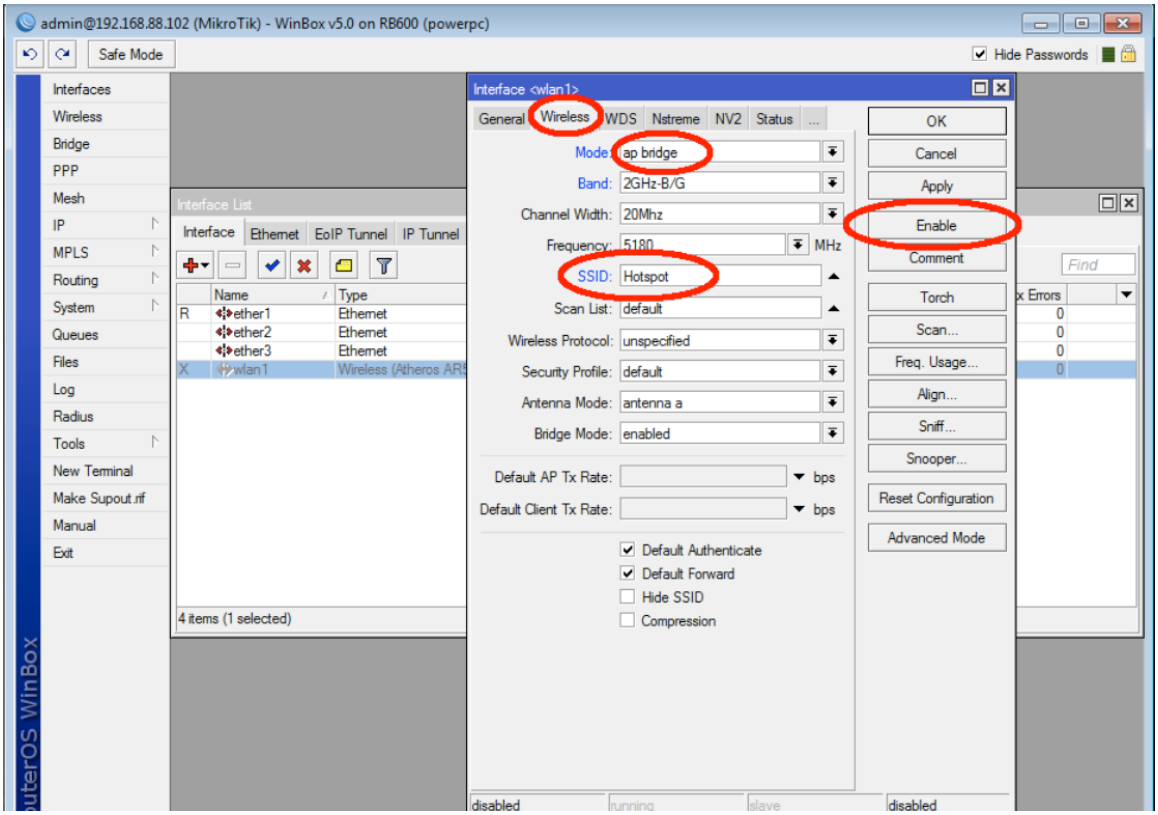


والان بعد ان تم اسناد عنوان للمنفذ اللاسلكي فيجب ان نقوم بأعداده ليستقبل الاتصالات اللاسلكية فننقر على تبويب (interface) نقرة مزدوجة وبعدها ننقر على رمز المنفذ اللاسلكي كما في ادناه:

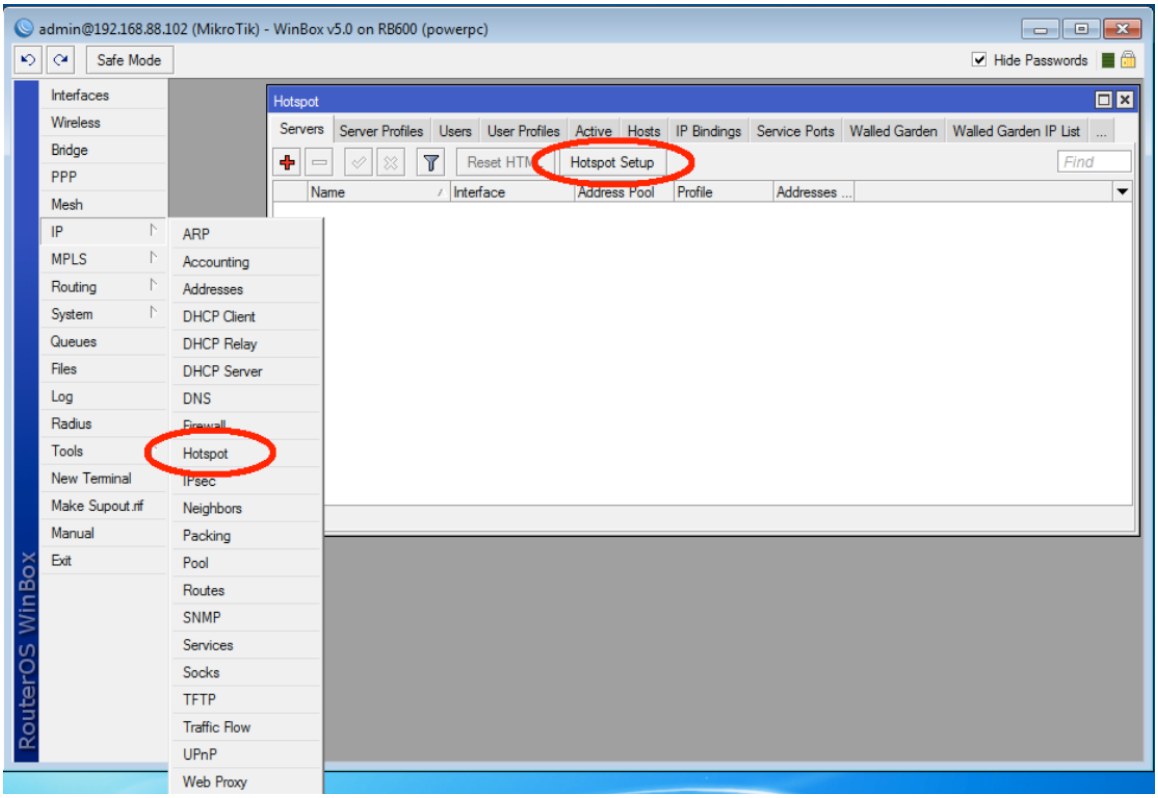


والان في صفحة اعدادات الكرت اللاسلكي ننقر على تبويب (wireless) ونختار نمط العمل ليكون (AP_Bridge mode) وهذا النمط سيجعل الكرت اللاسلكي للراوتر خاصتنا يعمل كنقطة وصول لاسلكية (Wireless access point) للزبائن للأتصال عن طريقها. ونضبط النطاق (Band) على (2GHZ-B/G) وهو النطاق الاكثر شيوعاً في الاجهزة اللاسلكية ومن

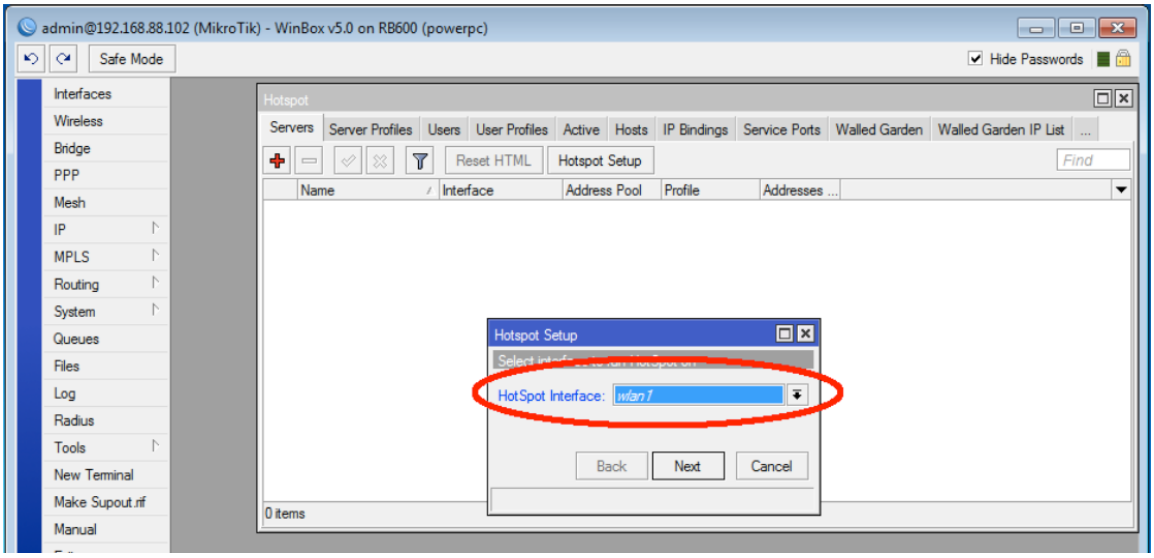
ضمنها الحواسيب المحمولة (labtops) واخيراً نضبط اسم الشبكة (Service Set Identifier SSID) وهو الاسم الذي سيظهر للمستخدمين للأرتباط به وليكن اي اسم ويفضل وضع كلمة دلالة معينة او حتى رقم الهاتف الشخصي لكي يستطيع المستخدمين الاتصال بك والاستفسار عن امكانية الاشتراك معك وننقر على (apply) ثم ننقر على (enable) لتمكين العمل في هذا المنفذ وكما في النافذة ادناه:



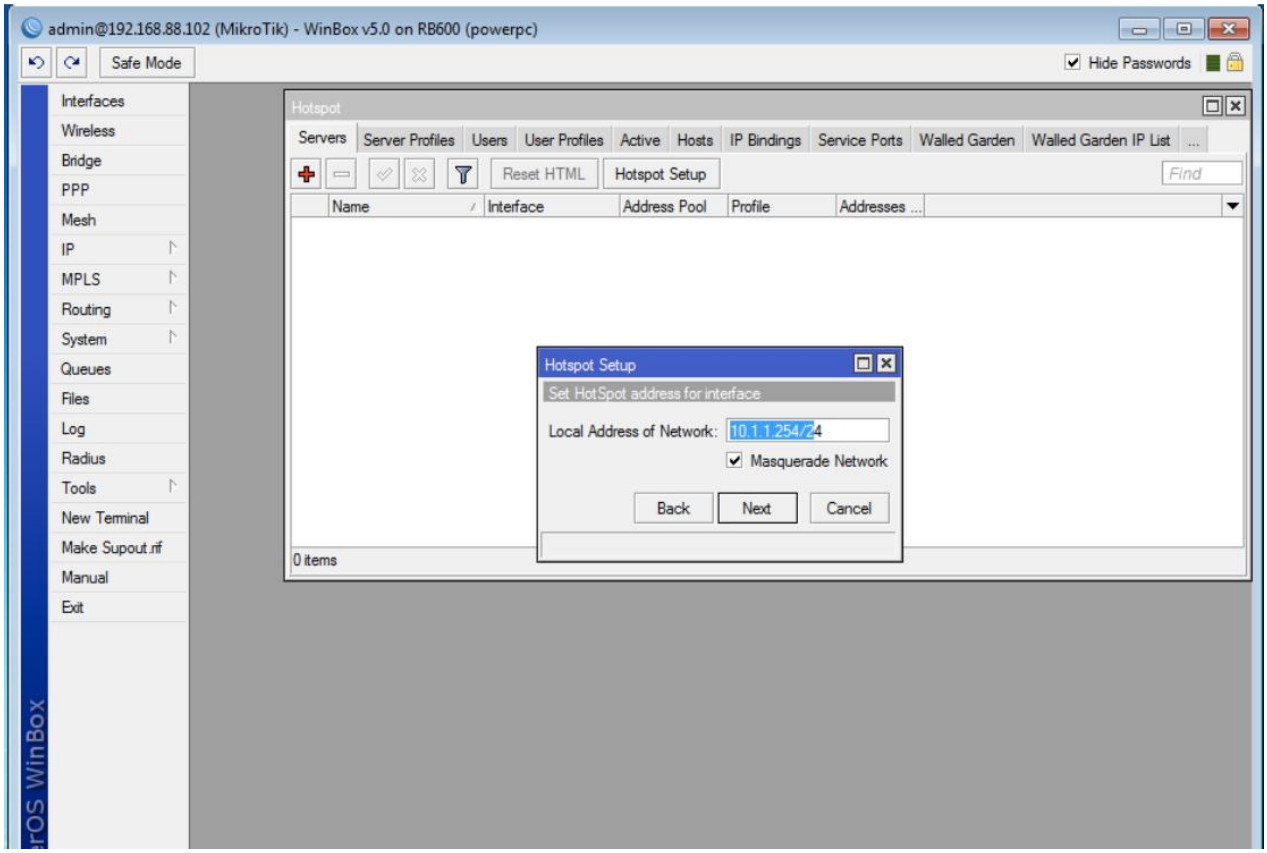
والان يمكن اكمال اعدادات الهوت سبوت بأتباع الخطوات في النافذة التالية:



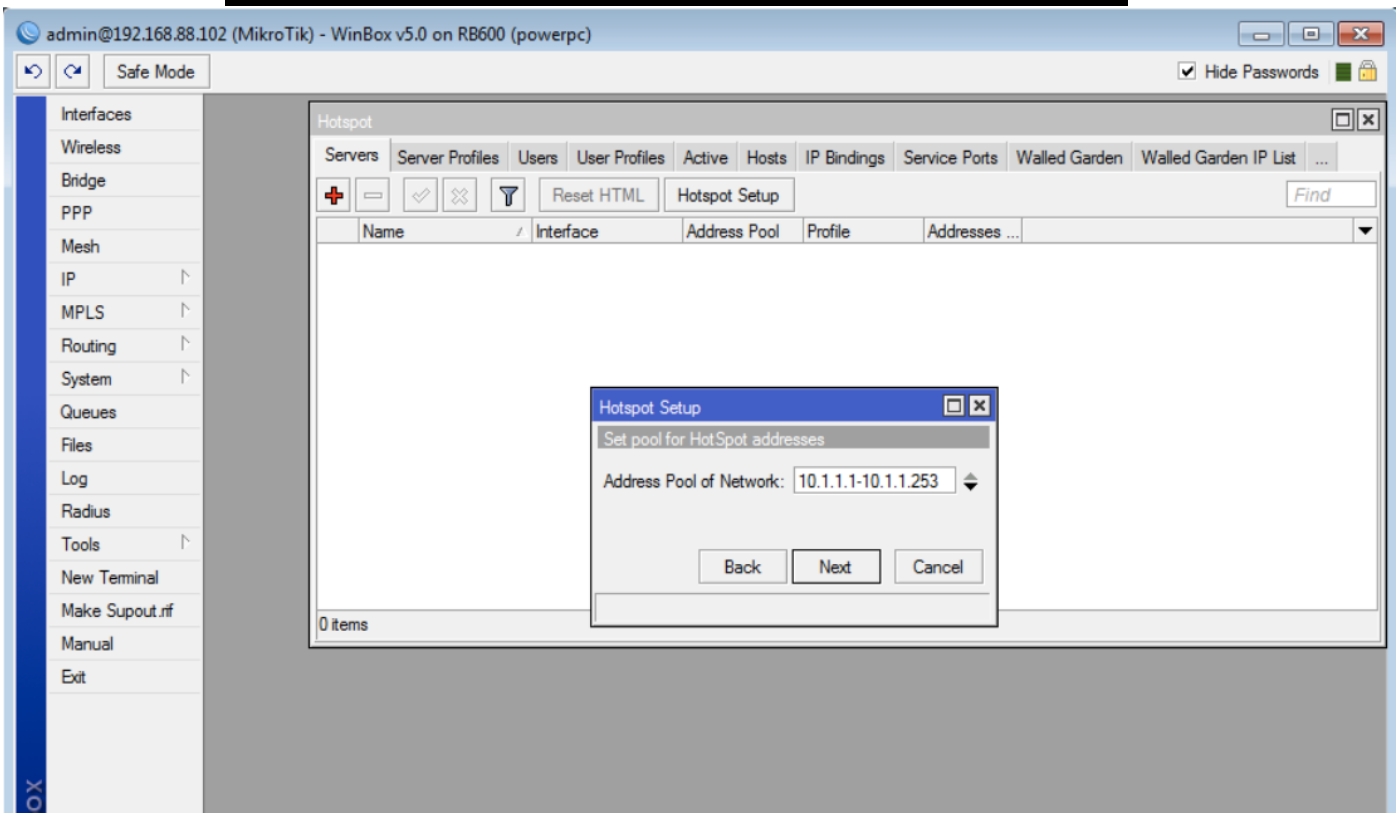
اول خطوة في اعداد الهوت سبوت هو اختيار المنفذ (سلكي او لاسلكي) والذي سيوفر خدمة الهوت سبوت للمستخدمين وهو في حالتنا هذه (wlan) فنختاره كما في الصورة التالية ثم ننقر على (next):



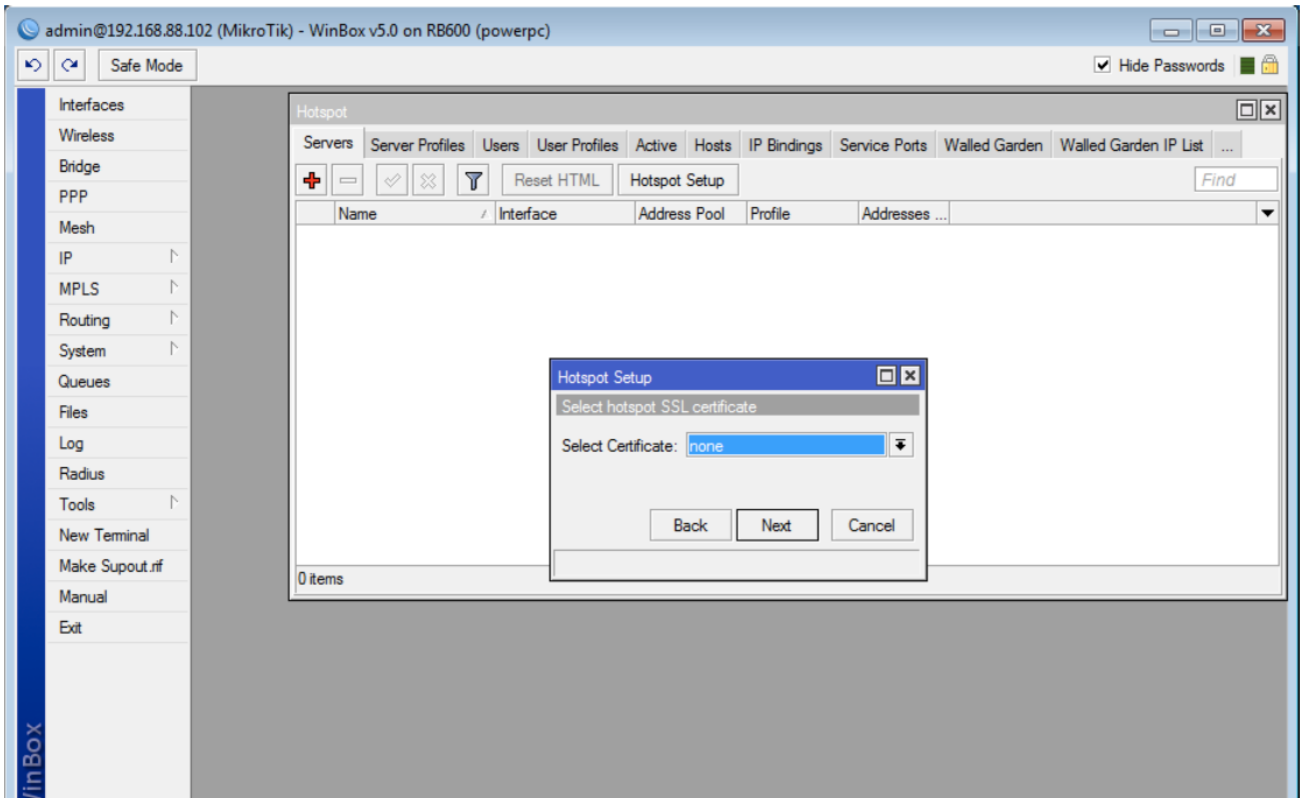
في الخطوة المقبلة يجب تحديد العنوان المحلي (local IP address) للهوتسبوت والذي يجب ان يعتمد على العنوان الذي تم اسناده سابقاً الى الكرت اللاسلكي للمايكروتك وسيقوم المايكروتك بملئه تلقائياً اعتماداً على الاعدادات السابقة ويفضل عدم تغييره. تأكد ان خيار تنكر الشبكة (masquerade network) قد تم اختياره وتحديده ثم انقر على (next) وكما في النافذة التالية:



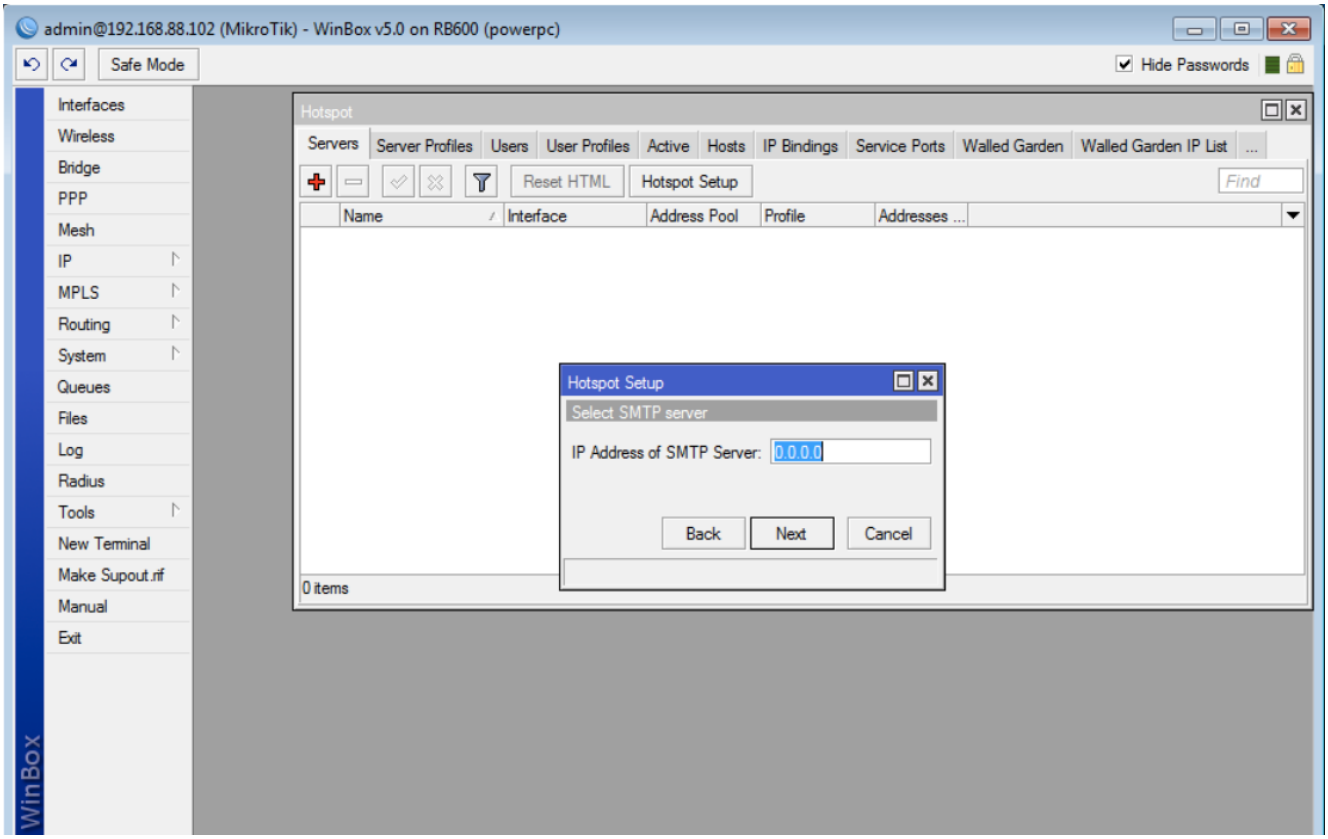
هنا يجب تحديد مدى العناوين في حوض عناوين ال (IP address pool) وسيتم ملئه تلقائياً ايضاً اعتماداً على العنوان الذي سبق ادخاله للكرت اللاسلكي للجهاز ويفضل عدم تغييره وكما في النافذة ادناه:



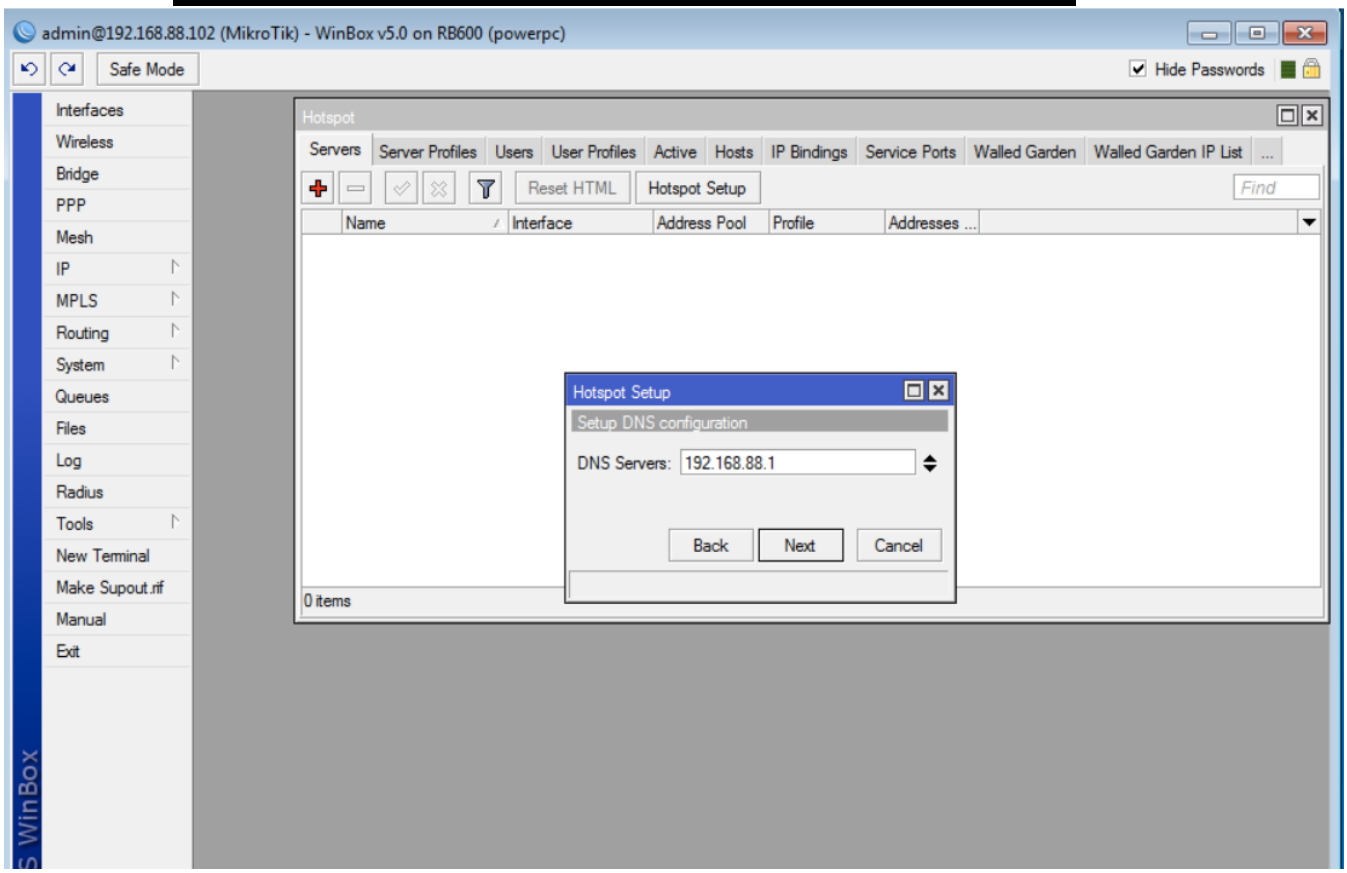
والان نصل الى مرحلة اختيار نوعية التشفير والامنية للشبكة ففي حالة اختيار احد ال (SSL/HTTPS certificates) نقوم بتحديدها هنا والا فنترك الحقل بحالة (none) وكما في النافذة ادناه:



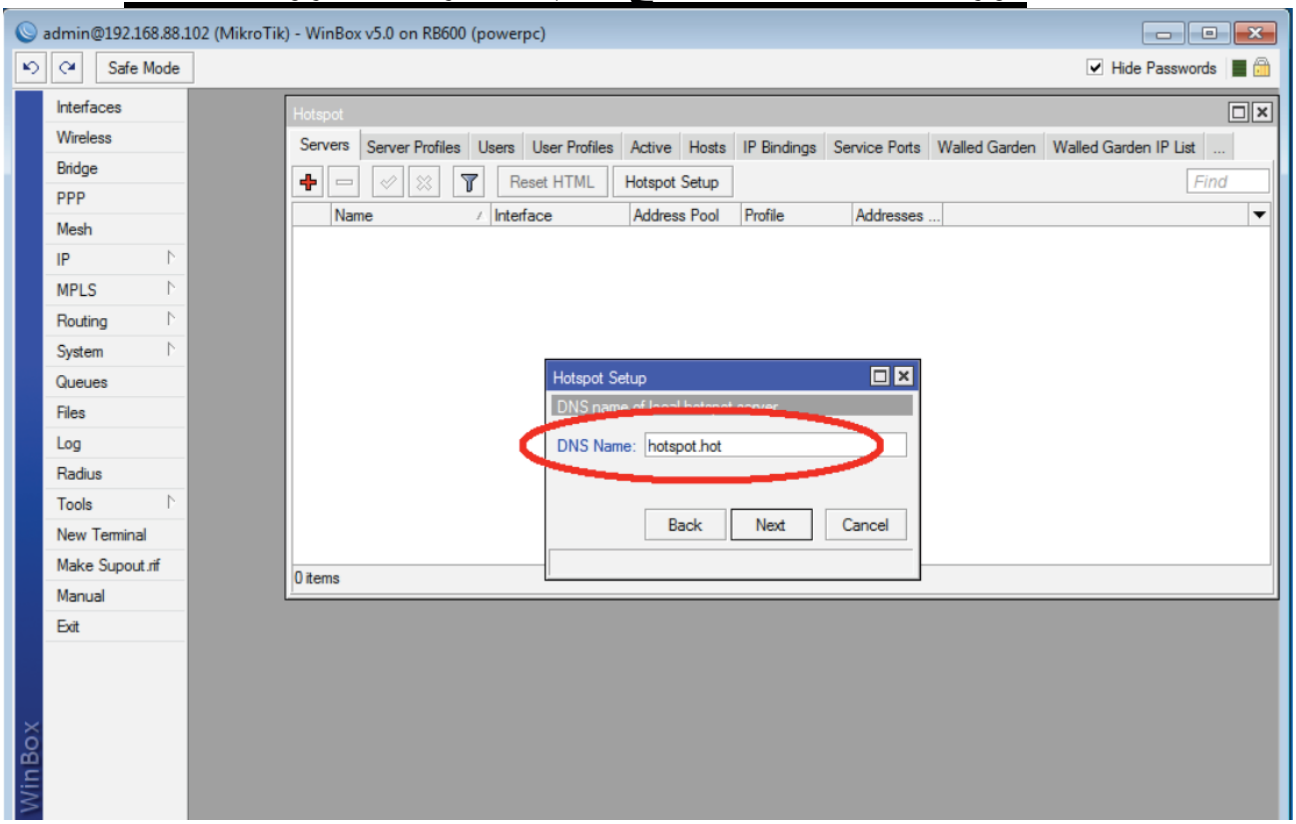
كما قلنا سابقاً فأن من اهم تطبيقات الهوت سبوت هو في المطارات والفنادق ودور الضيافة للوفود الاجنبية وهنا يجب على المسافرين عبر البحار ومن دول اخرى ان يقوموا بتعديل خيارات سيرفر بروتوكول نقل البريد البسيط (SMTP Server) ويقوم هذا الخيار بالسماح للمايكروتك بمسك كل المرور القادم من زبائن الهوت سبوت واجباره على استخدام السيرفر الذي سنحدد عنوانه هنا واذا لم نرد فعل ذلك نترك العنوان فارغاً اي (0.0.0.0) وكما في النافذة ادناه:



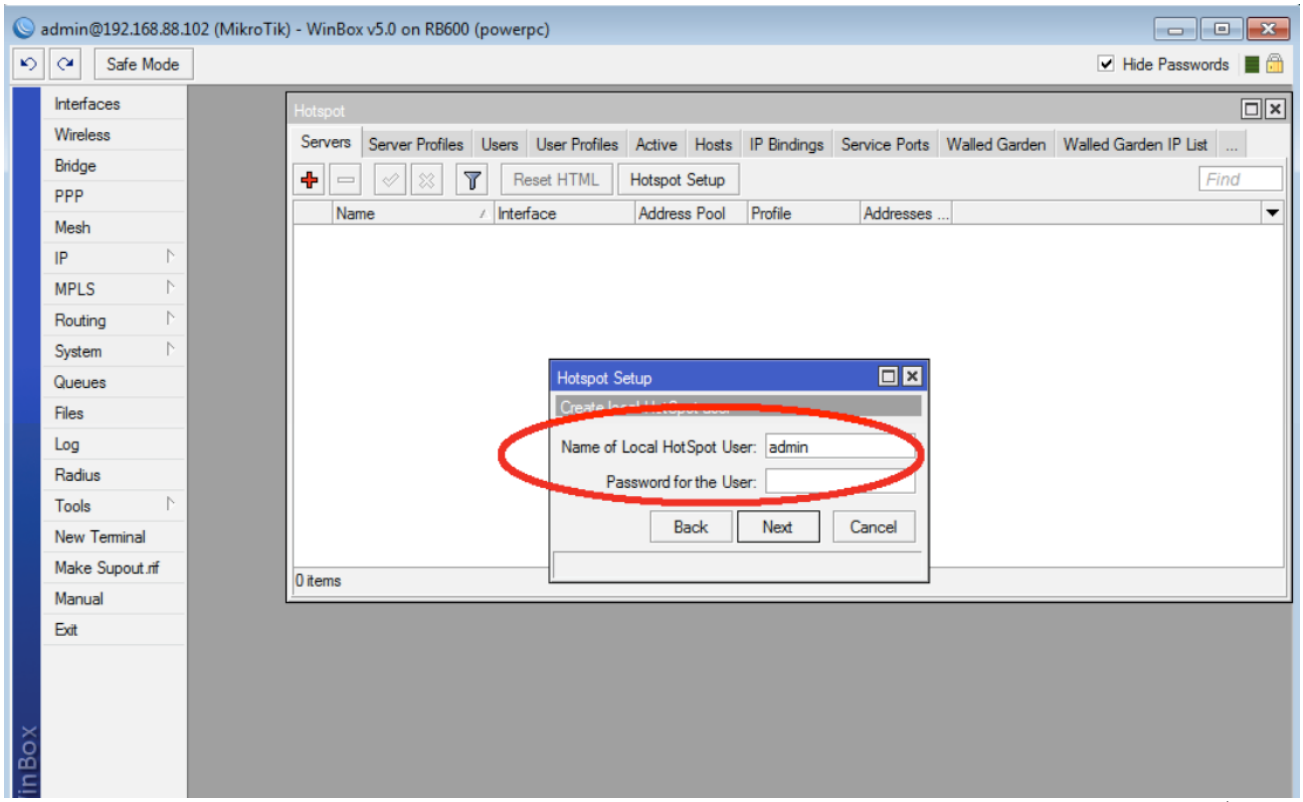
وتستمر اعدادات الهوت سبوت ونصل الى مرحلة تحديد اعدادات ال (DNS) ونضع هنا عنوان السيرفر الذي نريد ان يستخدمه الزبائن ويمكن ايضاً ان يتم ملئه تلقائياً استناداً الى المعلومات التي نستلمها من سيرفر ال (DHCP) وكما في النافذة ادناه:



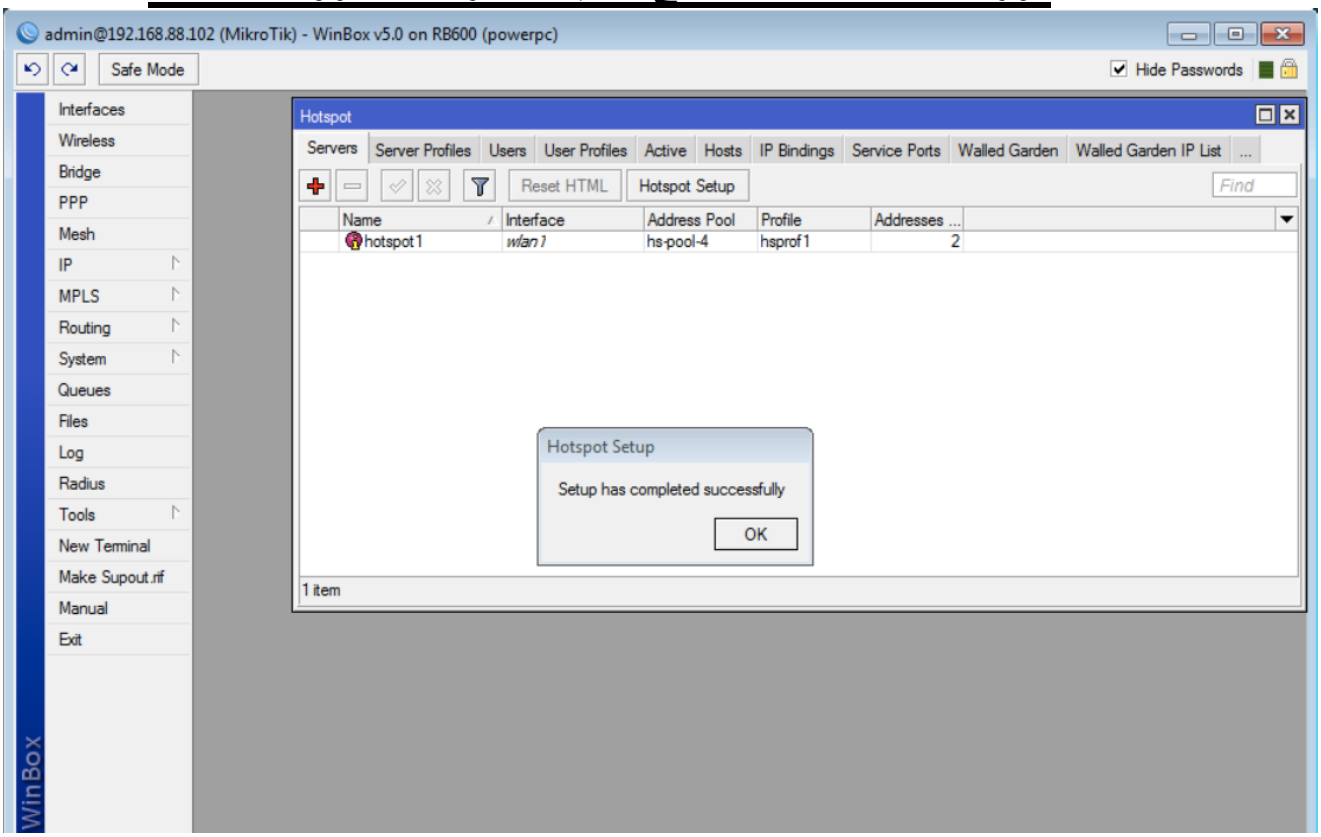
والان تظهر نافذة تطلب ادخال اسم ال (DNS) وهو مهم جداً في عمل الهوت سبوت حيث انه موقع الانترنت الذي يتم تحويل المستخدمين اليه تلقائياً حين نطلب منهم تسجيل الدخول عن طريق اسم المستخدم وكلمة المرور المعطاة لهم مسبقاً ويفترض في هذا العنوان (الاسم) ان لا يشابه اي عنوان موقع انترنت فمثلاً لا يمكننا استخدام الاسم (www.yahoo.com) او غيره من الاسماء للمواقع الشائعة بل وحتى غير الشائعة لتجنب التضارب والذهاب بالخطأ الى الموقع الاخر ويفضل احياناً ان يضم العنوان نقطة (dot) وكما في المثال التالي:



والان نصل الى نافذة الاعدادات الاخيرة والتي يمكن من خلالها تسجيل اول مستخدم بتحديد اسم المستخدم (user name) وكلمة المرور (password) والتي يجب ان يقوم المستخدمون بإدخالها ليستطيعوا الوصول الى الانترنت عبر الهوت سبوت خاصتنا وكما في النافذة ادناه:



واخيراً تظهر النافذة التالية:



والان انتهينا من اعداد الهوت سبوت ويستطيع المستخدمون الاتصال بشكل لاسلكي بعد ان يضبط المستخدمون اعدادات اجهزتهم اللاسلكية (laptops or PC with WIFI card) وحالما يقوم اي مستخدم بالاتصال بالشبكة اللاسلكية سيتم الطلب منه ادخال اسم المستخدم وكلمة المرور المعطاة له مسبقاً وبعدها ستظهر نافذة الانترنت.

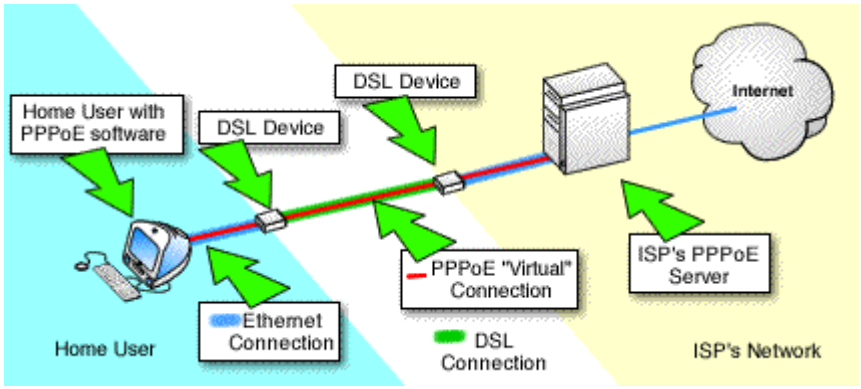
التراسل النفقي (tunneling communication) وتطبيقاته في المايكروتك

تتميز بيئة الشبكات بالوسائط المشتركة سواء اكانت سلكية او لاسلكية والسبب في ذلك ان كل من المرسل والمستلم يكون عادة متعدد المتطلبات في الوقت الواحد فتجد ان الحاسوب الواحد يتصفح صاحبه عدة صفحات ومواقع في نفس الوقت ويقوم بتنزيل عدة ملفات في نفس الوقت وكذلك فأن السيرفر الواحد يخدم مئات وربما الالف الزبائن في نفس الوقت ويستخدم نفس الوسط الناقل سلكي او لاسلكي للوصول الى الجميع وبذلك يكون تعميم وسائط النقل هو وسيلة لاستغلال الوقت وزيادة الكفاءة وتغطية عدد اكبر من التطبيقات والمستخدمين والمراسلات في وقت واحد.

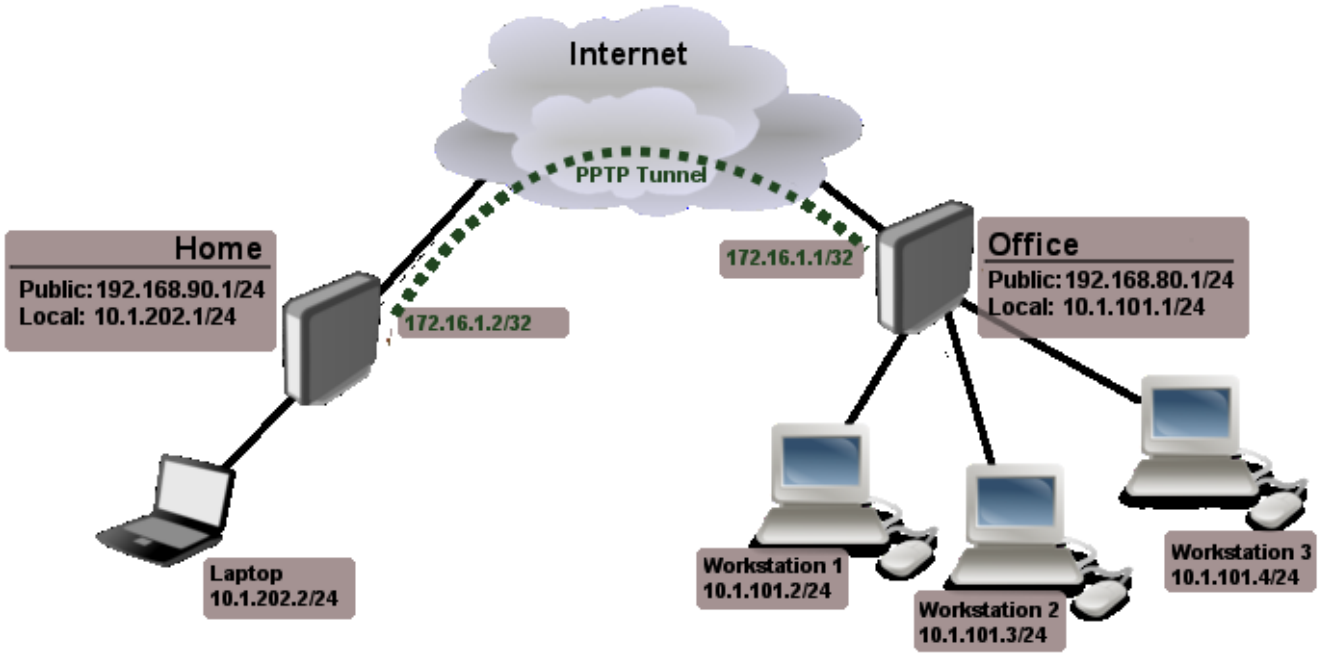
ولكن نفس هذه الميزة الحسنة لزيادة الكفاءة والمرونة والاستغلال لموارد الشبكة جاءتنا بسلبية كبيرة وهي مشكلة الامنية والخصوصية حيث ان المرور المشترك للبيانات يخلق مشاكل في الحفاظ على الامنية ويسهل على المخترقين والمخربين قابلية الوصول الى البيانات الخاصة بأشخاص اخرين الامر الذي يتطلب وجود حلول لهذه المشكلة وقد بدأت الحلول بالظهور مبكراً وتنوعت بين تقسيم الشبكة الى شبكات فرعية او جزئية افتراضي (Virtual Local Area Network VLAN) او شبكات خاصة افتراضية (Virtual Private Networks) وهذا على المستوى السلكي بأستخدام الموجهات (Routers) والمحولات (switches) واما في الوسط اللاسلكي المفتوح فالمشكلة اعقد واكبر لأن البث المتنوع والمتعدد يعتمد على تقسيم حيز الاستلام والاستقبال الى قنوات (channels) متاحة للجميع ويستطيع الجميع وضع جهاز استلام وضبط تردد الاستقبال فيه واستلام كل انواع البث في ذلك التردد ولذلك ظهرت الكثير من الحلول لهذه المشكلة ومن اوائل هذه الحلول هو الاتصال عبر نفق وهمي في الفضاء المفتوح يضمن للمرسل ان المستلم المقصود فقط هو من سيفهم البيانات المرسلة اليه بوضع مفتاح تشفير خاص في جهة الارسال لتشفير البيانات المرسلة بحيث لا يستطيع فهمها وتحليلها الا من يمتلك ذلك المفتاح والذي يقوم

في الطرف الاخر بفك التشفير وارجاع البيانات المستلمة الى صيغتها الاصلية القابلة للفهم وقد سميت مجموعة البروتوكولات التي تدعم هذه الخاصية ببروتوكولات الاتصال من نقطة الى نقطة (Point to Point Protocol PPP) وهو باختصار بروتوكول اتصال بين نقطتين في الشبكة يوفر خاصية التشفير (encryption) والدخول باسم مستخدم وكلمة مرور (Authentication) وضغط البيانات المرسلة (compression) ويستخدم في كل انواع الشبكات تقريباً من الاسلاك التسلسلية وخطوط الهاتف وخطوط النقل الرئيسية (trunk lines) والهواتف الخلوية والالياف الضوئية واتصالات موجات الراديو وابسط تطبيقات هذا النوع هو وسيلة الاتصال الاكثر شيوعاً بين مزودي الخدمة (ISP) والزبائن والمسماة الاتصال واسع النطاق (broadband connection) وفي ادناه اشهر تطبيقات هذا البروتوكول:

١- بروتوكول نقطة الى نقطة عبر الايثرنت (Point to Point Protocol Over Ethernet PPPOE) والذي يوفر قابلية تحكم وادارة كبيرة بالمستخدمين والشبكة وذو فائدة كبيرة لمزودي الخدمة ويعتبر الان هو البروتوكول الاكثر شيوعاً في تزويد خدمة الانترنت من قبل (ISP) للمشتركين عبر الانواع المختلفة من خطوط الاشتراك الرقمي (Digital Subscriber Line xDSL) وخطوط المودم وشبكات الايثرنت الطبيعية ويعتبر هذا البروتوكول هو امتداد للبروتوكول (PPP) الا ان الفرق الوحيد ان هذا البروتوكول يستخدم الايثرنت للأتصال على خلاف البروتوكول الاصلي الذي كان يستخدم الخطوط التسلسلية (serial cables). يستخدم هذا البروتوكول بشكل رئيسي لأدارة اتصالات المستخدمين بواسطة اسم مستخدم وكلمة مرور سواء مع العناوين الثابتة او المتغيرة (Static or DHCP addresses) ويعمل في الطبقة الثانية (data link layer) من مكدس الشبكات ذو الطبقات السبع ويعمل في كافة انواع المحولات (Switches) والجسور (bridges).

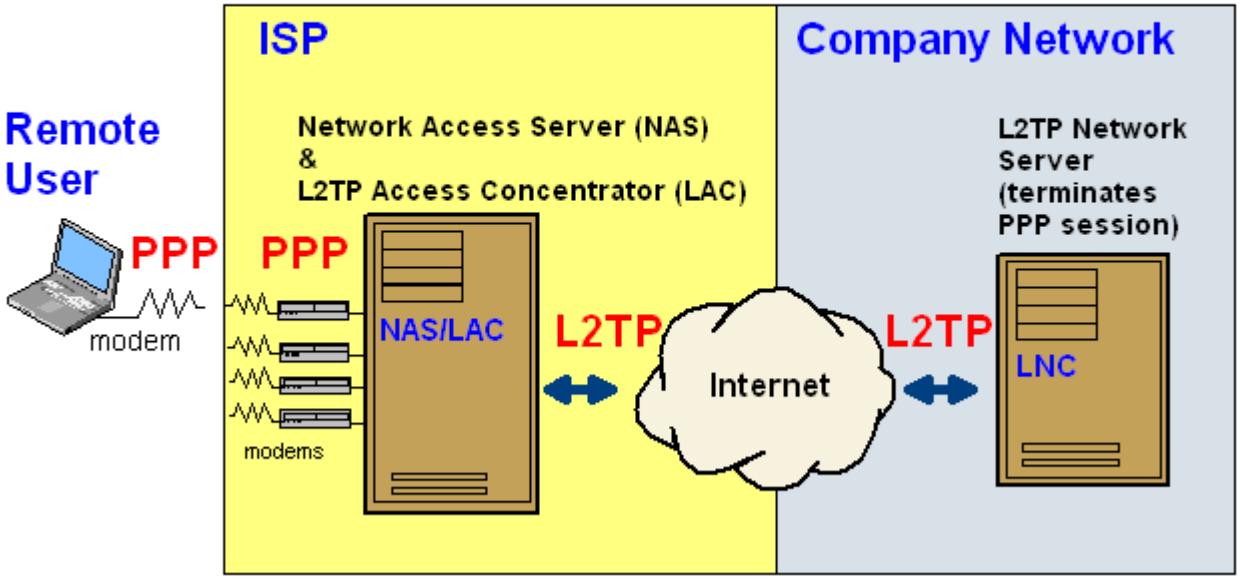


٢- بروتوكول النفق من نقطة الى نقطة (Point to Point Tunnel Protocol PPTP): وهو عبارة عن نفق مؤمن يوفر قابلية ارسال واستقبال البيانات المعنونة ب (IP) عبر PPP حيث يقوم هذا البروتوكول بكبسلة (encapsulation) رزم البيانات وارسالها في رزم (IP). يقوم هذا البروتوكول بدمج كل من ال (PPP) وال (MPPE) وهو تشفير مايكروسوفت من نقطة الى نقطة (Microsoft Point to Point Encryption) لعمل روابط مشفرة والغرض من هذا البروتوكول هو عمل روابط مؤمنة تدار بشكل جيد بين الموجهات في طرف والزبائن للبروتوكول (PPTP) من طرف اخر كذلك بين الموجهات فقط ويتوفر الدعم لهذا البروتوكول في كل نظم التشغيل تقريباً بما فيها الويندوز وله دعم كبير في نظام تشغيل المايكروتك وكما سيرد لاحقاً.

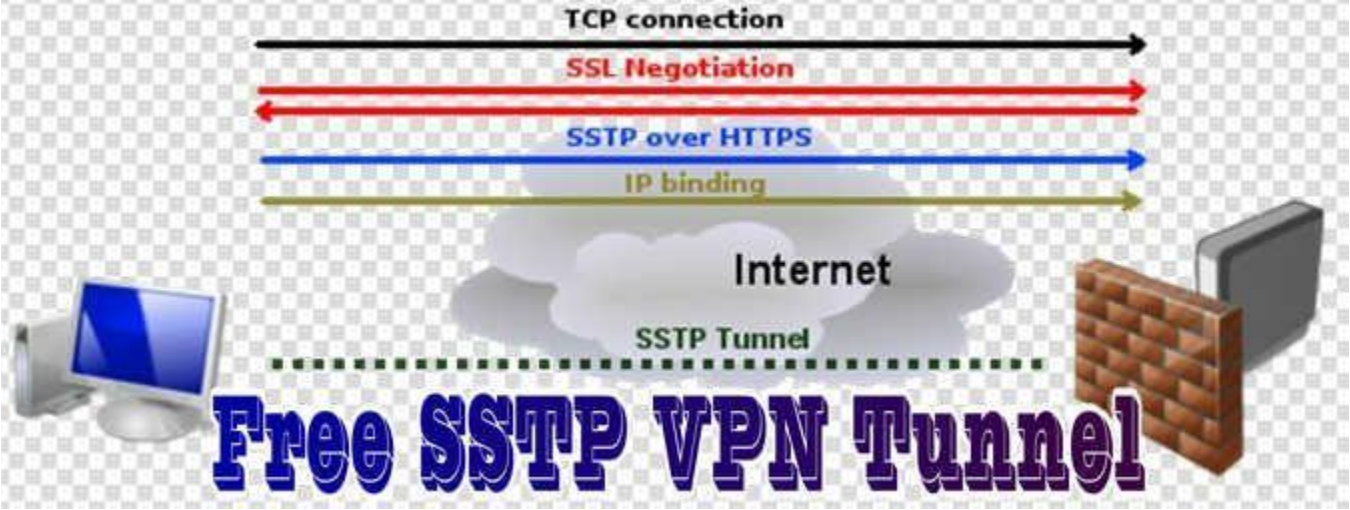


٣- بروتوكول النفق للطبقة الثانية (Layer 2 Tunnel Protocol L2TP): وهو بروتوكول نفقي لدعم الشبكات الخاصة الافتراضية (VPN) او كجزء من ايصال خدمات الشبكة الدولية من قبل ال (ISP) وعلى خلاف البروتوكولات السابقة فأن هذا البروتوكول لا يوفر تشفير او سرية بذاته وانما يعتمد على الية النفق الذي سيقوم بالارسال والاستقبال من خلاله وهو في الحقيقة عبارة عن حصيلة جمع اثنين من البروتوكولات الاقدم وهما بروتوكول سيسكو للتوجيه (Cisco Layer 2 Forwarding Protocol L2F) وبروتوكول ال (PPTP).

From Computer Desktop Encyclopedia
© 2005 The Computer Language Co. Inc.



٤- بروتوكول النفق ذو المقبس الامن (Secure Socket Tunnel Protocol SSTP): ويقوم بنقل نفق النقطة الى نقطة عبر قناة طبقة المقبس الامنة من الاصدار الثالث (Secure Socket Layer SSL 3.0) وبأستخدام المنفذ ٤٤٣ في ال (TCP) مما يجعله يمر افتراضياً عبر كل الجدران النارية وسيرفرات البروكسي. ويتم الاتصال بالخطوات المبينة في الرسم والشرح ادناه:



- بداية يتم انشاء اتصال بين الخادم والزبون عبر المنفذ (TCP 443).
- يقوم ال (SSL) بفحص صحة وثيقة السيرفر (server certificate) واذا كانت صحيحة يكمل اتمام الاتصال والا فأنه يلغيه.
- يقوم الزبون بأرسال رزم التحكم الخاصة بال SSTP عبر جلسة (HTTPS) والتي تؤسس ماكنة حالة (state machine) في كل من طرفي الاتصال (الخادم والزبون).
- تحصل حالة نقاش بين ال (PPP and SSTP) ويتم الزام العنوان (IP binding) لواجهة ال (SSTP).
- والان اصبحت قناة ال SSTP جاهزة ومعدة ويمكن تغليف وكبسلة الرزم من البيانات وبدء ارسالها.

والان نصل الى زبدة الموضوع وهي كيفية دعم كل هذه البروتوكولات في اجهزة مايكروتك؟ والجواب على ذلك في ثلاث حروف (BCP):

نعم انه بروتوكول التحكم الجسري (Bridge Control Protocol) وهو البروتوكول المدعوم من قبل نظام تشغيل راوترات المايكروتك (MikroTik RouterOS) ويسمح بعبور بيانات الايثرنت عبر رابط PPP ويكون تكوين هذا البروتوكول جزء مستقل من نفق ال PPP وغير مرتبط بأي عنوان IP او واجهة نقطة لنقطة وباختصار يسمح هذا البروتوكول لعمليتي ال (Bridging and routing) لتحصل في نفس الوقت بشكل مستقل واما اعدادات هذا البروتوكول في ال(winbox) فستكون محور درسنا القادم ان شاء الله.

اعداد وتنظيم وشرح وتوضيح : مصطفى صادق لطيف – العراق – ميسان

للمزيد زوروا الموقع الرسمي : WWW.MUSTAFASADIQ0.WORDPRESS.COM

انتظروا بقية الدورة في الجزء الثاني قريباً ان شاء الله