الدليل الشامل لإدارة الشبكات الصغيرة والمنزلية باستخدام جهاز ال (TP-Link)

يعتبر ال (TP-Link) واحداً من أكثر الأجهزة للشبكات الصغيرة والمنزلية شيوعاً لما يوفره من رخص ثمنه وسرعته العالية وامكانيات التحكم والأمان الكبيرة نسبة الى سعره والمرونة في قابلية الوصول والتحكم به بواجهات رسومية ونوافذ سهلة التعامل معها وكذلك التنصيب البسيط لمكوناته وخصائصه لخدمة الزبون في دائرة صغيرة او في المنزل.
تجدر الإشارة الى ان هذا الجهاز تتوفر منه الكثير من الإصدارات والانواع المتعددة التي تختلف الى حد ما في امكانياتها الشبكاتية فبعضها يحتوي هوائي واحد وبعضها اثنين او ثلاثة ولكن واجهاتها الرسومية ونوافذ اعدادها التي سنقوم بشرحها هي نفسها لكل الأنواع مع اختلافات بسيطة تبعاً لعدد المنافذ السلكية واللاسلكية والعدد الأعلى للأجهزة المسموح بإضافتها الى الشبكة وفي ادناه صورة مختصرة لعدد من أنواع هذا الجهاز:

خصائص راوتر ال (TP-Link) اللاسلكي:
يجمع هذا الجهاز خصائص عدة أجهزة شبكات في نفس الوقت فهو يقوم بوظيفة الربط بين شبكتين مختلفتين في العناوين والمديات مما يجعله يعمل كموجه (router) ويقوم بعملية توزيع الخطوط الى أجهزة سلكية كسويتش (switch) ويقوم ببث الشبكة الى أجهزة لاسلكية مما يجعله يقوم بدور نقطة الوصول (access point) ويقوم ايضاً بتوفير وظيفة الجدار الناري ومتحكم الوصول وسيرفر ال (RAID) وغيرها الكثير مما يلخصها النقاط التالية:

١- يدعم كل بروتوكولات الاتصال اللاسلكي ضمن المقياس (IEEE 802.11, a, b, g, n) او ما يسمى اختصاراً (WIFI) وبمعدل نقل بيانات يصل الى ٣٠٠ ميكا بت بالثانية.
٢- منافذ سلكية لشبكات ال (WAN،LAN) وبسرعات تصل الى ١٠٠ ميكا بت بالثانية.
٣- قابلية الامن والتشفير وبعدة بروتوكولات.
٤- قابلية الوصول الى الانترنت وانشاء شبكة داخلية بين مستخدميه.
٥- دعم الخادم الافتراضي والتوجيه الثابت (static routing) وتطبيقات خاصة بال (DMZ).
٦- دعم ال (Dynamic DNS).
٧- توفير الاتصال التلقائي او الاتصال المبرمج بالإنترنت في أوقات محددة.
٨- توفير وظائف ال (NAT, DHCP) داخلياً وتوزيع العناوين (IP) على المستخدمين بشكل تلقائي.
٩- دعم الشبكة الخاصة الافتراضية (VPN).
١٠- توفير الرقابة الابوية والتحكم بالوصول.

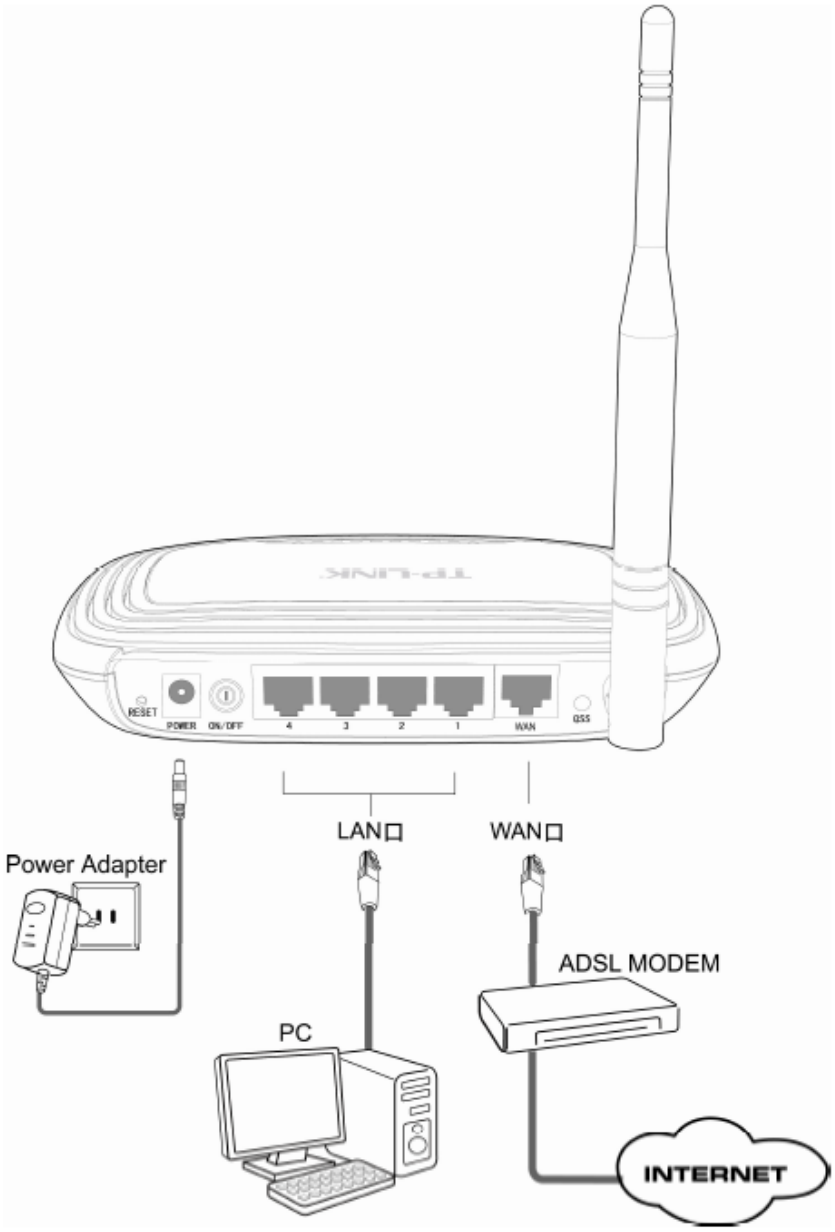
١١ـ التشفير اللاسلكي باستخدام بروتوكولات ومفاتيح (٦٤/١٢٨/١٥٢-bit WEP).
١٢ـ توفير احصائيات وقياسات للمرور.
١٣ـ توفير قابلية التحديث لنظام تشغيله (firmware) والتحكم عن طريق واجهة ويب.
١٤ـ قابلية إضافة جهاز ذو مواصفات خاصة بخاصية (unpn).

الشكل العام للجهاز ومكوناته الخارجية:

يحتوي الجهاز على مجموعة من الازرار والمقابس والدايودات الباعثة للضوء (Light Emitting Diodes LED) التي تشير الى حالة المنافذ السلكية واللاسلكية وكذلك زر الطاقة (power switch) للتشغيل والاطفاء وزر (QSS) لأضافة جهاز لاسلكي يدعم التنصيب الامن (wireless device with WIFI protected setup) وكذلك زر إعادة الضبط (reset) والذي عند النقر عليه لدقيقتين يقوم بأرجاع الجهاز الى ضبط المصنع الخاص به ويفقد كل اعدادات جديدة قام المستخدم بضبطها.

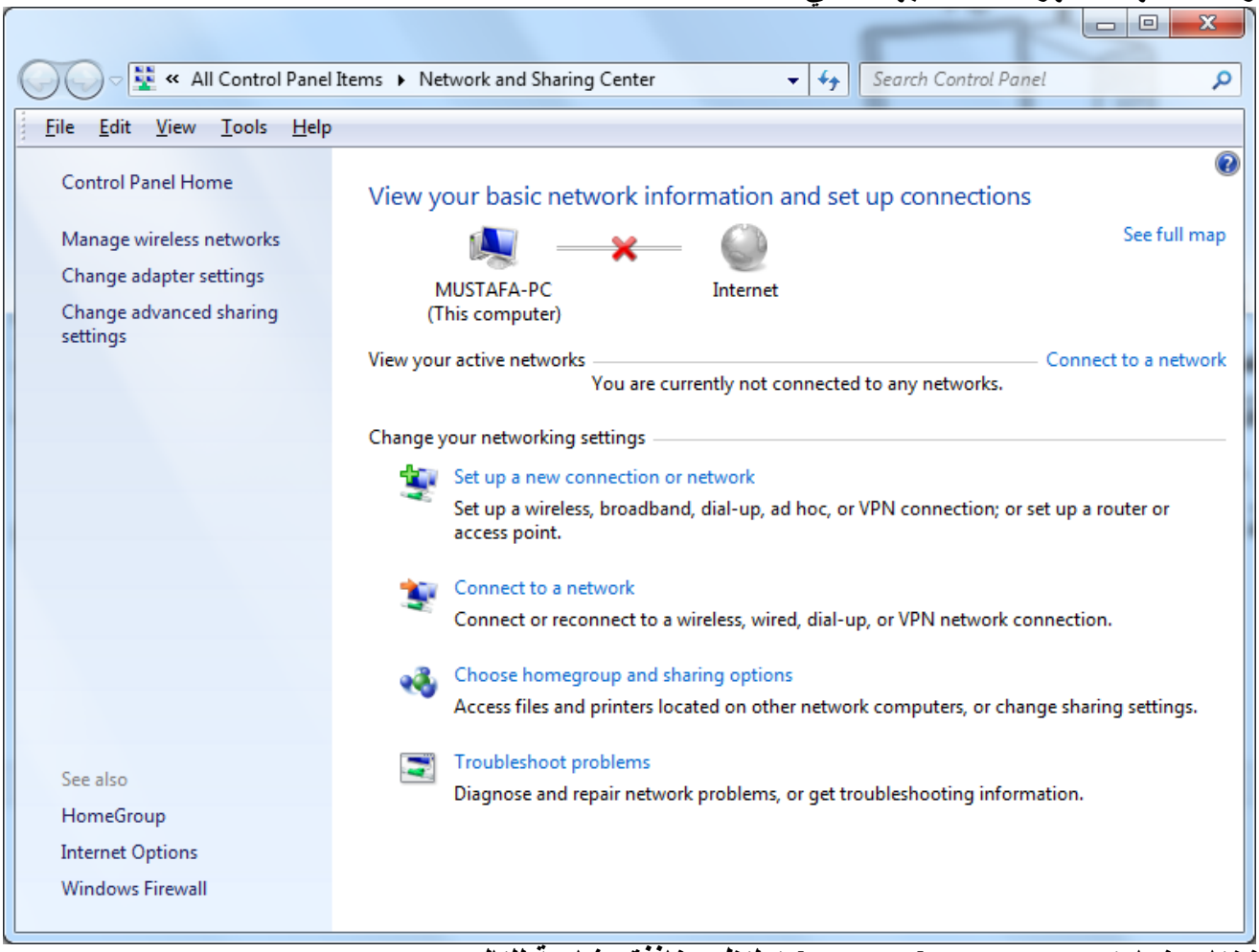
ضبط الجهاز لأول مرة:

بعد ربط الجهاز الى الهوائي (nanostation) او (mikrotik) او أي جهاز اخر يربط الشبكة المحلية او المنزلية بمزود الخدمة (ISP) وربط باقي مكونات الجهاز مثل الاسلاك وكيبل الطاقة كما في الصورة التالية:

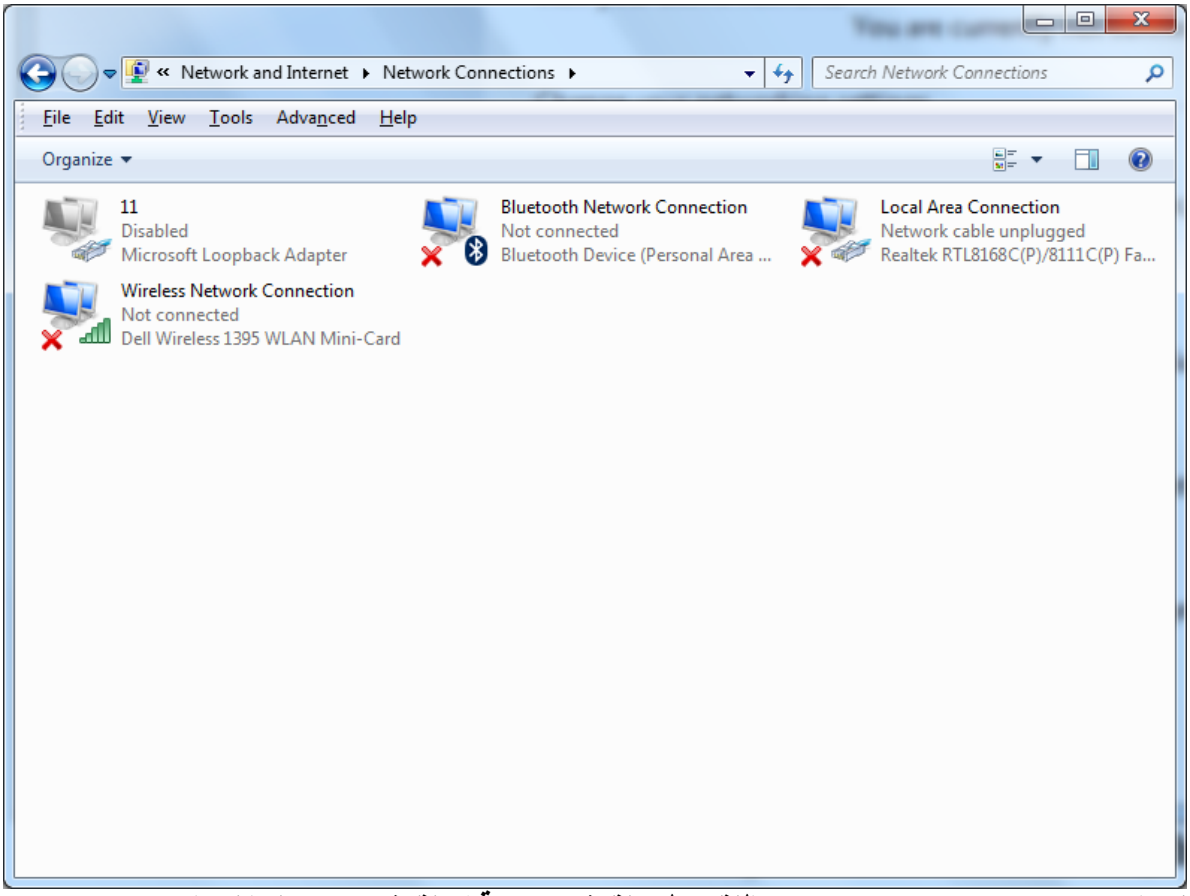


وكما نرى نربط محول الطاقة والاسلاك من نوع (RJ-45) للشبكة السلكية المحلية (LAN) ونربط السلك القادم من الهوائي الى منفذ الشبكة العالمية (WAN) تماماً كما في الريم أعلاه ونقوم بتشغيل الجهاز ونربط اليه جهاز حاسوب على أحد المنافذ

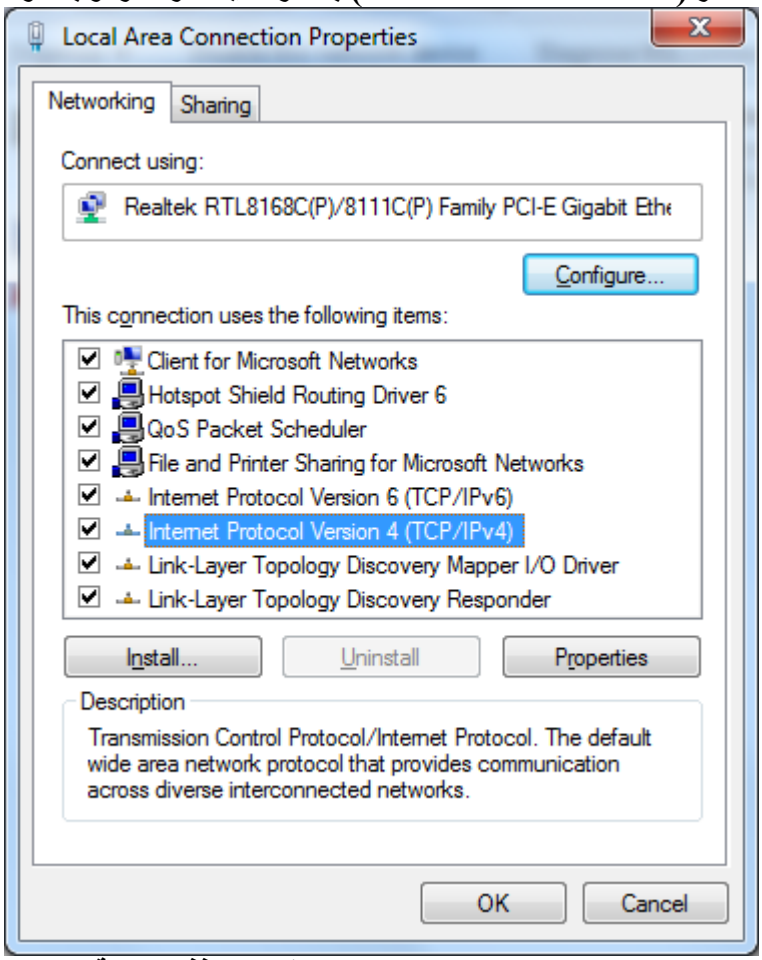
السلكية وقبل البدء بأعداد الجهاز توجد عدة خطوات يجب القيام بها في الحاسوب الشخصي الذي سيستخدم في ضبط اعدادات الجهاز حيث يجب ان نجعل الجهاز يستقبل عناوينه من الراوتر لكي يستطيع الاتصال به ويتم ذلك بأتباع الخطوات التالية:
نذهب الى قائمة البدء (start) ثم الى لوحة التحكم ((control panel ومنها نختار (network and sharing center
وعند فتحها ستظهر نافذة مشابهة للتالي:



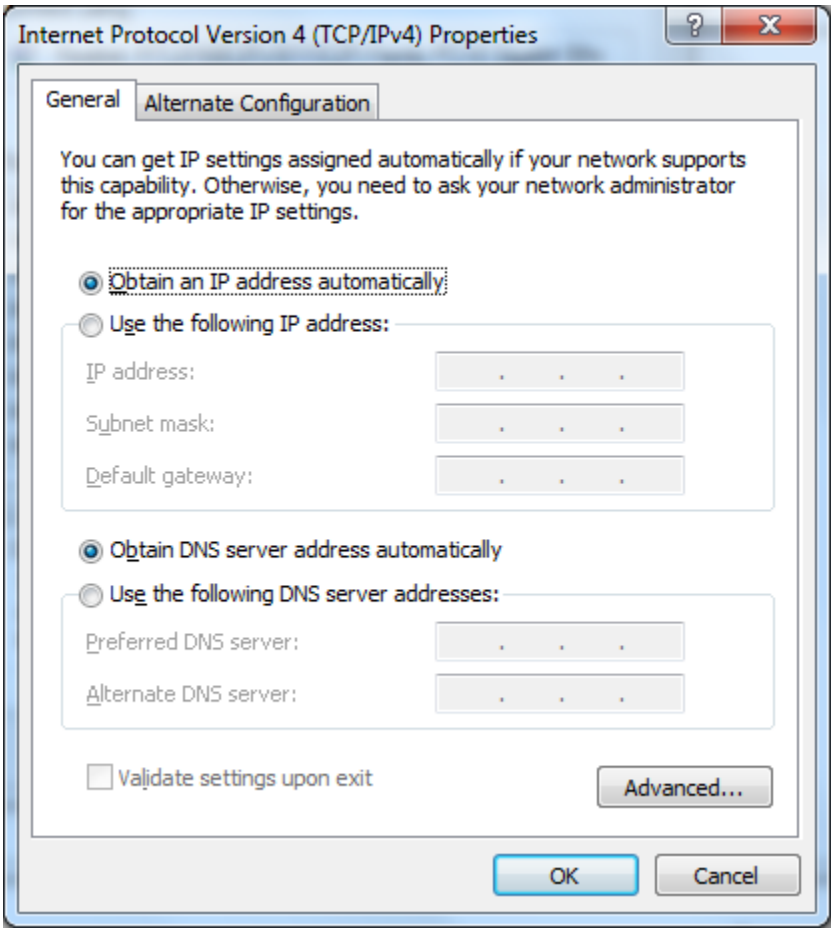
نختار منها (change adapter settings) لتظهر نافذة مشابهة للتالي:



نختار (local area connection) بالنقر عليه نقرة مزدوجة او نقرة يمين ومنها نختار (properties) لتظهر النافذة التالية:



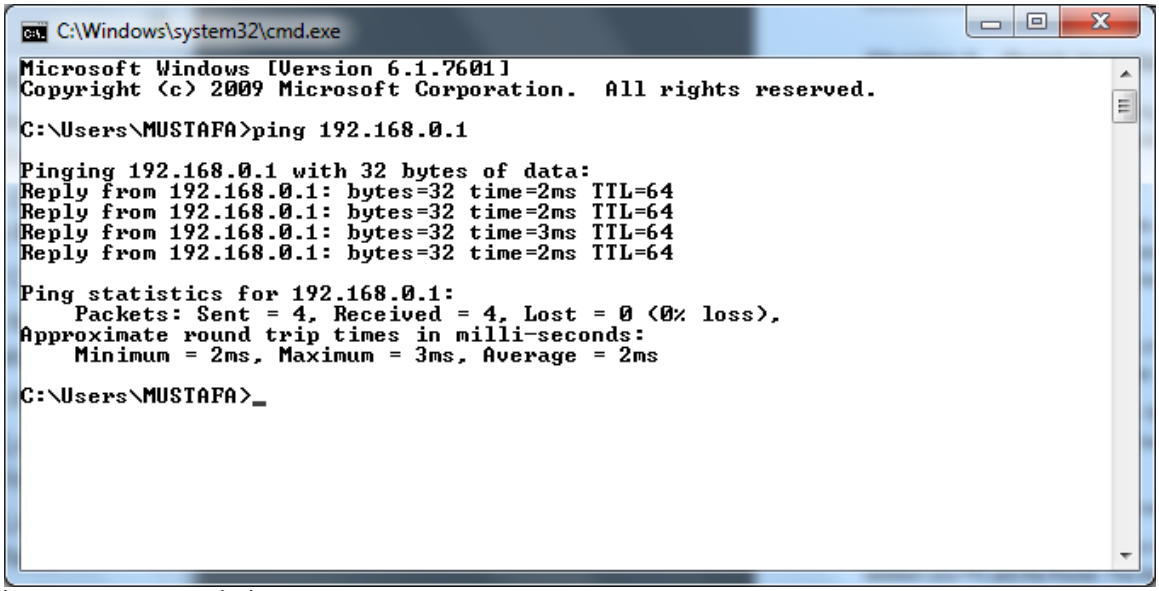
نختار منها ما مؤشر بالنقر المزدوج لتظهر النافذة التالية:



نختار منها (obtain my IP address automatically) ثم (ok) وهكذا انتهت خطوات اعداد الحاسوب ليكون متهيئاً للاتصال بالراوتر وضبط اعداداته وهو ما سنتناوله في الدرس القادم.

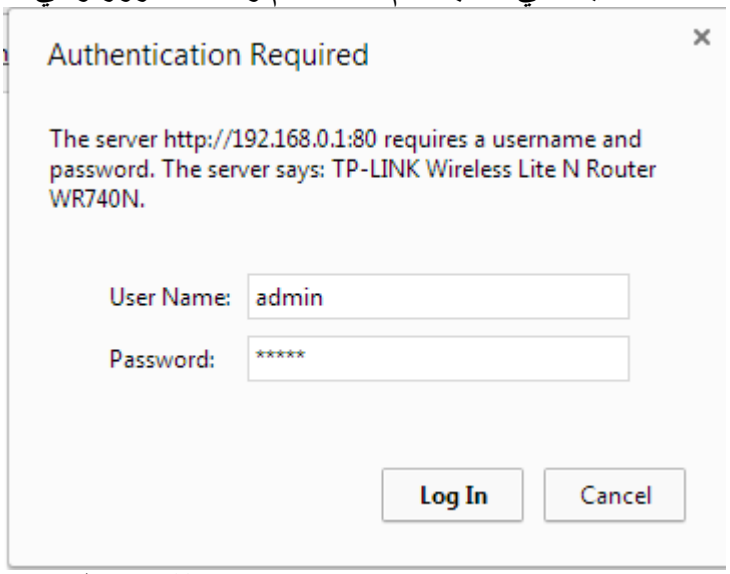
الدرس الثاني:

وصلنا في الدرس الأول الى ربط الحاسوب الشخصي الخاص بنا الى الراوتر (TP-link) بكيبل من نوع (RJ-45) وهو احد مرفقات الجهاز في العلبة التي يتم شحنه بها وبعد ان ضبطنا اعدادات الحاسوب ليستلم عناوين ال (IP) من الراوتر بشكل تلقائي نأتي الى مرحلة ضبط اعدادات الراوتر وهناك عدة طرق منها ما سنشرحه الان ويسمى الضبط السريع (quick installation**) وتبدأ بفحص الاتصال بين الحاسوب والراوتر الذي يكون عنوانه التلقائي (192.168.0.1) فندخل الى قائمة البدء (Start) ومنها نختار زر التنفيذ (run) ونكتب بداخله (cmd) لفتح محرك الايعازات في الشاشة السوداء التي تشبه واجهة الدوز ونكتب الايعاز التالي (ping 192.168.0.1) لفحص اتصال حاسوبنا بالراوتر فأن كانت النتيجة كما في النافذة التالية فهذا يعني ان الاتصال متحقق:**

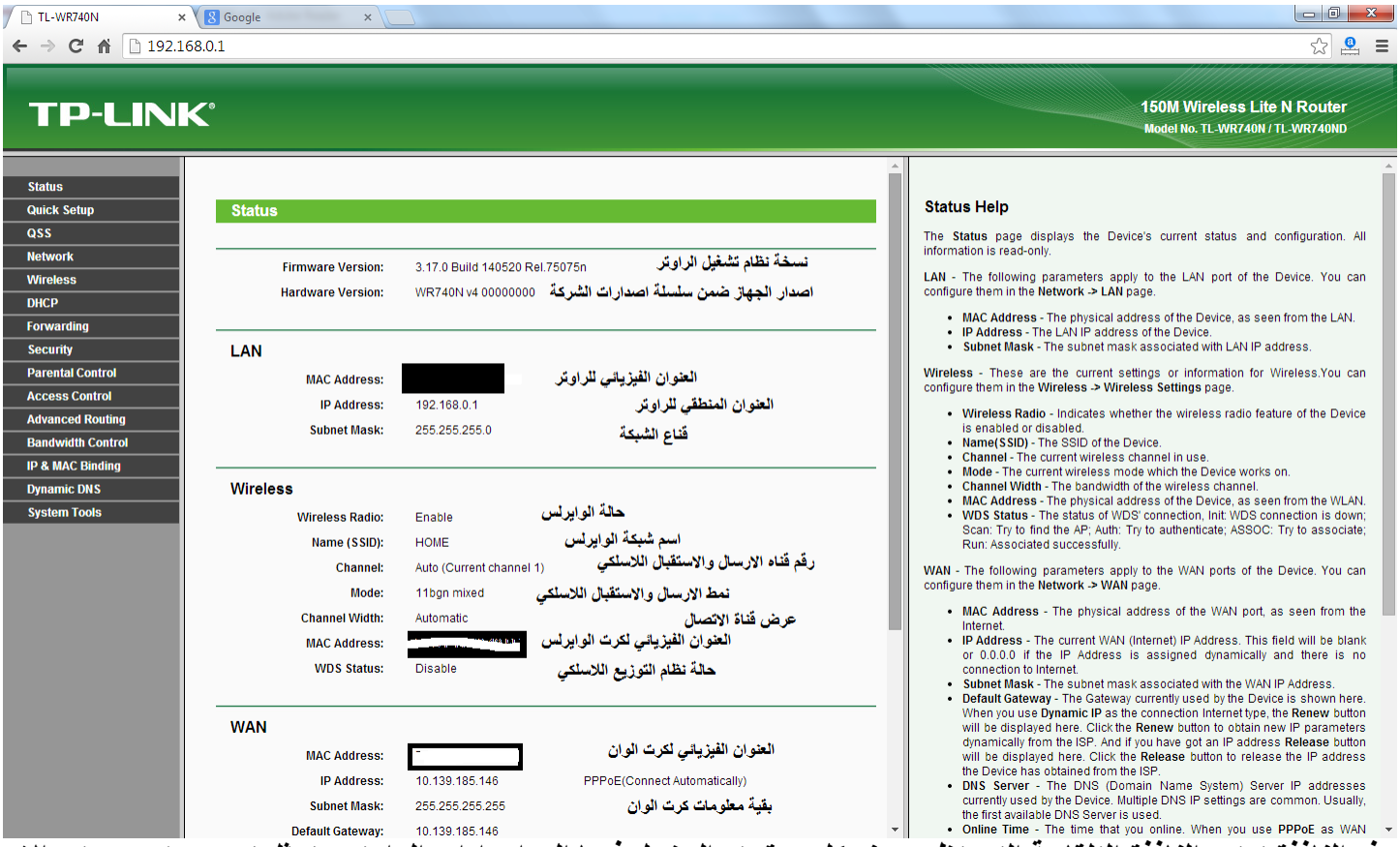


واما ان ظهرت لنا (request time out) **او** (destination unreachable) **فهذا يعني وجود خلل في الاتصال بين الحاسوب والراوتر ويجب إعادة الدرس الأول وضبط الاعدادات كما ذكر هنا ثم البدء من جديد.**

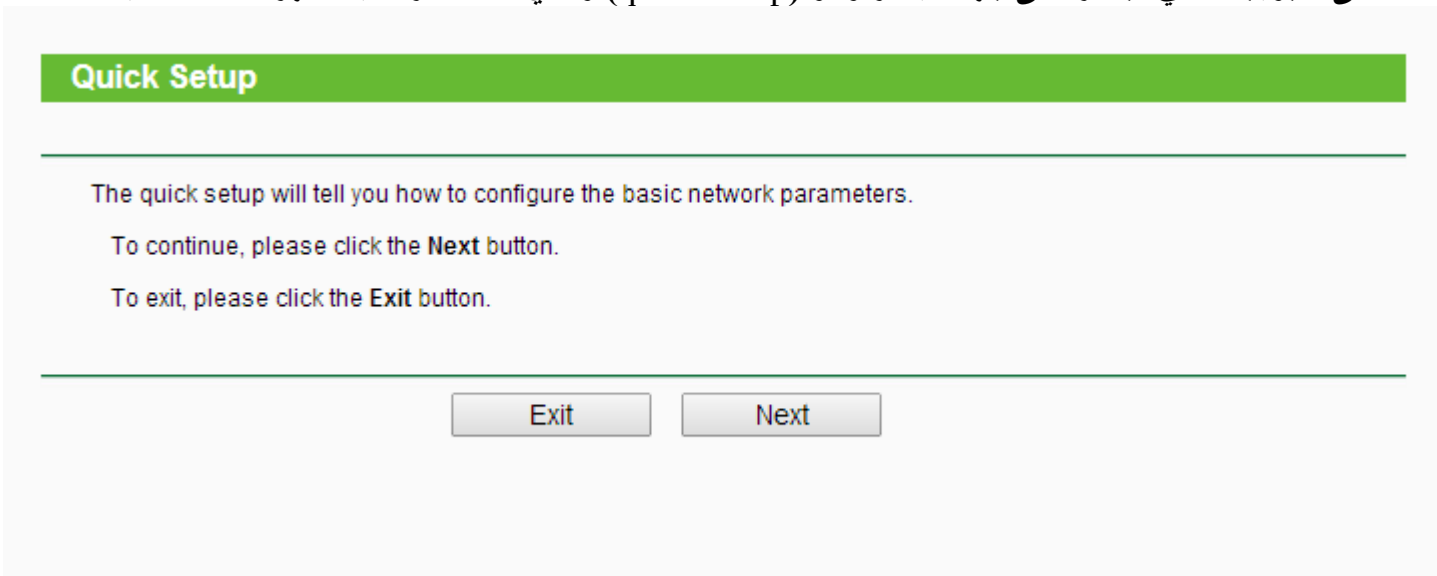
بعد ان تأكدنا ان جهازنا قادر على الاتصال بالراوتر نقوم بفتح متصفح الانترنت (Mozilla Firefox، internet explorer، google chrome, opera, …) **او أي متصفح اخر ونكتب في شريط العنوان عنوان الراوتر** (192.168.0.1) **لتظهر النافذة التالية التي تطلب اسم المستخدم وكلمة المرور وهي تلقائياً قبل أي ضبط** (Admin) **لكليهما:**



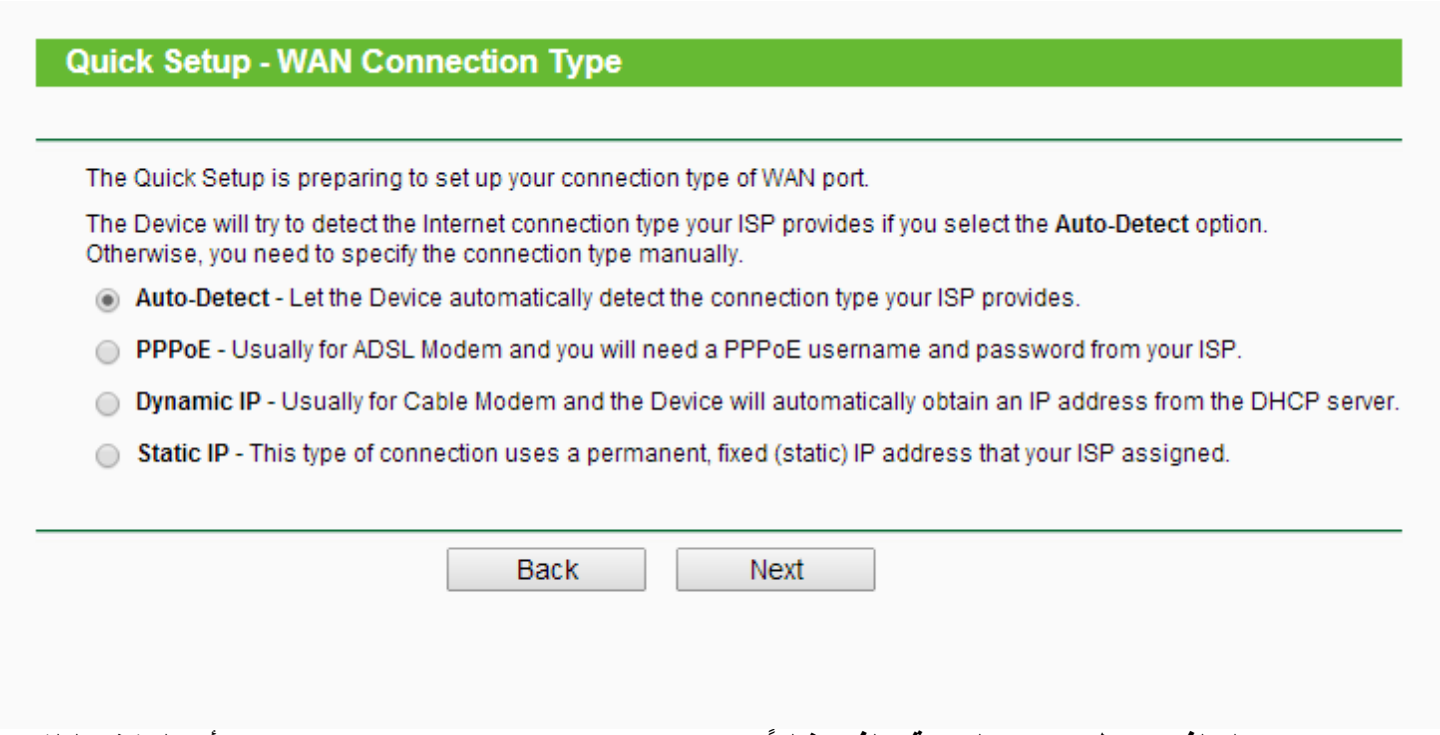
وبعدها وعند النقر على (log in) **ستظهر النافذة التالية:**



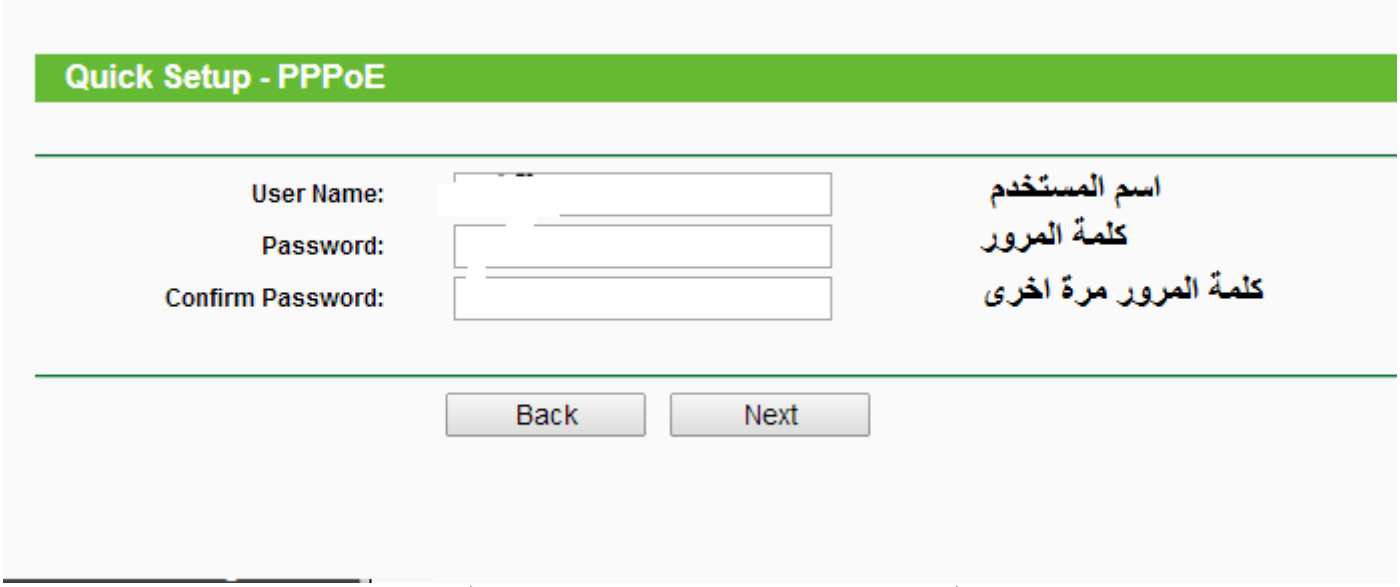
هذه النافذة تعتبر النافذة التلقائية التي تظهر عند كل مرة يتم الدخول فيها الى اعدادات الراوتر وتمثل تبويب (status) والان ننتقل الى التبويب الثاني مباشرة الى جهة اليسار وهو (quick setup) والذي عند النقر عليه تظهر النافذة التالية:



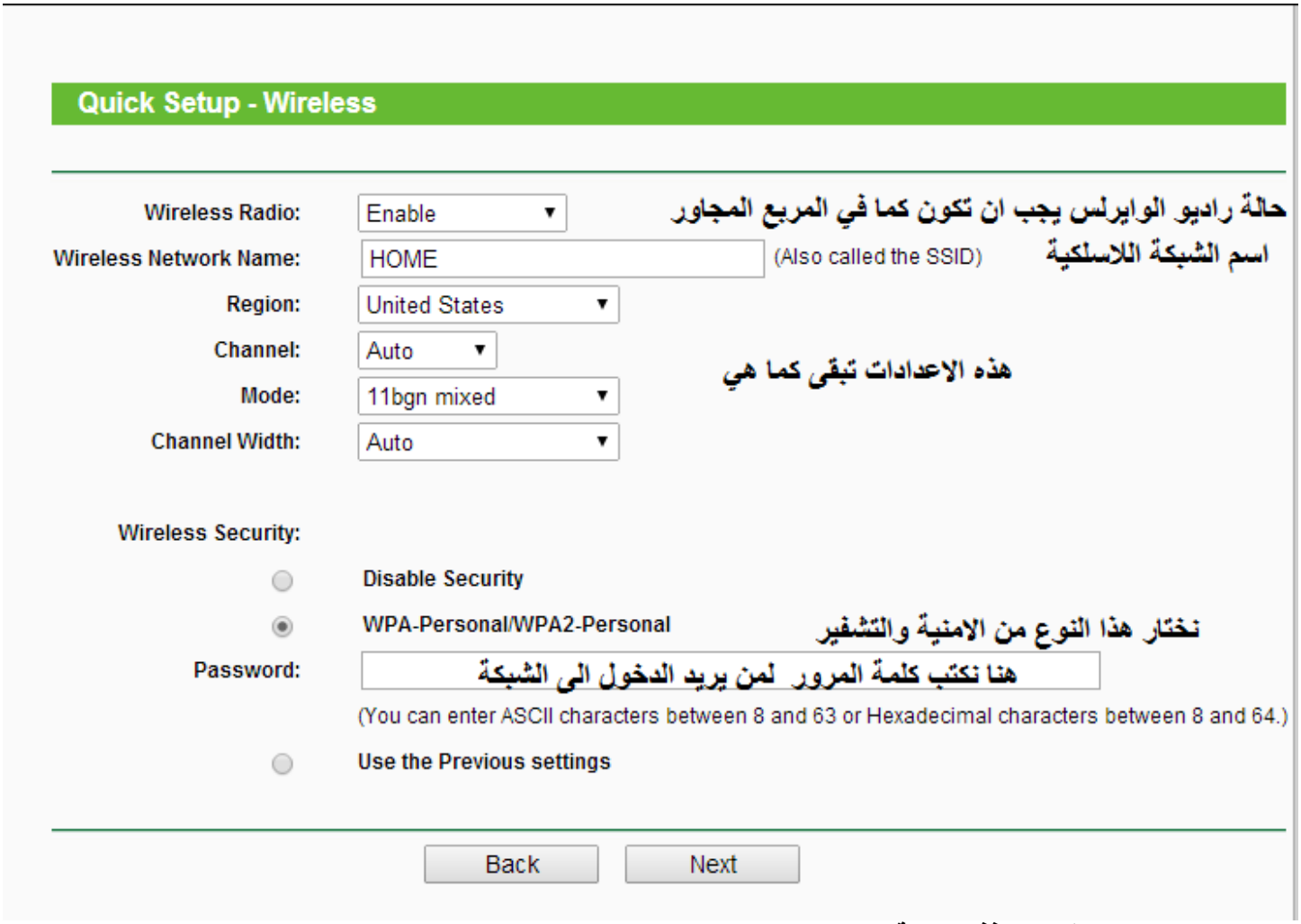
ننقر على (next) لتظهر النافذة التالية:



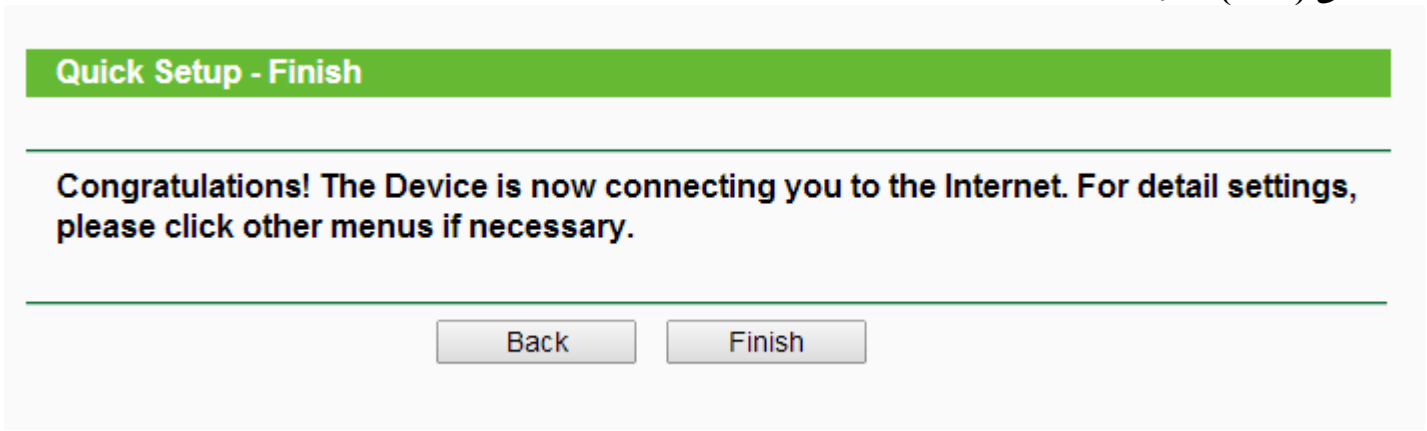
نختار نوع الاتصال الذي يربطنا بمزود الخدمة والذي غالباً ما يكون (PPPOE) او نختار (auto detect) أي الكشف التلقائي لنوع الاتصال علماً ان الراوتر في هذه الحالة يجب ان يكون متصلاً عن طريق منفذ ال (WAN) بالهوائي (antenna) من نوع (nanostation, picostation, mikrotik, …) وعند النقر على (next) تظهر النافذة التالية:



وهنا نقوم بإدخال اسم المستخدم وكلمة المرور التي حصلنا عليها من مزود خدمة الانترنت ثم ننقر على (next) لتظهر النافذة التالية:



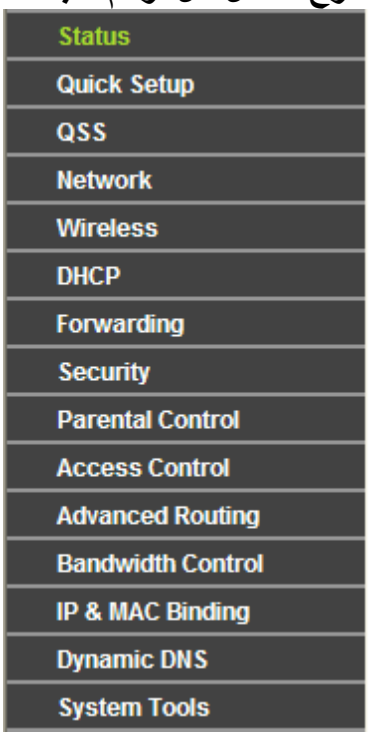
ننقر على (next) لتظهر النافذة التالية:



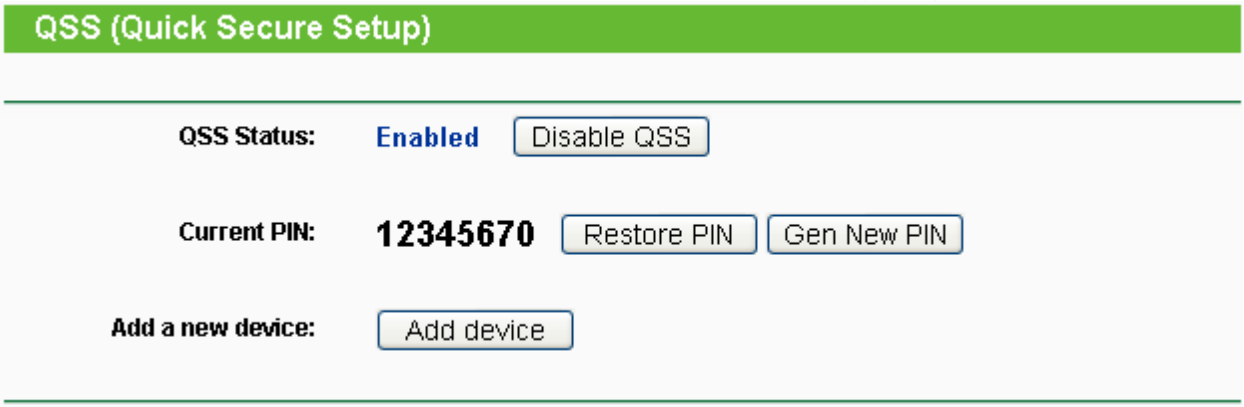
وهكذا نكون قد أنهينا اعداد الراوتر للاتصال بالإنترنت وتوزيع الانترنت على المشتركين في الشبكة المنزلية او الصغيرة.

الدرس الثالث من دورة إدارة الشبكة المنزلية

بعد ان استعرضنا الخصائص الرئيسية لراوتر ال (TP-link wireless) والضبط السريع له في الدرسين السابقين نصل الى شرح مفصل لكل قوائم ضبط الموجه وهي ١٥ قائمة كما في الشكل التالي:



وقد قمنا بشرح اول قائمتين منهما وهما قائمة الحال (status) وقائمة الضبط السريع (quick setup) ونصل اليوم الى شرح قائمة الضبط الأمن السريع (Quick Secure Setup QSS) وتمكننا هذه القائمة من إضافة جهاز لاسلكي الى الشبكة بشكل سريع ويتم ذلك بعدة طرق سأشرح ابسطها واترك للقاري اللبيب استكشاف البقية في جهاز موجه الشبكة المنزلية الخاص به. عند النقر على تبويب (QSS) تظهر النافذة التالية:



وكما هو واضح من عناوين الازرار والقيم فأن معانيها كما يلي:

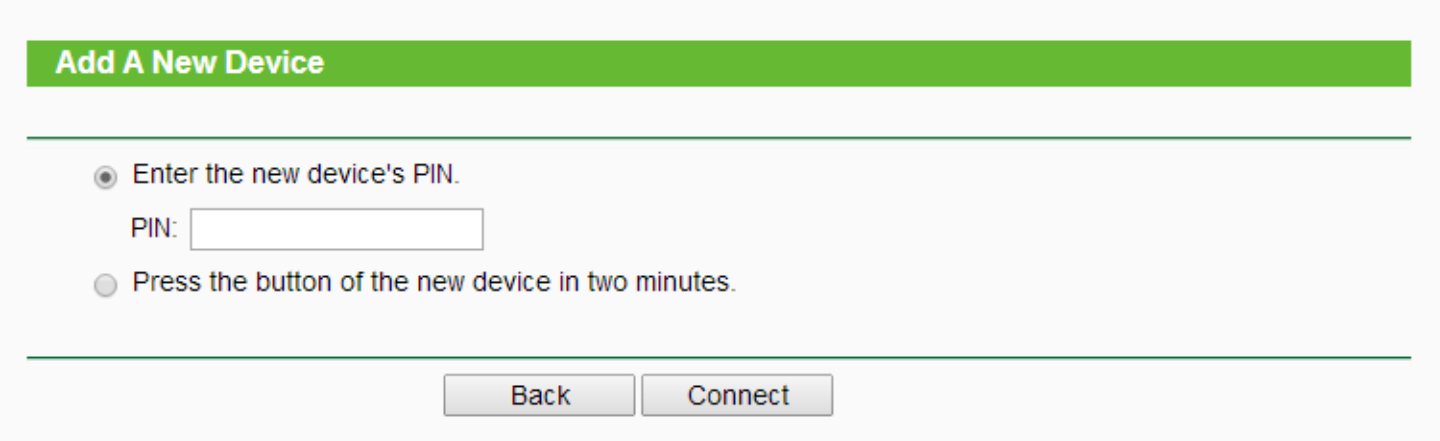
١- (QSS status): وهي حالة الضبط الامن السريع حالياً ويمكن ان تكون (تمكين enable) او منع (تقنين disable).

٢- (current PIN): وهو قيمة المفتاح الحالي الذي يعتبر بمثابة كلمة المرور للانضمام الى الشبكة بحسب هذا الضبط ويمكن انشاء رمز (PIN) جديد من زر (Gen New PIN) او استعادة الرمز الأصلي بالنقر على (Restore PIN).

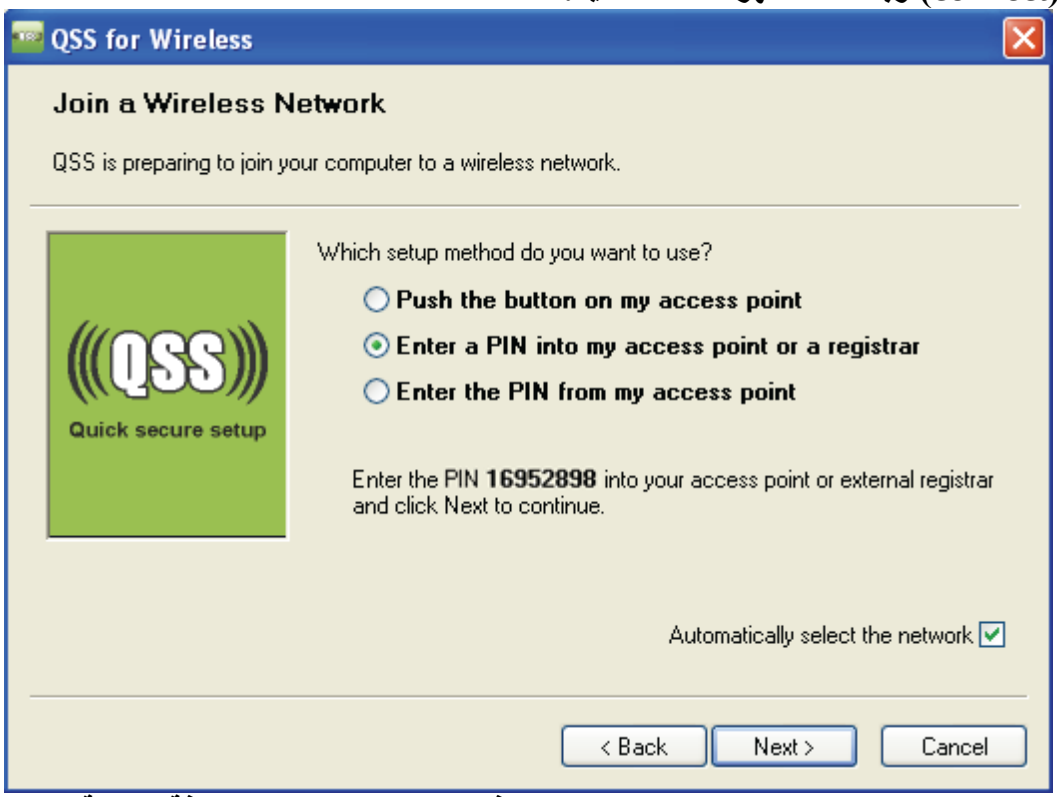
٣- (Add new Device): وتعني إضافة جهاز جديد وهو الزر الذي سأعتمده في الشرح وكما في ادناه:

ملاحظة: توجد أجهزة نقال او هواتف ذكية لا يمكنها الانضمام الى الشبكة بإدخال الكلمة السرية للشبكة فقط لأنها لا تدعم نفس بروتوكول الاتصال (WIFI) الذي يدعمه الراوتر وهذه الأجهزة تحتوي رمز (PIN) معروف بالنسبة للجميع وهو ما يتم طلبه من صاحب الجهاز حين يحاول إعادة ضبط الجهاز او تغيير اعداداته وهو ما سنستخدمه في شرحنا هذا.

الان نبدأ: عند النقر على زر (add new device) تظهر النافذة التالية:

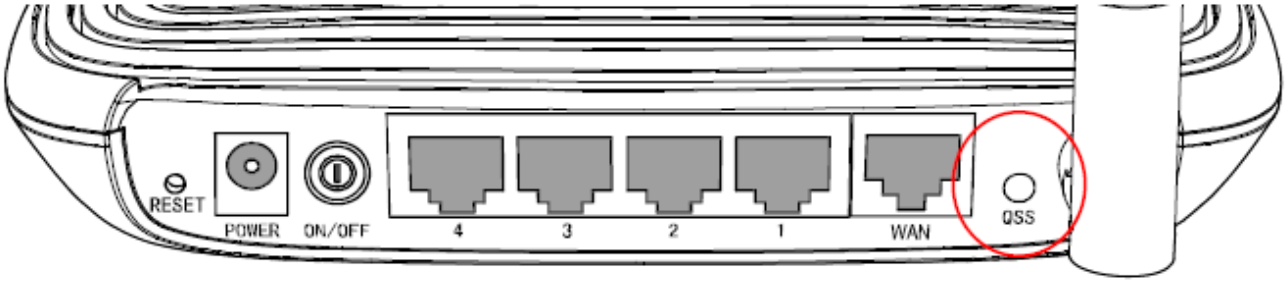


هنا لدينا خيارين وهما اما ان ندخل رمز (PIN) الخاص بالجهاز وهو رقم يتكون من ٨ مراتب وبالنسبة للأجهزة القديمة التي لا تدعم ال (Wi-Fi) فيكون عادة أربع مراتب يمكن تغييره ثم ادراجه هنا لإضافة الجهاز الى الشبكة ثم النقر على (connect) وبعدها ستظهر النافذة التالية:

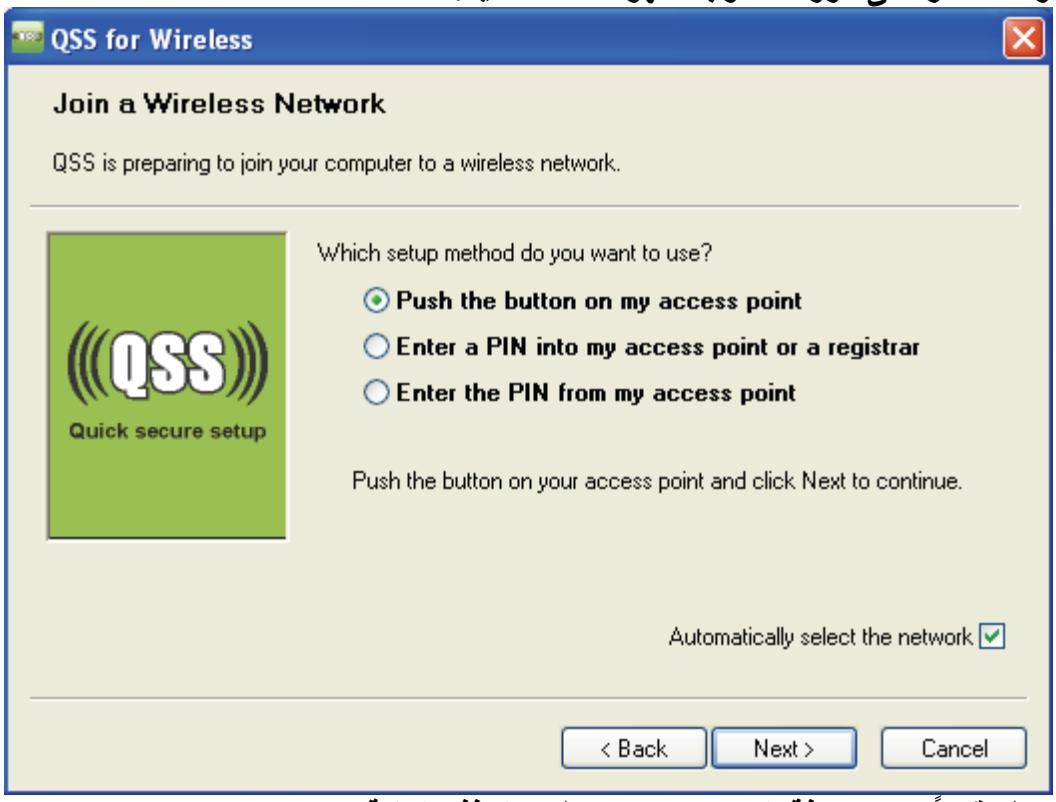


نختار كما هو مؤشر وننقر على (next) والان نذهب الى الجهاز لنرى إضافة الشبكة المنزلية الخاصة بنا الى جهات الاتصال في متصفح انترنت النقال او الجهاز اللاسلكي القديم.

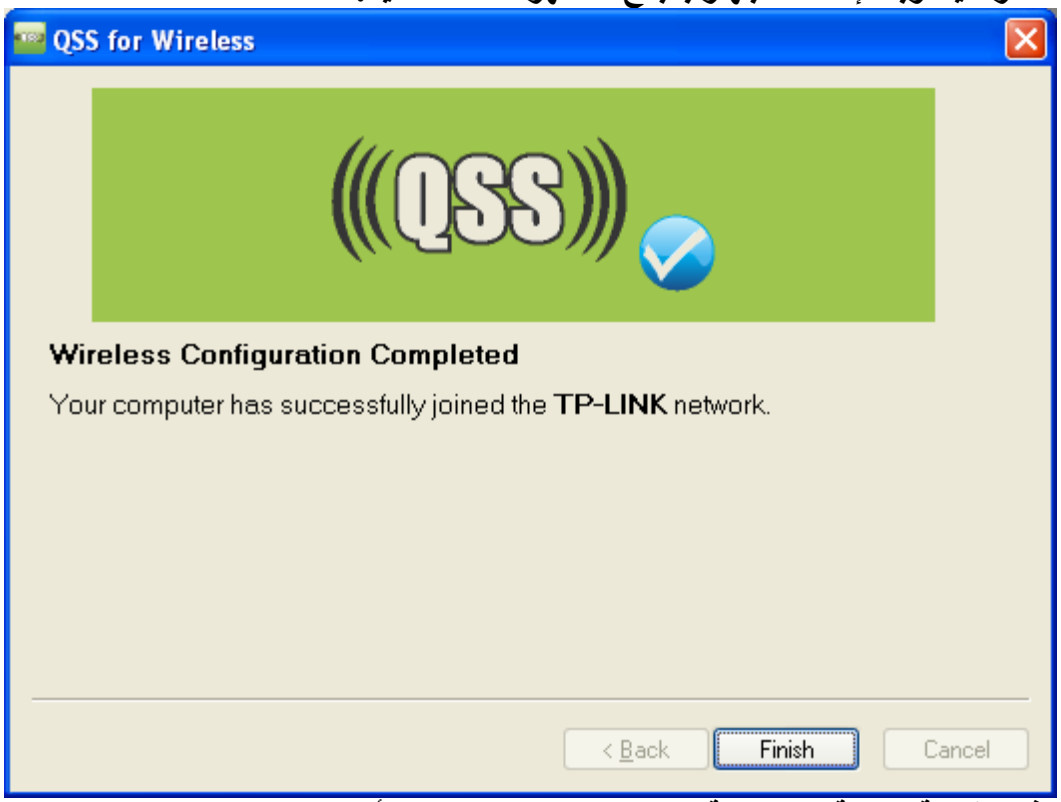
اما الخيار الاخر فيتمثل باختيار (press the button….) فعند اختياره يجب النقر على زر (QSS) في الجهاز المراد اضافته وذلك النقر على زر (QSS) في جهاز الراوتر الخاص بنا في نفس الوقت وبحدود دقيقتين بعد اختيار الخيار الثاني حيث ان هذا الزر موجود في خلفية الجهاز كما يلي:



وعند النقر على الزر المطلوب تظهر النافذة التالية:



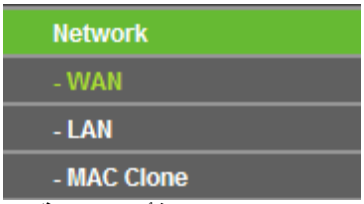
ننتظر قليلاً وبعد إضافة الجهاز بنجاح ستظهر النافذة التالية:



هذه الطريقة مجربة ومضمونة وسيعمل الجهاز اللاسلكي كأنه يحتوي (Wifi) ويتصفح الانترنت بشكل طبيعي وبدون التداخل مع الإشارة الخاصة بالاتصال الخلوي وبدون التأثير على الرصيد وكما اشرت فهناك الكثير من الخيارات والطرق لعمل ذلك الا اني اخترت اكثر طريقتين اختصاراً وسهولة وان شاء الله يتم التنفيذ بنجاح ولكن الحذر عند التعامل مع رمز ال (PIN) فأن تغييره بشكل غير صحيح او نسيانه يسبب مشاكل للجهاز.

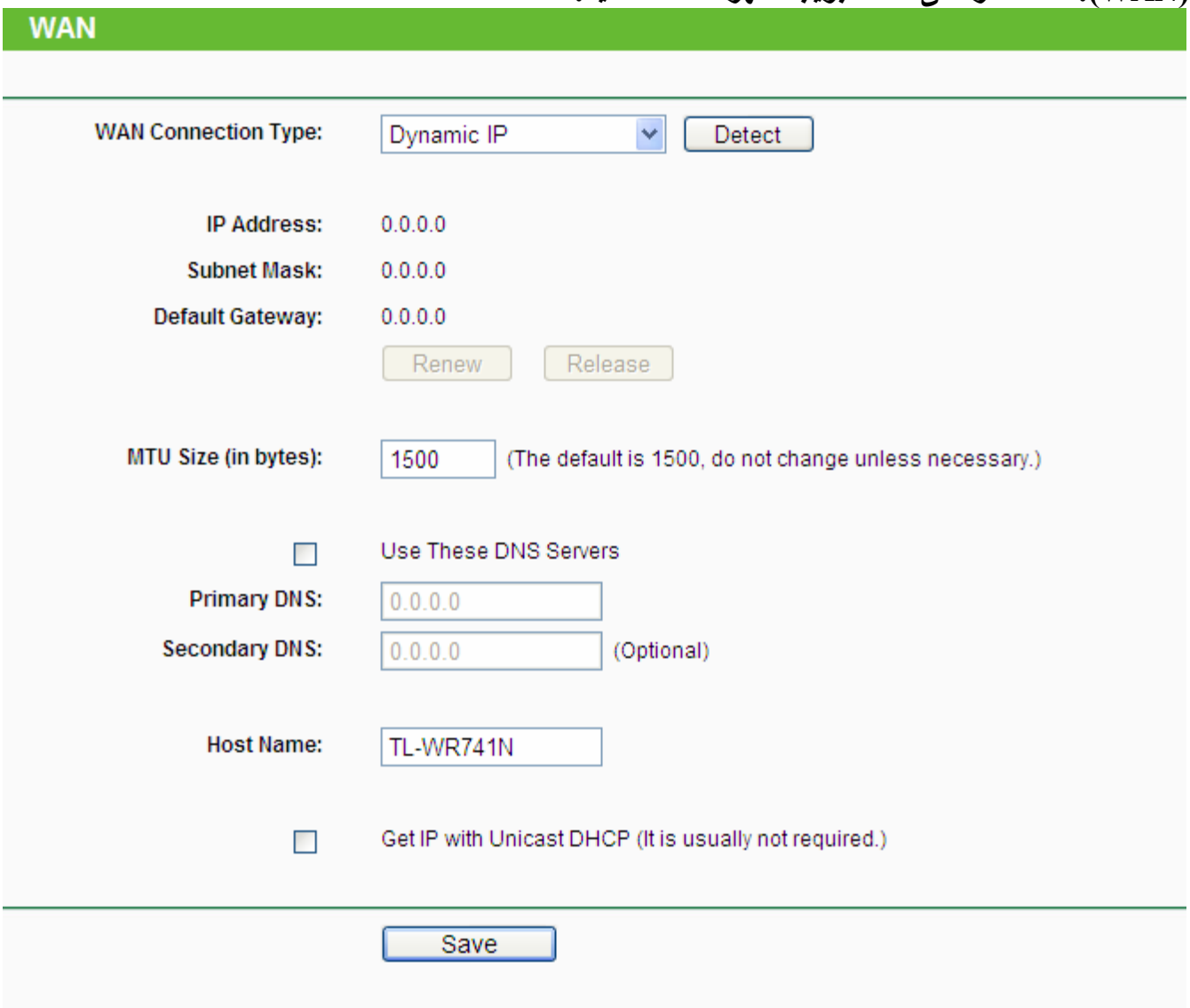
الدرس الرابع من دورة إدارة الشبكة المنزلية

وصلنا اليوم الى شرح قائمة (Network) ضمن سلسلة قوائم جهاز ال (TP-LINK wireless router) والتي عند النقر عليها تظهر الخيارات التالية:



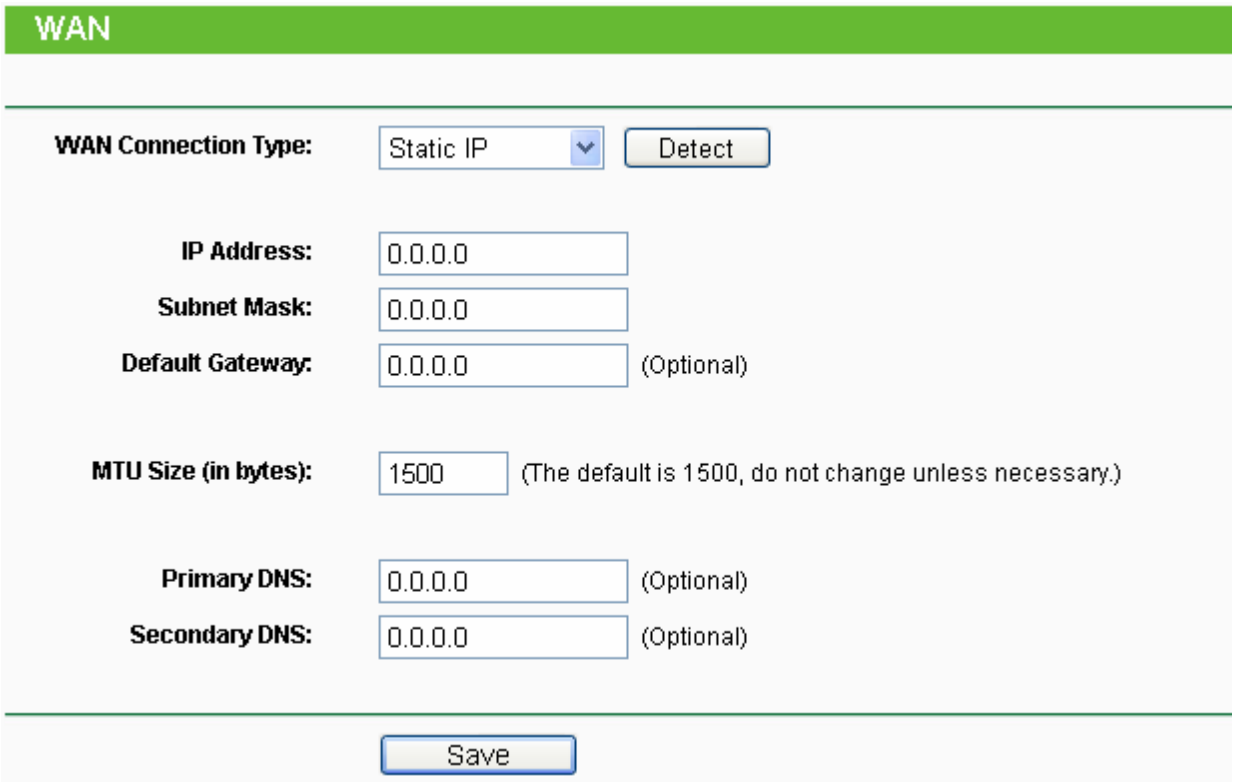
وكما هو واضح فأن الشبكة التي يتصل بها الراوتر هي الشبكة المحلية (LAN) والشبكة العالمية (WAN) مع خيار نسخ العنوان الفيزيائي (MAC clone) وسنأتي على شرح محتويات كل تبويب على حدة:

(WAN): عند النقر على هذا التبويب تظهر النافذة التالية:

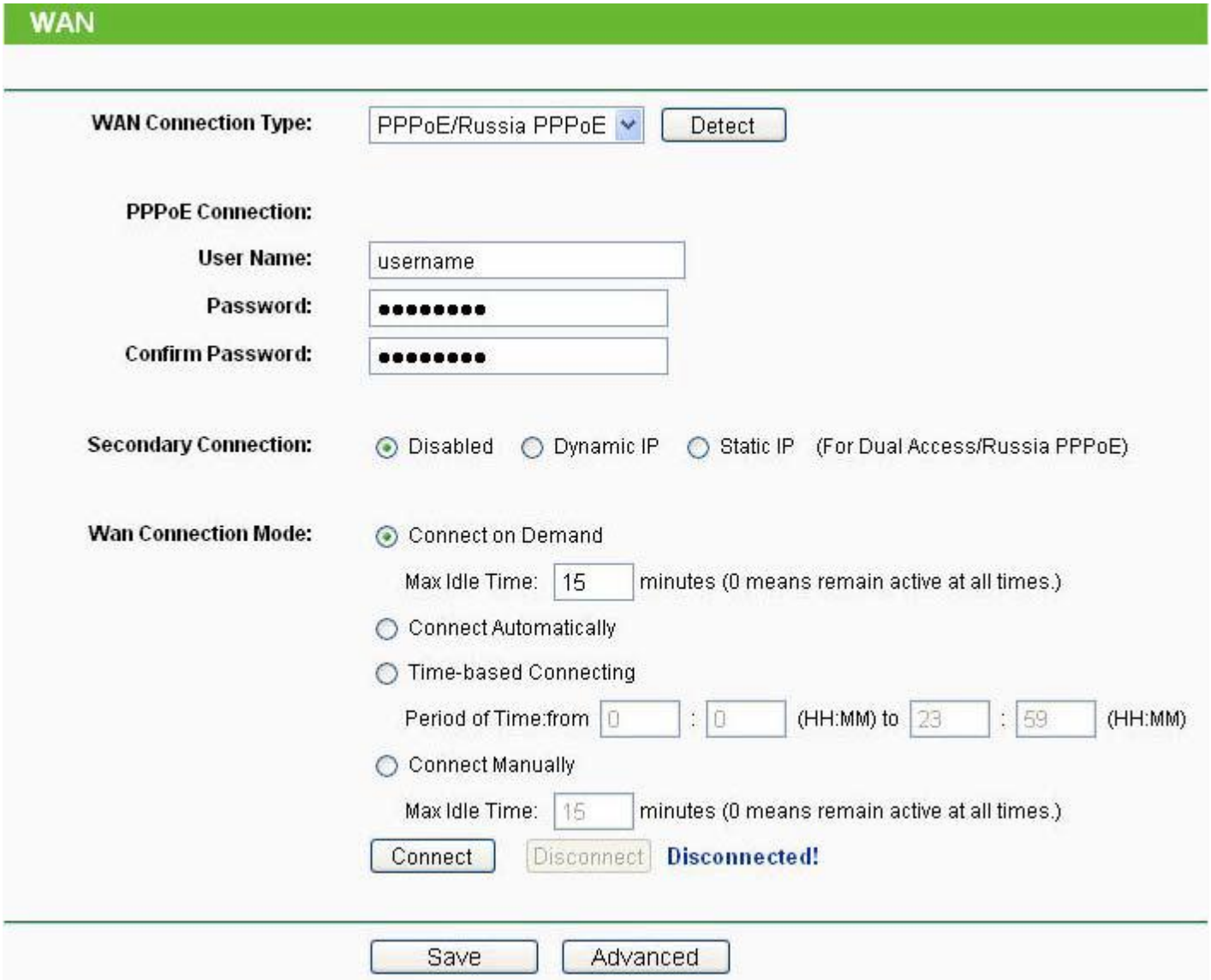


تظهر هذه النافذة ان كان مزود الخدمة (ISP) يستخدم عناوين (IP) ديناميكية أي ان لديه سيرفر (DHCP) يقوم بمنح العناوين الى الحواسيب المتصلة به ديناميكياً بشكل تلقائي وهنا يتم ادخال المعلومات التي تزود لك من قبل مجهز الخدمة من عنوان سيرفر (DNS) الابتدائي والثانوي وكذلك اكبر كتلة ارسال (Maximum Transmission Unit MTU) والتي يفضل ان تبقى على حالها بدون تغيير حيث ان ال (MTU) لكل شبكات الايثرنت (Ethernet) هو (1500) ولا يتم تغييره الا بطلب مباشر من قبل مزود الخدمة واخيراً في حالة عدم الحصول على ال (IP address) بشكل طبيعي يتم اختيار (وضع علامة صح) امام مربع (Get IP with Unicast DHCP) وذلك عندما لا يستخدم مزود الخدمة خدمة البث للعناوين (Broadcast IP addresses) وهي حالة نادرة الحدوث وبعد اكمال ادخال المعلومات المطلوبة ننقر على (save).

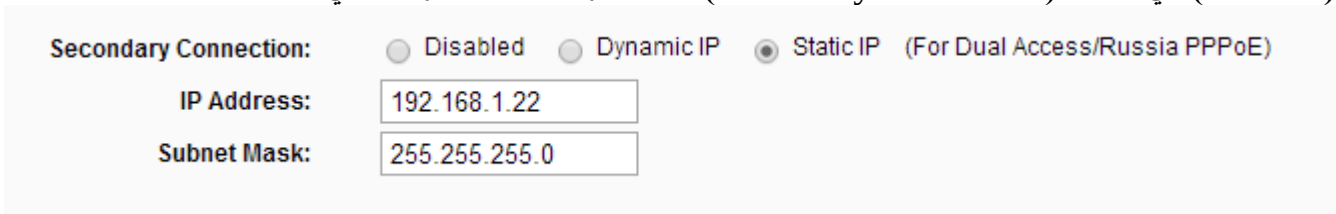
في حالة كون مزود الخدمة يستخدم (static IP) أي عناوين ثابتة ولا يعتمد على سيرفر ال (DHCP) نختار (Static IP) لتظهر النافذة التالية:



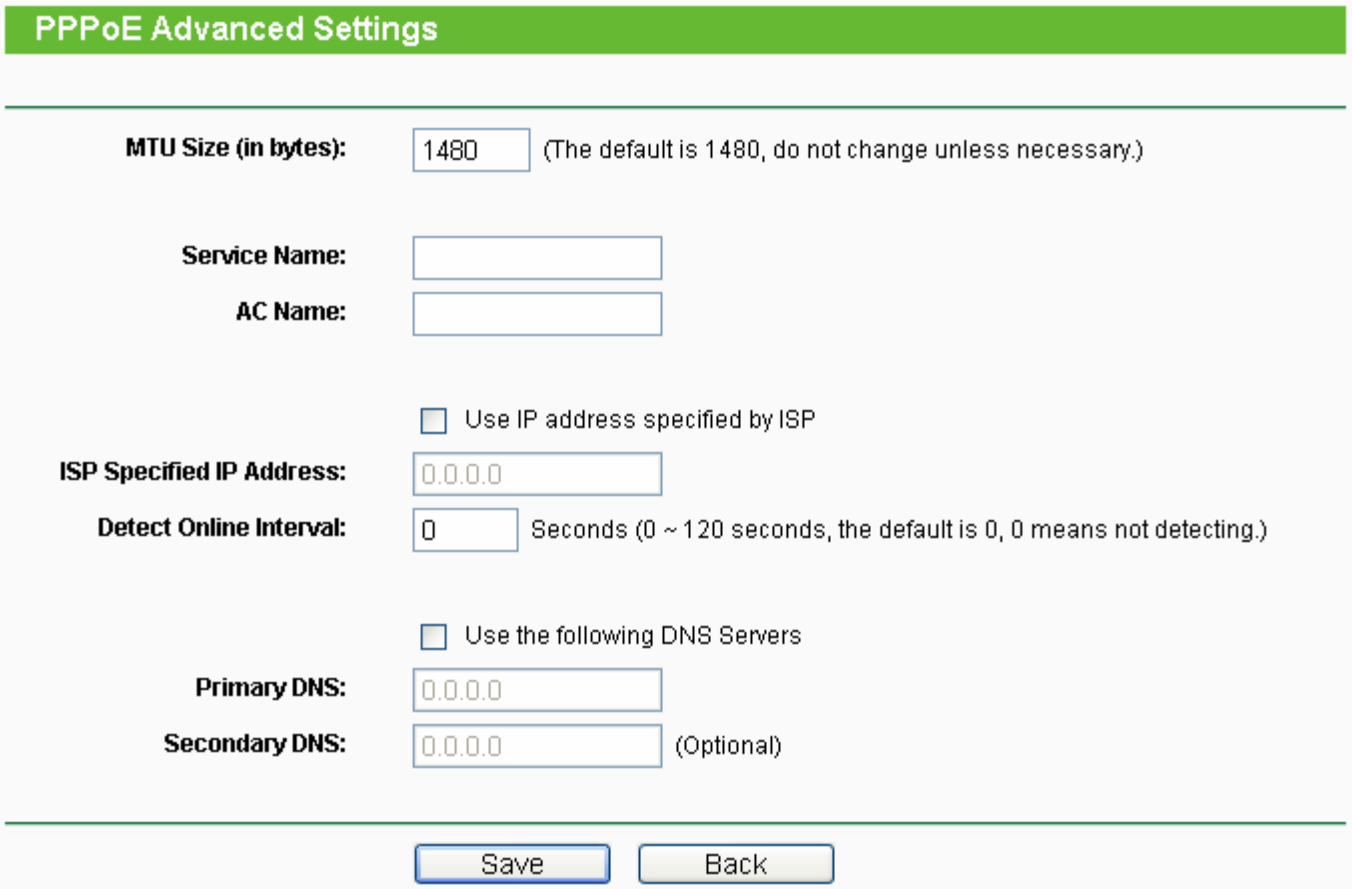
وهنا يجب ان يقوم مزود الخدمة بتجهيزنا بكل المعلومات المطلوبة لإدخالها هنا وهي عنوان ال (IP) وقناع الشبكة (Subnet mask) وعنوان بوابة الشبكة (Default gateway) وهو هنا اختياري (optional) كما مؤشر لأن هذا العنوان هو تلقائياً نفس عنوان مزود الخدمة واخيراً (MTU, Primary DNS, Secondary DNS) وكما يتم تزويدها لنا من قبل مزود الخدمة.
والان لو كان مزود الخدمة يستخدم خدمة ال (PPPoE) وهو الشائع هنا في الشرق الاوسط على الاقل فستظهر النافذة التالية:



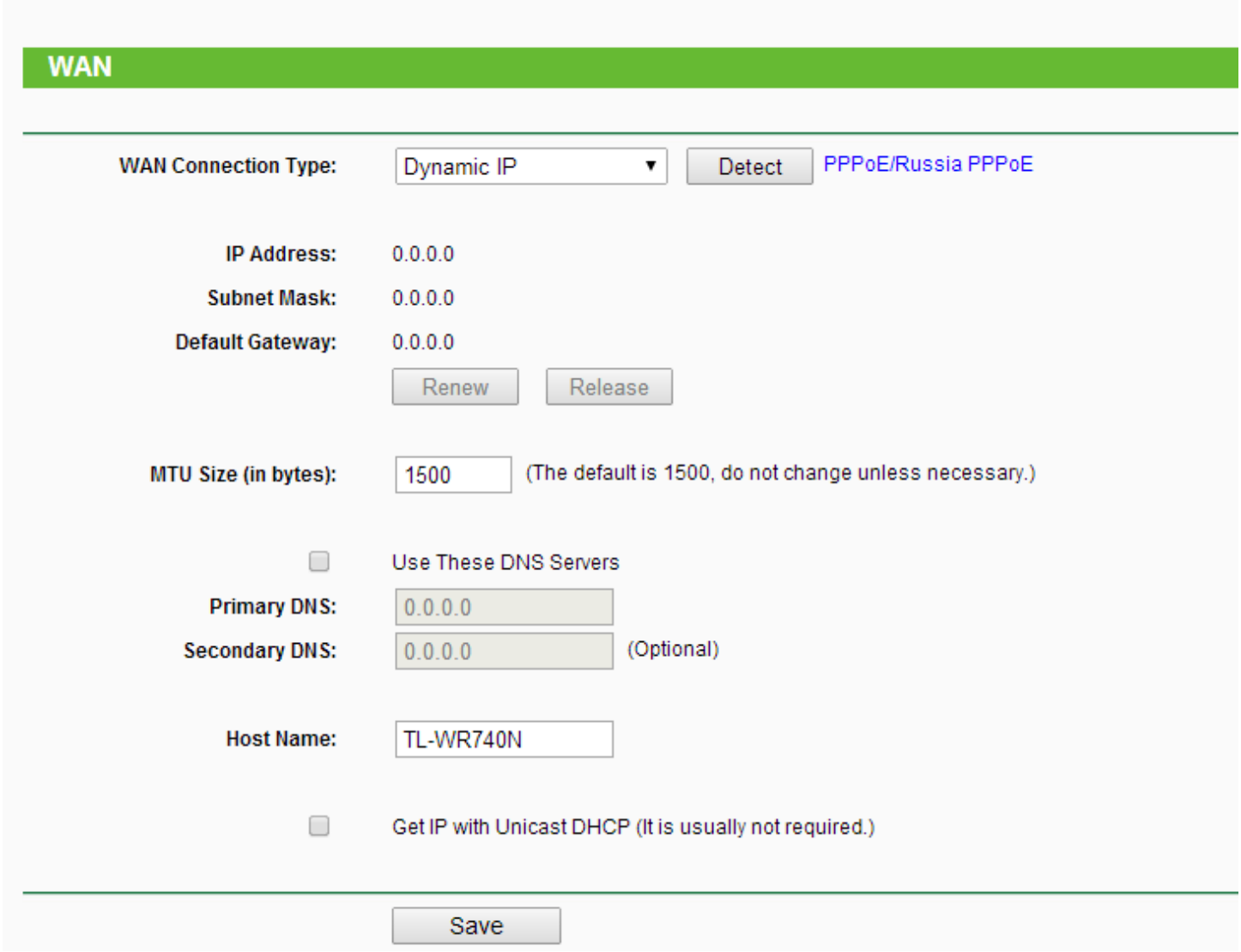
وهنا نقوم بإدخال اسم المستخدم (user name) وكلمة المرور (password) وابقاء بقية الخيارات كما هي او اختيار (static IP) في تبويب (Secondary connection) حيث تظهر نافذة مشابهة للتالي:



هنا قمنا بإدخال عنوان من نفس صنف عنوان الراوتر (192.168.0.1) حيث يمكننا استخدام أي عنوان اخر ضمن المدى (192.168.0.2-192.168.0.254) واما قناع الشبكة فكما مبين هو القناع التلقائي (Default subnet mask) للكلاس (Class C) والفائدة من هذا الخيار هو السماح لنا بالاتصال بالهوائي (Antenna) من نوع نانوستيشن او مايكروتك او أي هوائي اخر مباشرة عن طريق متصفح النت فبدل فصل كيبل الراوتر وربط كيبل النانو الى الحاسوب مباشرة لضبط اعداداته نستطيع تفعيل خيار ال (Static IP) وابقاء الاتصال كما هو والوصول الى الهوائي مباشرة.
وفي حالة اختيار ضبط المزيد من الاعدادات سنختار (Advanced) ولاحظ ان تنقر على (Save) قبل الانتقال الى تبويب متقدمة (Advanced) لتظهر النافذة التالية:

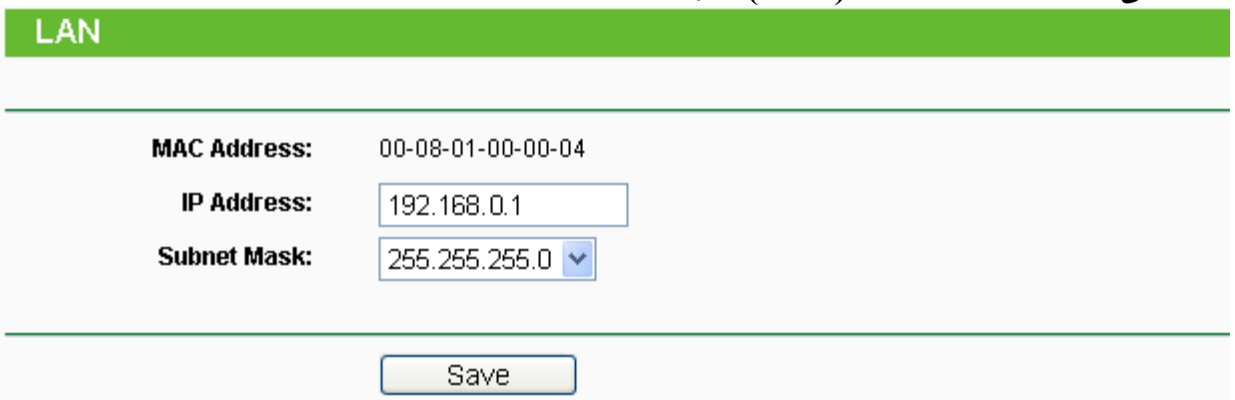


وهنا يجب الحذر من تغيير أي منها الا في حالة طلب مزود الخدمة ذلك او تزويده لك بمعلومات تخص محتويات هذه الصفحة. بخصوص بقية انواع الاتصال مع مزود الخدمة وهي (Bigbond cable, L2TP, PPTP) فلها اعداداتها الخاصة ومعلومات الاعداد التي يتم تزويدها من قبل مزود الخدمة ولا جديد بخصوصها فكلها مشابهة لما تم شرحه.
وفي حالة عدم معرفة نوعية اتصالك مع مزود الخدمة فببساطة انقر على زر (detect) في اول نافذة تظهر لك في تبويب (WAN) ليقوم بفحص واكتشاف نوع الاتصال كما في النافذة التالية:



ولاحظ ان الراوتر يستطيع كشف اول ثلاث انواع تم شرحها فقط وهي (Static, Dymanic, PPPoE) ولا يستطيع كشف الانواع الثلاثة الاخرى والتي يجب ان يعرفها المستخدم من خلال اتصاله بمزود الخدمة (ISP) ليعرفه له.

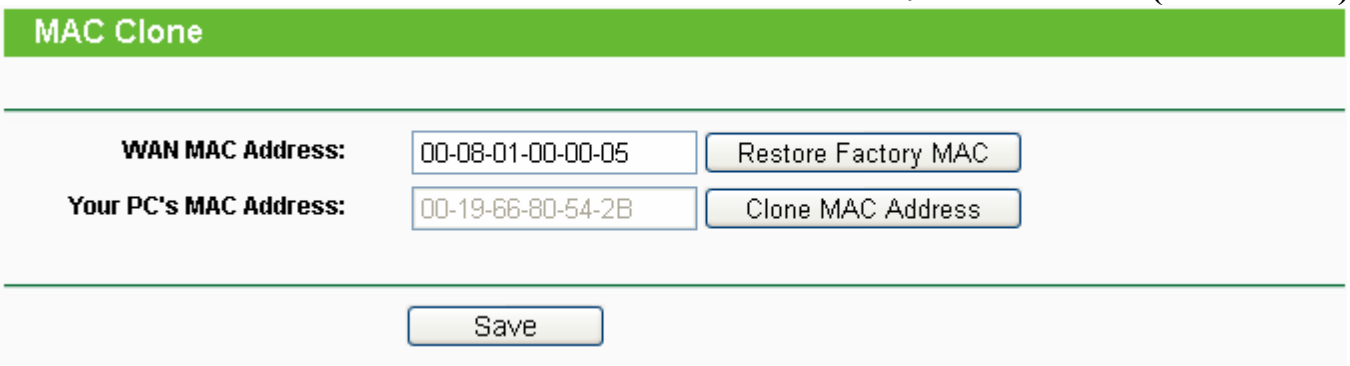
(LAN) لا يحتوي تبويب الشبكة المحلية سوى معلومات بسيطة تضم العنوان الفيزيائي والمنطقي وقناع الشبكة حيث عند النقر على تبويب الشبكة المحلية (LAN) تظهر النافذة التالية:



هنا يفضل تغيير عنوان الشبكة المحلية الذي يمكن من خلاله الوصول الى الراوتر عن طريق متصفح الانترنت وهو نفس العنوان الذي استخدمناه في الدرس الثاني والفائدة من تغييره هو لمنع بقية المستخدمين المتصلين بالشبكة من استخدامه لتغيير اعدادات الراوتر وحصر امكانيات ادارة الشبكة بمديرها فقط واما كيفية تغييره فسهلة جداً بمجرد ادخال العنوان الجديد والنقر على حفظ (Save).

ملاحظة: عند تغيير العنوان هنا يجب استخدام العنوان الجديد للوصول الى الراوتر عن طريق متصفح الانترنت وفي حالة تغيير العنوان بدون تغيير قناع الشبكة المقابل له سيقوم سيرفر ال (DHCP) بتغييره ليصبح مناسباً وصحيحاً.

(MAC clone): عند النقر عليه تظهر النافذة التالية:



- **WAN MAC address: ويمثل العنوان الفيزيائي لمنفذ الوان للراوتر ويمكن تغييره ولكن لا حاجة لذلك عادة.**
- **Your PC's MAC Address: ويمثل العنوان الفيزيائي لحاسوبك الشخصي الذي تستخدمه الان لضبط اعدادات الراوتر ويمكنك ان تنسخه وتجعله نفسه العنوان الفيزيائي للوان الخاص بالراوتر بالنقر على زر (clone MAC address) حيث انك سترى ان عنوان ماك حاسوبك سينسخ الى الحقل فوقه ولاسترجاع الماك الخاص بالراوتر ننقر على (Restore Factory MAC) واخيراً لحفظ التغييرات ننقر على (Save).**

كما ذكرت سابقاً لا حاجة لتغيير شيء هنا ولكن في بعض الاحيان يحتاج مزود الخدمة منك ان تنسخ عنوانك الفيزيائي وترسله له فمن هنا تستطيع الوصول له.

ملاحظات عامة تخص الدورة:

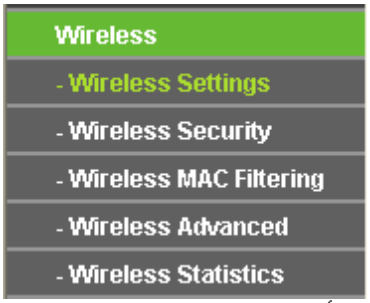
١- يتساءل بعض القراء والمتابعين للدورة عن اهمية كل هذه التفاصيل رغم ان خيار (Quick setup) هو الخيار الاسهل والافضل والاكثر استخداماً وفي معرض الجواب عن هذا التساؤل اقول باختصار ان الضبط السريع لا يوفر كل الامكانيات والسرعة والامنية القصوى التي يحتاجها المستخدم خصوصاً ان كانت الشبكة تضم عدداً لا بأس به من المستخدمين وتحتاج اداء عالي للجميع. وكذلك فأن التطرق الى بقية التفاصيل هو لعرض امكانيات هذا الجهاز الذي يوفر وظيفية الكثير من الاجهزة الغالية المعقدة وبأسلوب مبسط وقابلية ضبط بسيطة جداً متاحة للجميع حتى لغير المختص واخيراً فأن الضبط السريع يبقي الشبكة عرضة للتلاعب والتخريب والاختراق من قبل كل من لديه ابسط مقومات الاختراق والوصول وهو الامر الذي سنمنعه ان شاء الله بشكل نهائي في الدروس القادمة.

٢- هذه الدورة وامثالها لا تعجب البعض ويعتبرونها بديهية وسهلة وهذا صحيح بالنسبة لمستواهم المتوسط او المتقدم ولكن هناك الكثير من المبتدئين الذين هم بحاجة الى كل عون للبدء والنهوض وإذا بقينا نتداول الامور المتقدمة المعقدة فقط فمن سيأخذ بيد هؤلاء المبتدئين للتقدم والوصول الى ما وصلنا اليه؟ كذلك فهي فرصة للتطرق الى مفاهيم بسيطة تتغافل عن التطرق لها الكثير بل اغلب الدورات المتقدمة في مجال الشبكات.

٣- تحياتي وتقديري لكل من تابع وواصل المتابعة واستفاد شيئاً ونشر ما استفاد منه واسأل الله تعالى التوفيق للجميع لما فيه خير الجميع وغد أفضل.

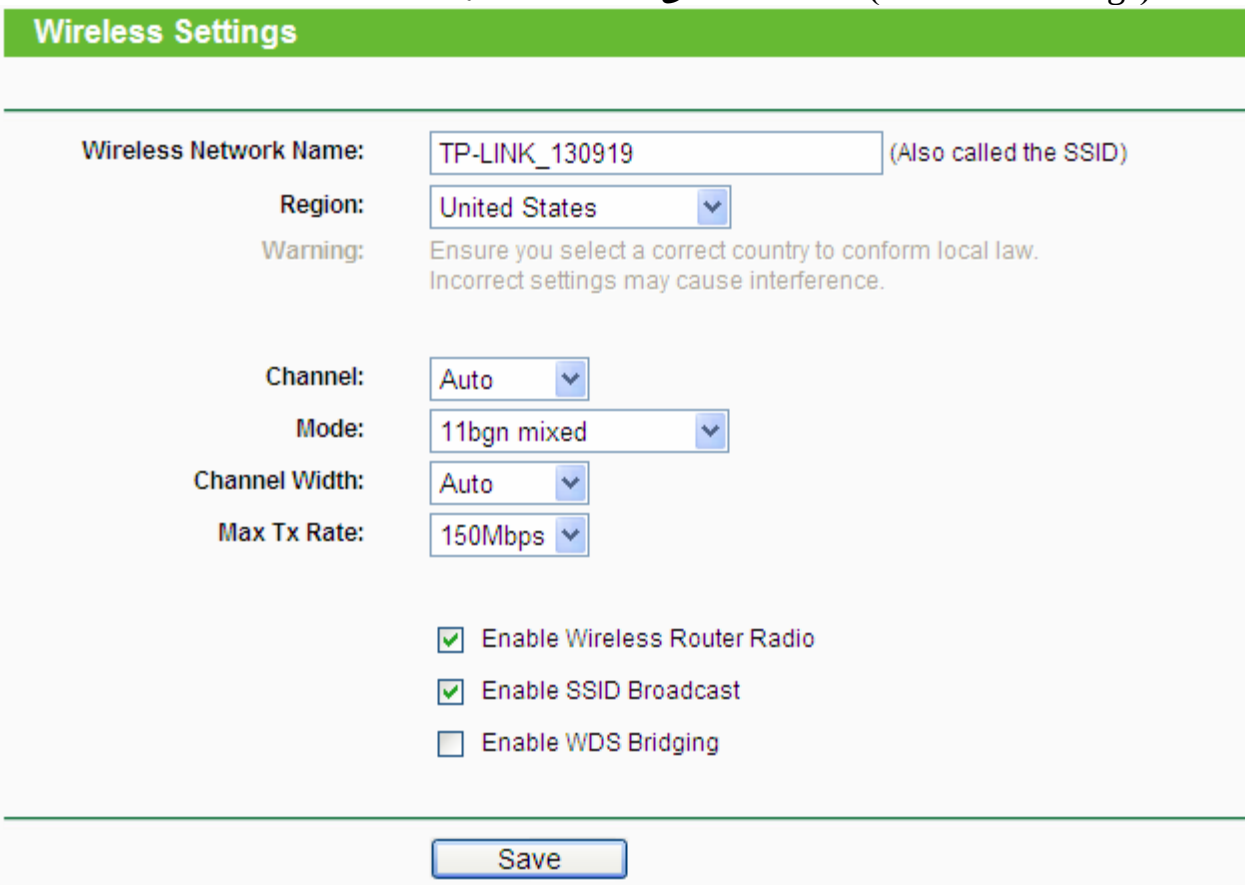
الدرس الخامس من دورة إدارة الشبكات المنزلية:

بعد ان شرحنا اول أربع قوائم في واجهة اعدادات ال (TP-link wireless router) نأتي اليوم الى شرح القائمة الخامسة والخاصة بالاتصال اللاسلكي المحلي (Wireless LAN) بين الراوتر والحواسيب المنزلية او أجهزة الهاتف الذكية في شبكة المنزل او الدائرة وعند النقر على هذه القائمة تظهر الخيارات التالية:

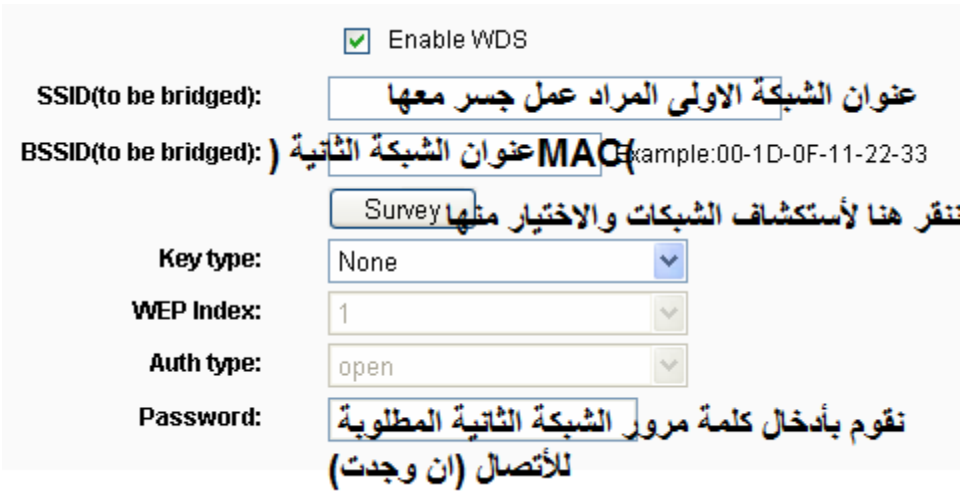


سنأتي الان لشرح كل منها على حدة وباختصار وحسب ما يحتاجه المستخدم غالباً:

- (Wireless Settings): وعند النقر على هذا التبويب تظهر النافذة التالية:

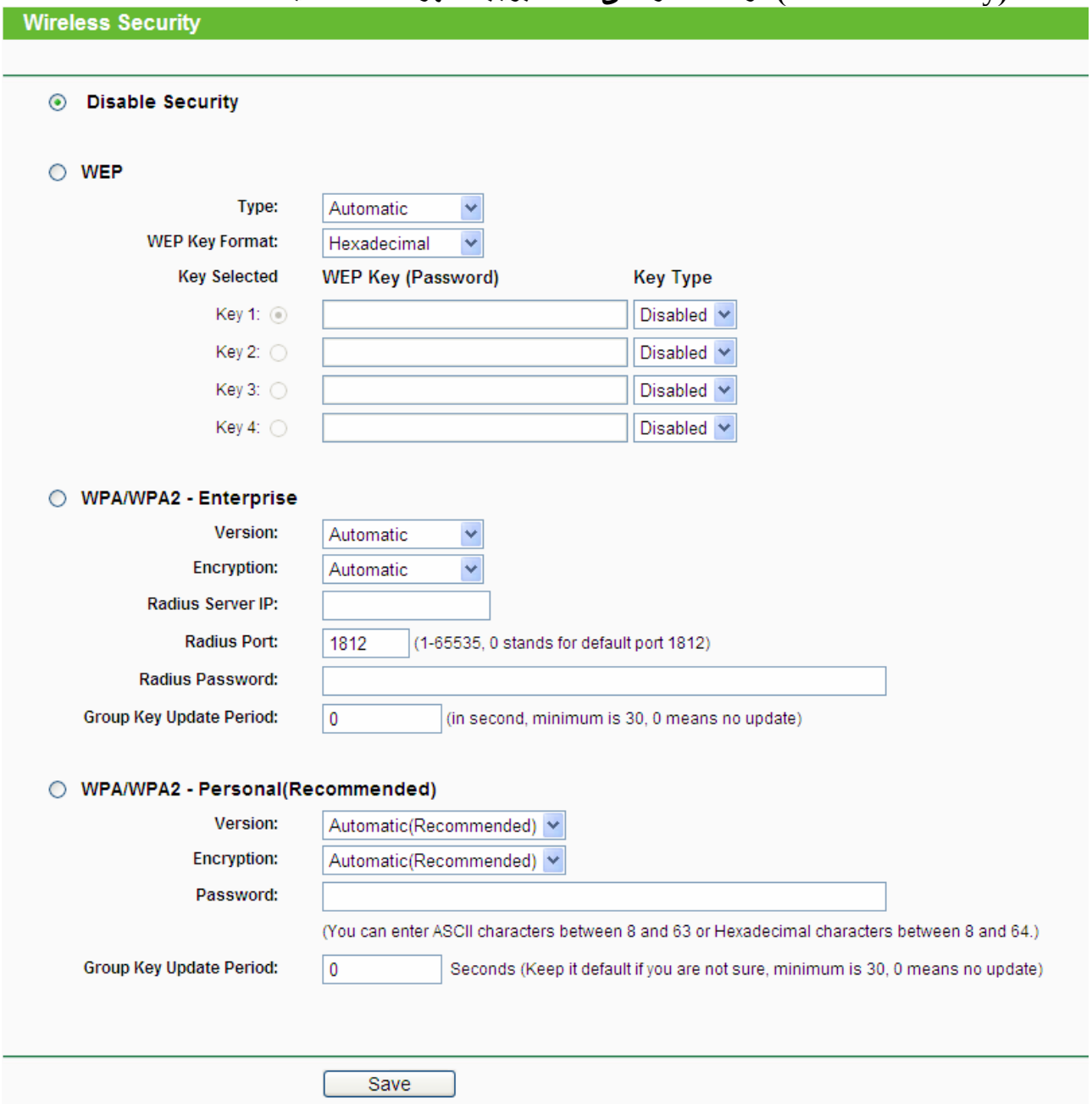


تضم هذه النافذة اسم الشبكة اللاسلكية (wireless network name) وهو نفسه اسم الشبكة الذي تم ضبطه في خيار الضبط السريع باسم (service set identification SSID) ويجب ان يعرفه كل مستخدمي الشبكة للاتصال بها.
كذلك تضم هذه النافذة منطقة عمل هذا الجهاز ويجب ضبطها لمنطقة العمل الفعلي لأن اختيار منطقة أخرى قد يسبب مشاكل قانونية ولكن هنا في الشرق الأوسط لا وجود لشيء كهذا ويمكننا اختيار أي منطقة بدون مشاكل!
الامر الاخر هو قناة البث اللاسلكي او التردد المستخدم (channel frequency) ويفضل اختياره (Auto) ليقوم الراوتر باختيار التردد المناسب الذي لا يتداخل مع ترددات بقية الراوترات حوله. واما نمط الارسال والاستقبال فيفضل ابقائه (11bgn mixed) لكي يسمح لكافة أنواع الأجهزة المزودة بخاصية الارسال والاستقبال اللاسلكي بمختلف مقاييسها بالاتصال. وتبقى بقية الخيارات كما هي ثم ننقر على (save).
ملاحظة: بعض الأحيان نحتاج الى توسيع الشبكة المنزلية او المحلية اللاسلكية الى مسافة ابعد فنقوم بربط عدة راوترات كجسور (bridges) وهنا نقوم بتأشير علامة صح في المربع امام خيار (enable WDS bridging) حيث تظهر النافذة التالية:



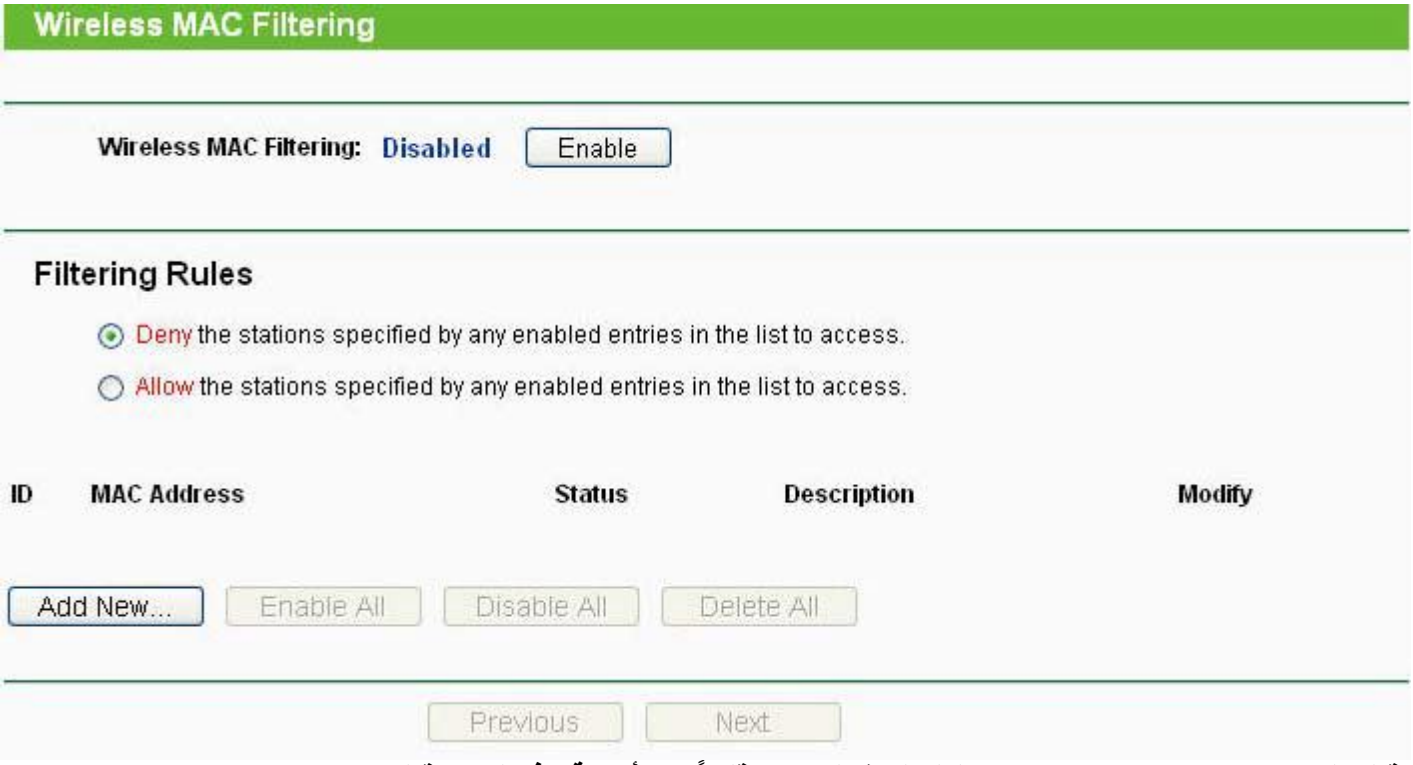
ونقوم بإدخال القيم المطلوبة كما في النافذة واما بقية القيم فهي نوع مفتاح التشفير او كلمة المرور (key type) وكذلك نوع الأمنية المستخدمة (WEP index) ونوع تخويل الدخول (Auth type) ويتم الحصول على المعلومات المطلوبة من مزود الخدمة او صاحب الشبكة الأولى.

- (wireless security): وعند النقر على هذا التبويب تظهر النافذة التالية:



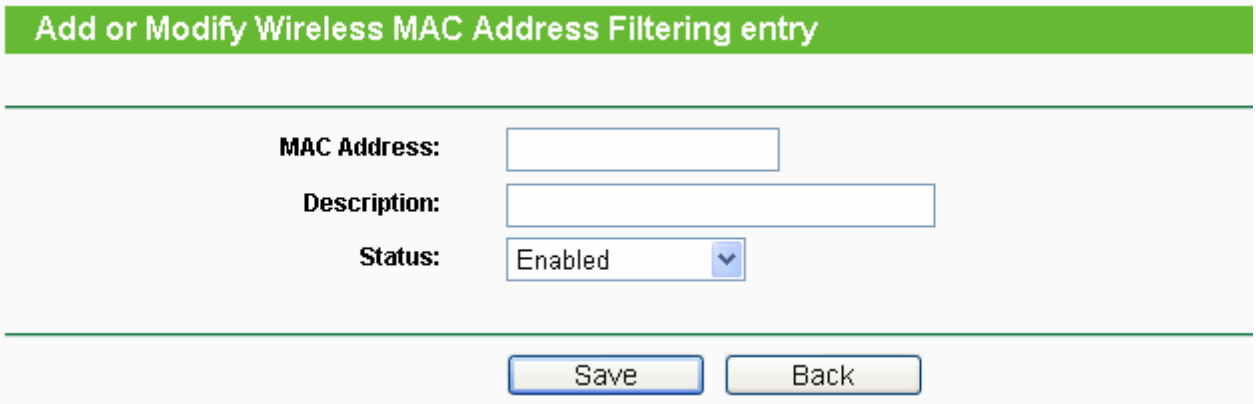
نقوم باختيار نوعية الأمنية المناسبة حيث انه لا يفضل تفعيل خيار (disable security) لأن الشبكة المحلية تكون عرضة للاختراق ودخول غير المخولين لها وإمكانية العبث بها او التأثير على جودة وكفاءة الاتصال واما حين نختار أي نوع من أنواع الأمنية والتشفير فنقوم بعدها بإدخال كلمة المرور او مفتاح التشفير حسب المواصفات المطلوبة وسيكون هو مفتاح الوصول والدخول الى الشبكة من قبل المستخدمين المنزليين او المحليين.

- (wireless MAC filtering): وهو الخيار الأهم في امنية الشبكة وعند النقر عليه تظهر النافذة التالية:

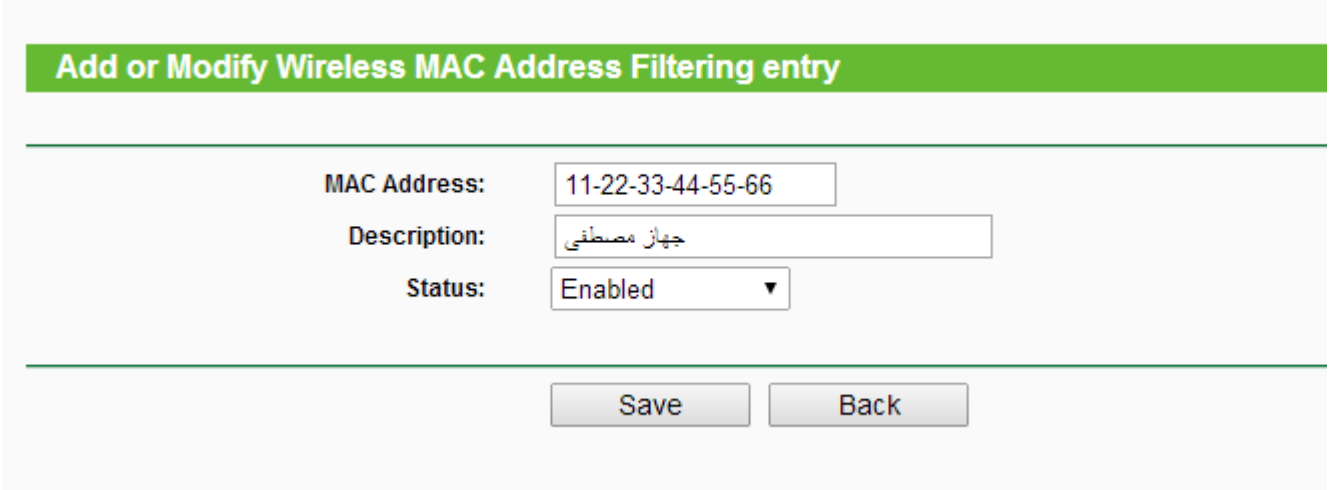


وقبل كل شيء يجب اختيار (enable) لتفعيله ثم لنتحدث قليلاً عن أهمية هذا الخيار قبل شرح اعداداته:
هنا نستطيع عمل ترشيح (filter) للحواسيب والأجهزة الذكية المسموح لها بدخول الشبكة والغير مسموح لها بذلك وكلنا يعرف مصطلح (allow) بمعنى سماح ومصطلح (deny) بمعنى منع ولذا فأنت بمجرد ان تنقر على خيار (allow) فهذا يعني انك تقول للجهاز (اسمح فقط للأجهزة المدرجة ادناه بالاتصال ولا تسمح لغيرها بفعل ذلك) وكذلك بمجرد النقر على زر (Deny) والذي يكون هو الخيار التلقائي المؤشر مسبقاً فأنت تقول للجهاز (امنع كل الأجهزة المدرجة ادناه واسمح لغيرها بالاتصال) لذا (((يجب الحذر من النقر على خيار السماح allow قبل ان تقوم بإضافة جهازك الى قائمة الأجهزة كما سنرى الان).
وهنا سأقوم بشرح مثال يوضح كيفية استخدام هذه الأدوات:
مثال: لنفترض اننا نريد ان يرتبط بشبكتنا جهازين فقط هما الجهازين الذين يكون عنوانهما الفيزيائي (11-22-33-44-55-66**) و (**1a-2b-3c-4d-5e-6f**) ومنع كافة الأجهزة الأخرى من الدخول الى الشبكة فماذا نفعل:**

- **نختار خيار المنع (deny) ثم ننقر على إضافة جديد (Add new) لتظهر النافذة التالية:**



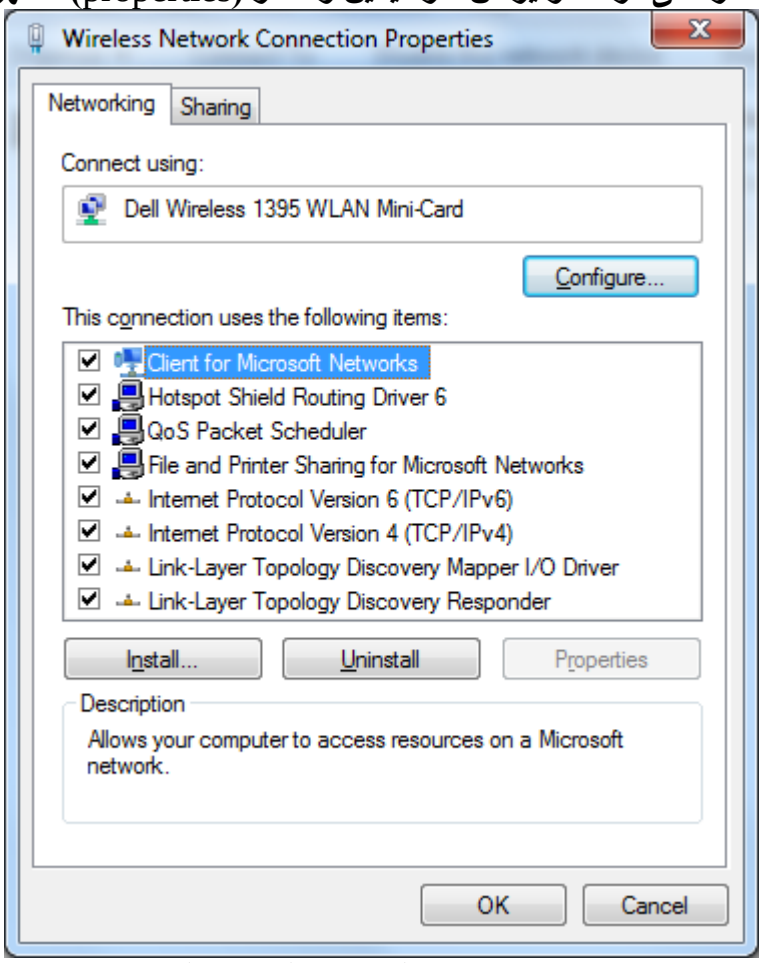
- **نقوم بإدخال معلومات الجهاز المراد السماح له ومنع غيره وهي تشمل العنوان الفيزيائي (**MAC Address**) ووصف مختصر للجهاز لتعريفه مستقبلاً (**description**) مثلاً (جهاز مصطفى) والحالة التي تريد تفعيلها له لتكون النتيجة مشابهة للتالي:**



وبنفس الطريقة نضيف معلومات الجهاز الثاني وننقر على (save) طبعاً في كل مرة والان ننقر على الزر الأخطر وهو (allow) وفي هذه النقطة فقط سيقوم الجهاز بالسماح للجهازين الذين يمتلكان العناوين الفيزيائية المدخلة سابقاً فقط بالدخول الى الراوتر ومنع كل بقية الأجهزة من ذلك.

اما كيف نحصل على ال (MAC address) الخاص بجهازي فبأتباع الخطوات التالية:

نفتح قائمة (start) ثم (control panel) ثم (network and sharing center) ثم (change adapter settings) ثم ننقر على كرت الوايرلس نقرة يمين ونختار (properties) لتظهر نافذة مشابهة للتالي:

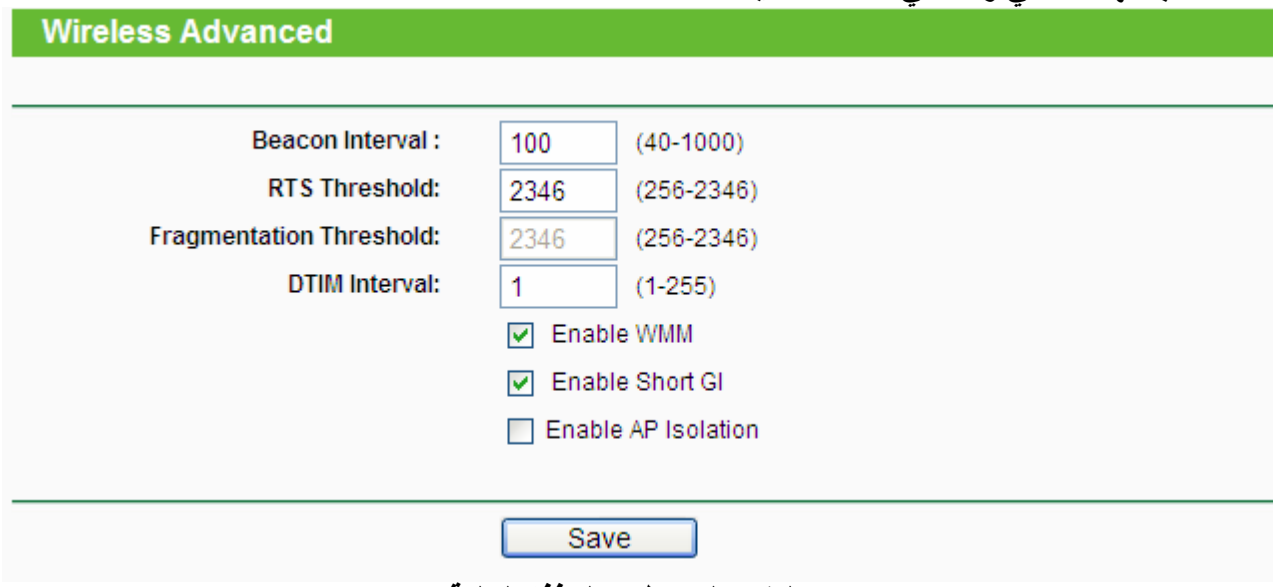


والان بمجرد ان نضع مؤشر الماوس على اسم الكرت (..... Dell Wireless) سيظهر عنوان (MAC address) الكرت اللاسلكي فنقوم بتسجيله لاستخدامه لاحقاً.

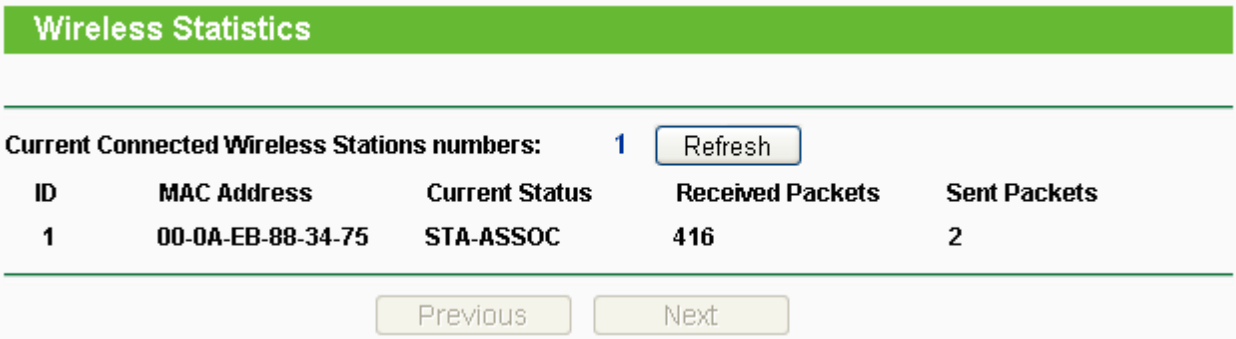
مشكلة محتملة: وانا احضر لهذا الدرس حصلت معي مشكلة بسيطة وهي انني قمت سهواً بالنقر على خيار (Allow) قبل ان أقوم بإدخال معلومات جهازي (MAC address) ولذا مباشرة قام الراوتر بفصل جهازي عن الشبكة ومنعي من الدخول لا انا ولا غيري أي ان الراوتر أصبح لا يسمح لأحد بالدخول مما اضطرني لعمل (reset) للجهاز من الزر الواقع في الخلف

بالنقر عليه (بعود ثقاب مثلاً) لمدة ١٥ ثانية حتى تضيء كل مصابيحه (LED's) مرة واحدة ثم تنطفئ وبذلك يعود الجهاز الى ضبط المصنع ونعيد الضبط من جديد.

- (wireless advanced): ويحتوي الكثير من الخيارات التي لا يحتاجها المستخدم في الشبكة الصغيرة بل ويفضل ابقائها كما هي وكما في النافذة التالية:



- (wireless statistics): وعند النقر عليه تظهر النافذة التالية:

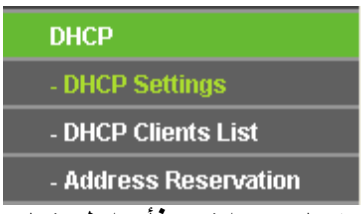


وتظهر فيها معلومات واحصائيات الأجهزة المتصلة بالشبكة اللاسلكية الان من العنوان الفيزيائي وحالة الاتصال (current status) والبكتات المستلمة (received packets) والبكتات المرسلة (sent packets) وتقوم هذه الصفحة بعمل إنعاش (Refresh) تلقائياً كل خمس ثواني او يمكن النقر على زر (refresh) لعمل تحديث يدوي للصفحة لمعرفة وجود او عدم وجود مرور (traffic) او ارسال واستقبال في الشبكة.

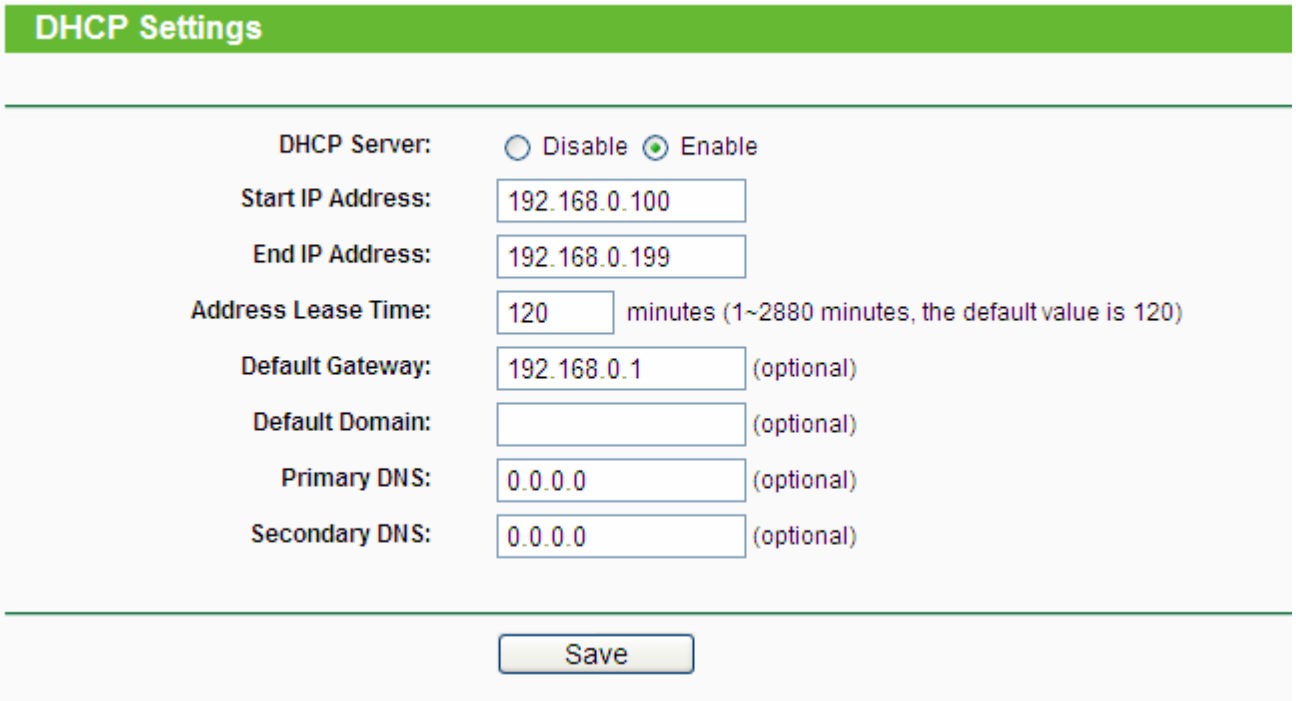
الدرس السادس من دورة إدارة الشبكات المنزلية

وصلنا اليوم الى قائمة بروتوكول ضبط الزبون الديناميكي (Dynamic Host Configuration Protocol DHCP) وقبل الحديث عن ضبط اعداداته نتحدث قليلاً عن وظيفة هذا البروتوكول الذي يعتبر أحد الخدمات التي يوفرها كل أنواع الراوترات والسيرفرات كالويندوز سيرفر واللينكس ووظيفته الرئيسية هي منح واسناد عناوين (IP address) وقناع الشبكة (Subnet mask) وبوابة الشبكة (Default Gateway) وعنوان سيرفر نطاق العناوين (Domain Name Server DNS) الابتدائي والثانوي الى كل الحواسيب والأجهزة الذكية المتصلة بالشبكة بشكل تلقائي وبدون تدخل المستخدمين ولا إدخالها بشكل يدوي من قبل مدير الشبكة كما كان يحصل سابقاً قبل تطوير هذا البروتوكول حيث كان مدير الشبكة يقوم بإدخال هذه المعلومات يدوياً الى كل الأجهزة المتصلة بالشبكة حين كان العدد قليلاً واما الان وقد زاد عدد الحواسيب المتصلة بكل شبكة حتى بلغ الالاف فمن الصعب بل المستحيل فعل ذلك كما كان يحصل سابقاً لذا جاء هذا البروتوكول ليحل هذه المشكلة وقد نجح في ذلك لحد الان.

عند النقر على قائمة (DHCP) تظهر الخيارات التالية:



وكما هو واضح فأن اول خيار وهو الأهم يشمل اعدادات هذا البروتوكول (DHCP settings) والذي عند النقر عليه تظهر النافذة التالية:



عند وجود أي نوع من أنواع الراوترات في الشبكة فأنه يفعل بشكل تلقائي ليكون سيرفر (DHCP) وكما هو واضح في الصورة أعلاه فأن الخيار التلقائي هو التفعيل (enable) واما بقية الخيارات فكما يلي:

- (Start IP address): وهو عنوان اول (IP address) يمكن اسناده الى أجهزة الشبكة ويفضل ان يكون من ضمن نفس نطاق عناوين الراوتر ولأن عنوان الراوتر المحلي الذي يمكن الوصول الى الراوتر من خلاله هو (192.168.0.1) فيمكننا هنا اعتماد أي مدى جزئي او كلي ضمن الحدود التالية: (192.168.0.2-192.168.0.254) كما يمكن استخدام أي مدى ضمن نطاق العناوين الخاصة (private IP addresses) والتي تبينها الصورة التالية:

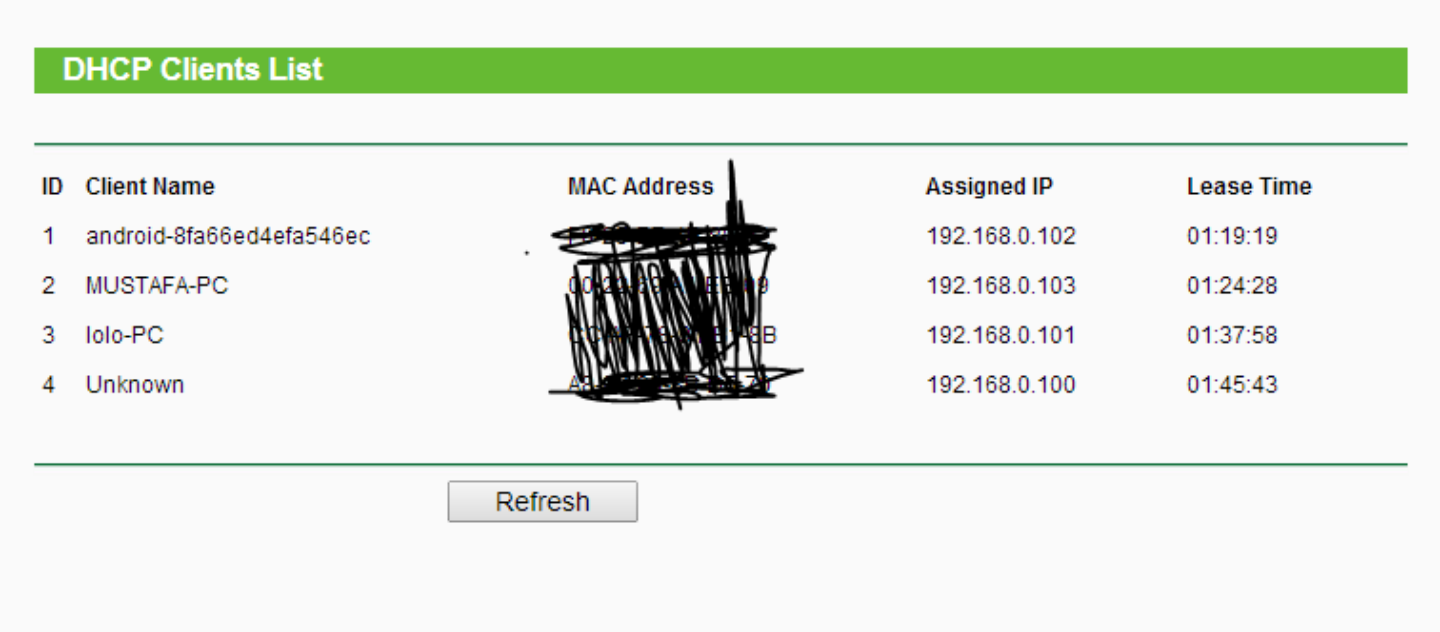
Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

- (end IP address): وهو عنوان اخر (IP address) يمكن اسناده الى الحواسيب المرتبطة بالشبكة ويمكن تقليل المدى المسموح للحواسيب للاتصال بالشبكة الى العدد المتوقع للحواسيب المعروفة للاتصال بالشبكة لتمييز حالة الاختراق ان حصلت إذا حاولت في يوم من الأيام الدخول ولم تستطيع بسبب عدم إمكانية اسناد عنوان لك فأعلم ان هناك جهازاً غير ما تعرفها قد دخل الى الشبكة ويكن معرفته بسهولة كما سنرى لاحقاً.
- (address lease time): زمن ايجار العنوان وهو المدة الزمنية التي يبقى فيها العنوان المعين مرتبطاً بحاسوب معين وبعدها يتم تغيير العنوان الخاص بهذا الحاسوب وتدوير العناوين بين الحواسيب بشكل ديناميكي ولذلك سمي (Dynamic HCP) وهو تلقائياً ساعتين (١٢٠ دقيقة) ويمكن جعله أكثر او اقل حسب حاجة المستخدم وتتراوح قيمته بين (١-٢٨٨٠) دقيقة.

- (default Gateway): وهو اختياري يمكن تركه بلا ضبط ويفضل ادخال عنوان الراوتر هنا (192.168.0.1) او أي عنوان اخر للراوتر ان تم تغييره.
- (default Domain): وهو اسم موقع شبكتك ويمكن تركه فارغاً او ملئه بعنوان مشابه للتالي (www.mustafasadiq0.wordpress.com).
- (Primary and secondary DNS): وهي اختيارية ايضاً يمكن ملئها بقيم في حال تزويدنا بها من قبل مزود الخدمة او في حالة الاشتراك في خدمة (Dynamic DNS) او (Open DNS) ويمكن تركها فارغة.

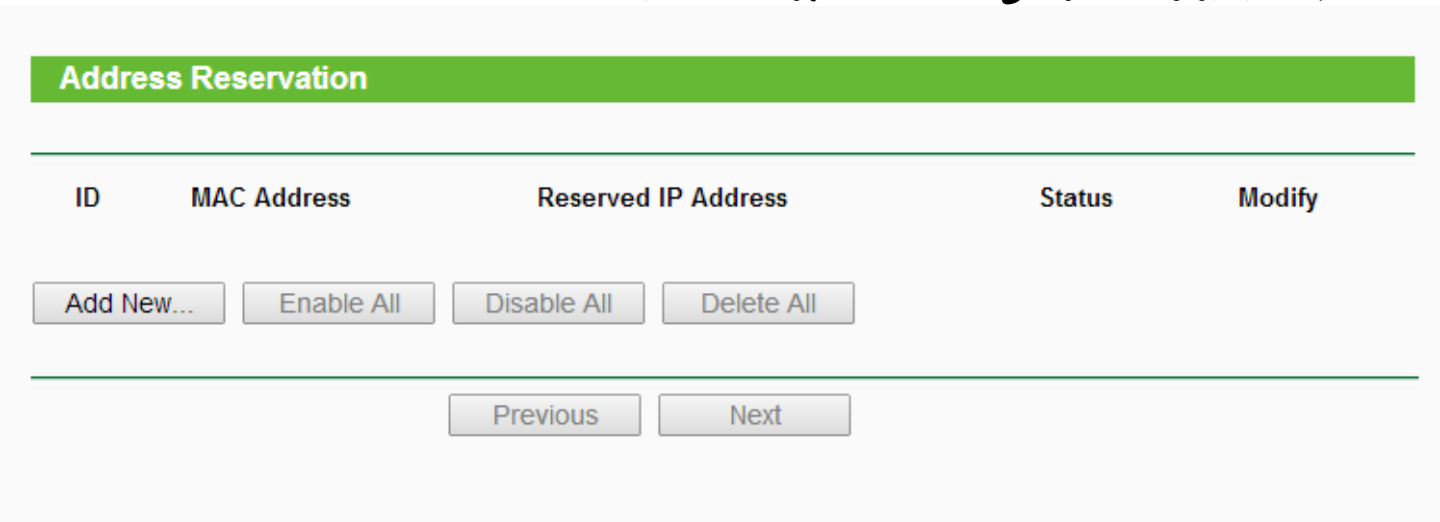
وبعد اكمال ضبط اعدادات هذه الصفحة لا ننسى النقر على زر (save).

- (DHCP clients list): ومن خلال هذه النافذة نستطيع رؤية من يتصل بالراوتر في الوقت الحاضر ومعلومات عن اسم الجهاز وعنوانه المنطقي (IP address) والفيزيائي (MAC address) والزمن المتبقي على استئجار العنوان الحالي لذلك الجهاز وكما في المثال التالي:



وعند النقر على زر الإنعاش (refresh) يتم تحديث المعلومات تلقائياً.

- الخيار الثالث في قائمة ال (DHCP) هي (Address Reservation) ووظيفته حجز عنوان منطقي (IP address) لحاسوب معين بشكل دائمي بحيث ان هذا الجهاز في كل مرة يتصل بالراوتر سيأخذ نفس العنوان ولا يتغير وتستخدم هذه الخاصية للحاسوب الذي يحتوي وظيفة خادم (server) لتوفير خدمة معينة لأن السيرفر يجب ان يكون له عنوان ثابت لا يتغير وعند النقر على هذه القائمة تظهر النافذة التالية:



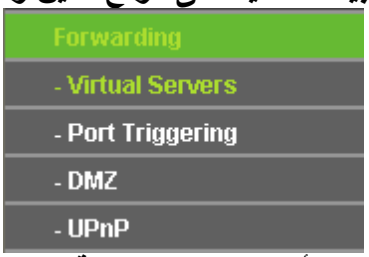
وكما هو واضح فأن أي حجز يتطلب مبدئياً النقر على (Add new) لتظهر النافذة التالية:

وهنا نقوم بإدخال العنوان الفيزيائي (MAC address) للجهاز المراد حجز (IP address) خاص له وكذلك نقوم بإدخال العنوان المراد حجزه ويجب ان يكون ضمن حيز العناوين الذي تم تحديده مسبقاً في التبويب (DHCP settings) واخيراً نفعل هذا الحجز باختيار (enable) وبعد حفظ التغييرات (save) تظهر النتيجة التالية:

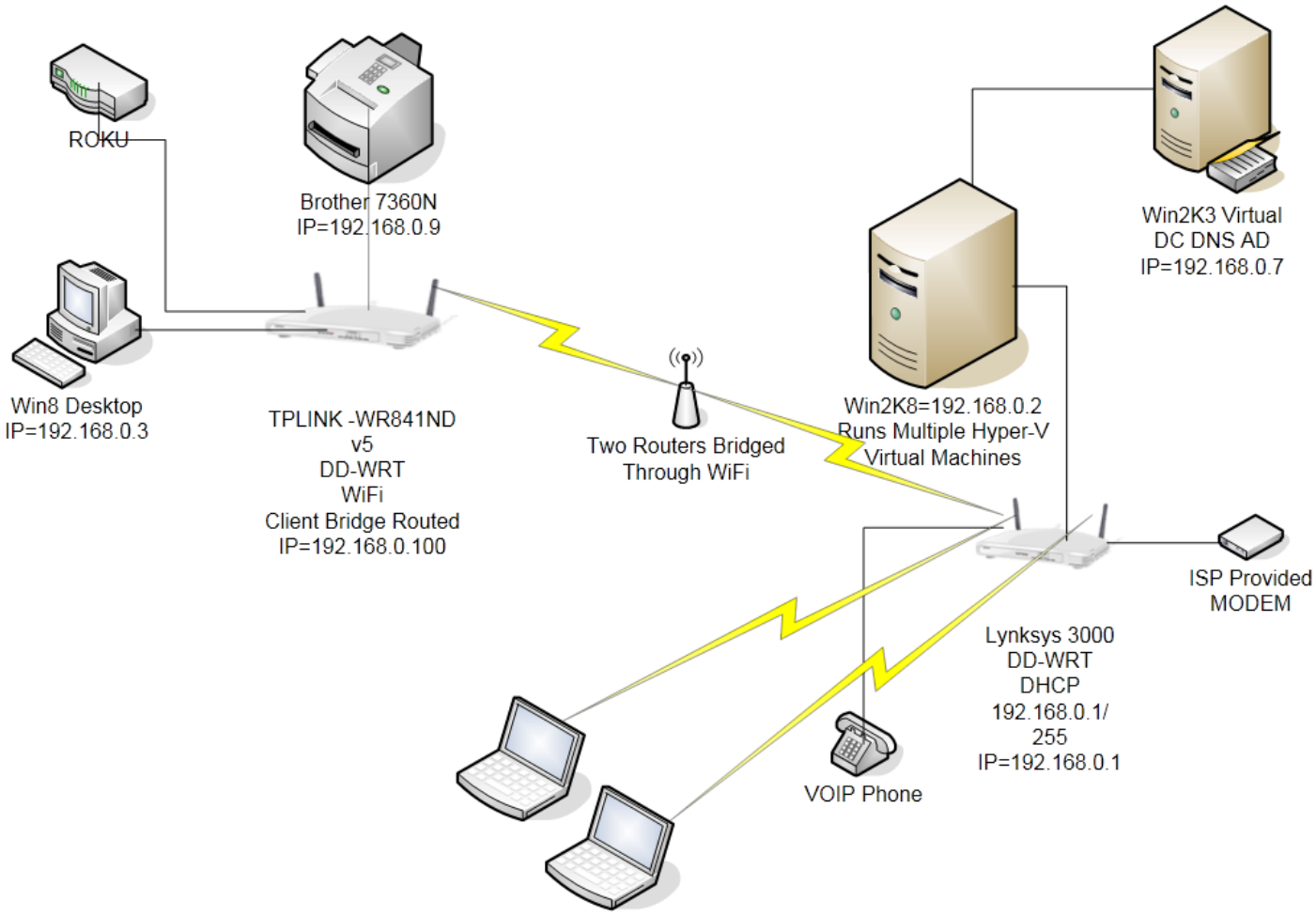
وبعد تفعيل وخزن العناوين المراد حجزها يمكن تفعيلها كلها (enable all) او تعطيلها كلها (disable all) او حذفها كلها (delete all) والانتقال بينها الى الامام (next) او الى الخلف (previous).

الدرس السابع من دورة ادارة الشبكات المنزلية:

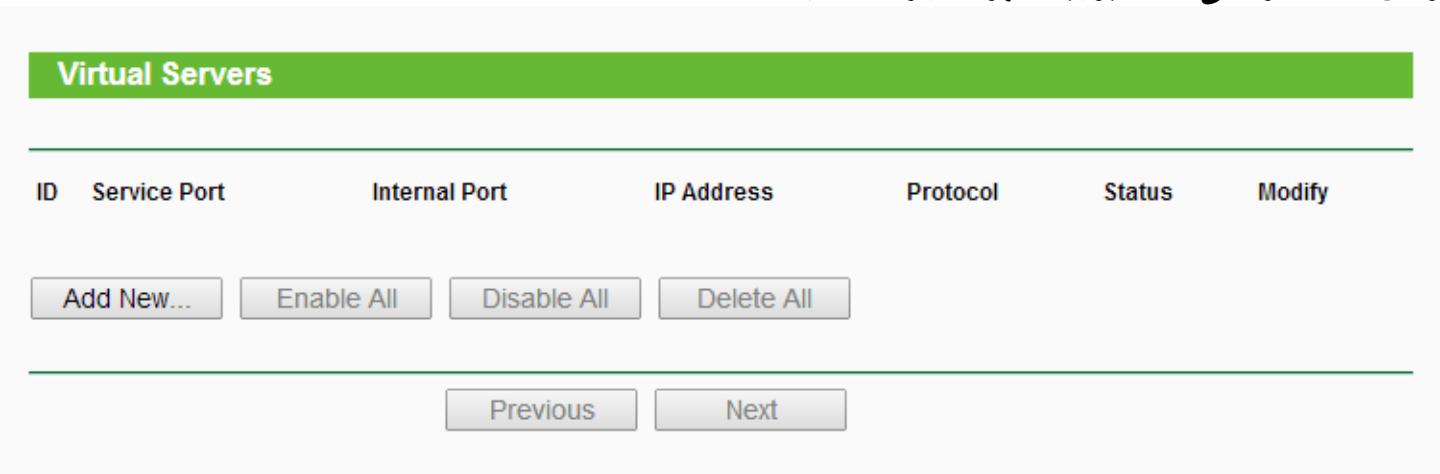
وصلنا اليوم الى تبويب (forwarding) ويعني التقديم للأمام او الارسال او الشحن ويعنى بالأمور التي تخص اعادة توجيه بيانات معينة الى موقع معين وحين النقر على هذا التبويب تظهر القائمة التالية:



ولنبدأ بالخيارات المتاحة واولها الخوادم الافتراضية او الوهمية (virtual servers) ويستخدم هذا الخيار لضبط توجيه البيانات الى جهاز خادم افتراضي موجود ضمن الشبكة المحلية وهو عادة عبارة عن جهاز حاسوب يقوم بوظيفة معينة مثل ان يكون (DNS server) محلي او (file server) او حتى (printer server) ويفترض ان يوفر هذا الجهاز خدمة معينة عبر منفذ (port) نقوم بضبطه ونفترض ان الشبكة المنزلية لدينا شكلها كما في المخط التالي:

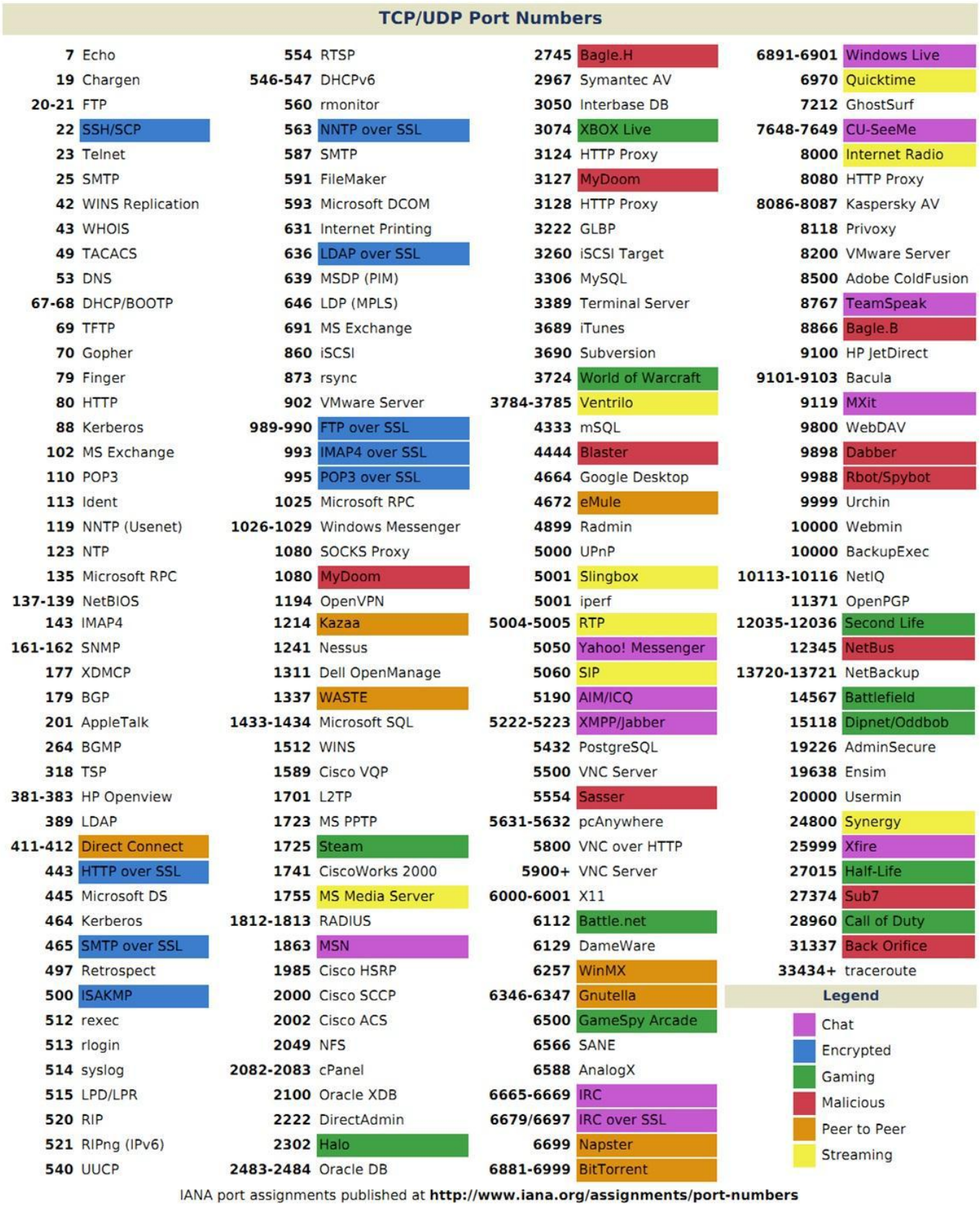


والان عند النقر على هذا التبويب تظهر الخيارات التالية:



هنا بداية وكما هو واضح لا نرى أي محتويات في حقول هذا الجدول ولكن لتبيان ما تعنيه هذه الحقول نشرح كل منها:

١- (service port): منفذ الخدمة المراد تقديمها وهنا يمكن استخدام المنافذ المعروفة والمستخدمة بشكل شائع او استخدام ارقام منافذ غير مستخدمة ولمعرفة الارقام المستخدمة للخدمات الشائعة يفضل مراجعة الصورة التالية:

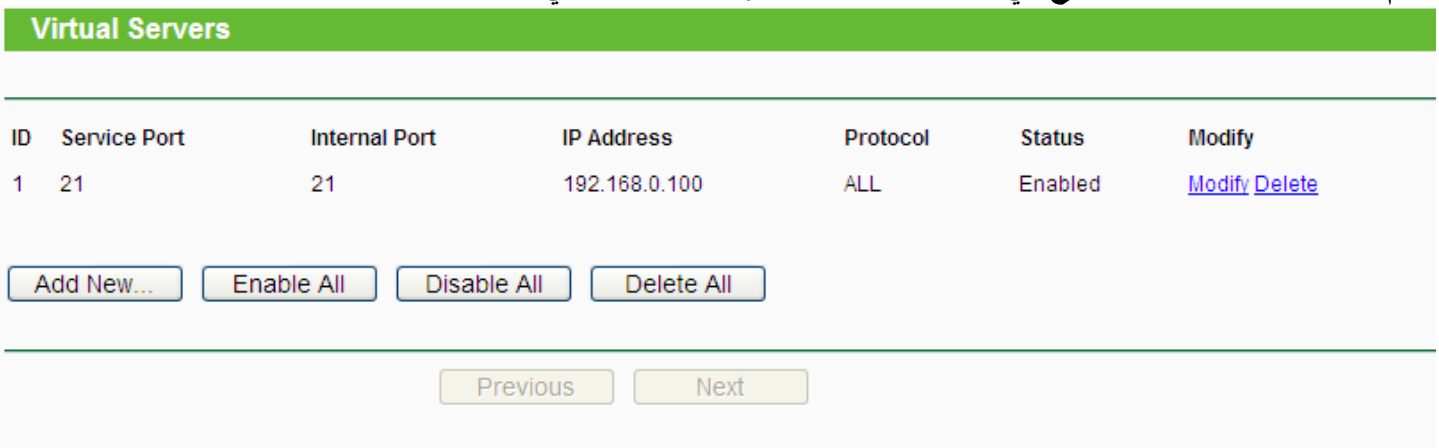


٢- (internal port) وهو رقم المنفذ الذي سيستخدم داخلياً في الشبكة المحلية للوصول الى الخادم الافتراضي ويفضل تركه فارغاً ان كنا قد استخدمنا رقم منفذ شائع من الجدول اعلاه.

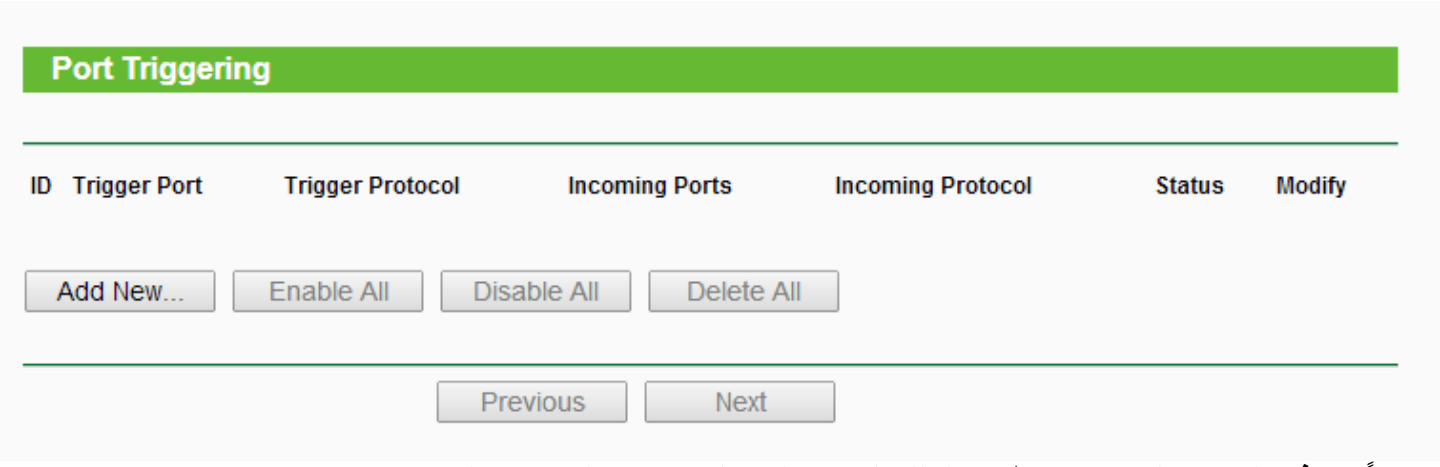
٣- (IP address): وهو عنوان الحاسوب او الجهاز الذي سيعمل كخادم افتراضي للشبكة المحلية ويفترض ان يكون هذا العنوان حقيقي (Real IP) او محجوز وثابت (reserved) لأن السيرفر في أي مكان يجب ان يكون له عنوان ثابت ليسهل الوصول اليه في أي وقت.

٤- (Protocol): وهو نوع البروتوكول الذي سيعمل عليه السيرفر حيث ان هناك نوعين رئيسيين من البروتوكولات هنا وهي (TCP, UDP) وان كنا لا نعرف أيهما نختار فنختار (ALL) أي الكل.
٥- (Status): الحالة وهل هي تمكين (enable) او ايقاف (Disable).
٦- (modify): تعديل لتغيير أي شيء من المواصفات السابقة للخادم الافتراضي بعد اكمالها وحفظها.
والان عند النقر على اضافة جديد (Add new) تظهر النافذة ادناه:

نقوم بضبط الاعدادات كما موضح في اعلاه وبعد الحفظ تظهر النافذة كما يلي:



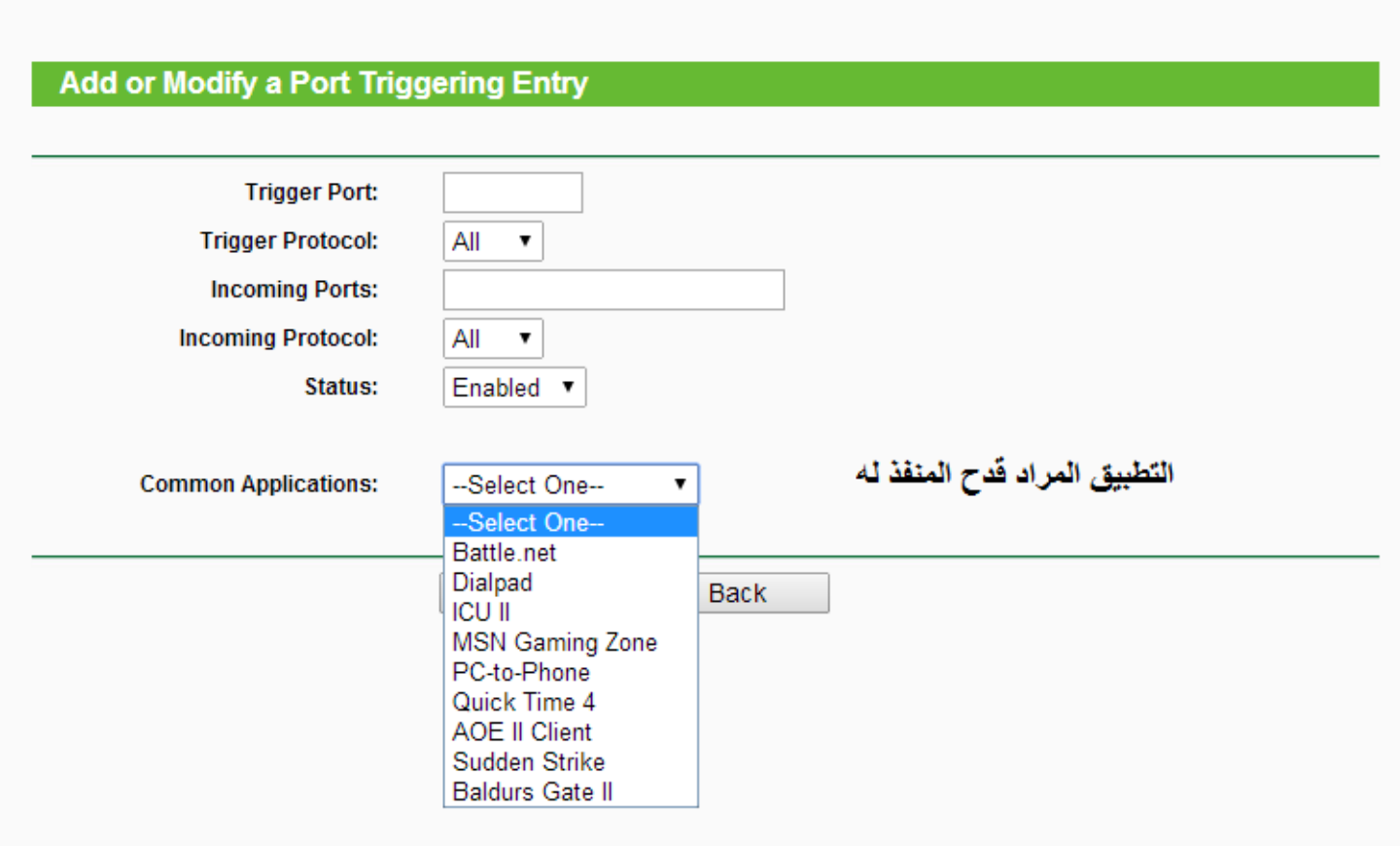
وكما هو واضح هنا نستطيع حذف الكل من (delete all) او تعطيل الكل (Disable all) او تمكين الكل (Enable all) او اضافة خدمة اخرى الى نفس الحاسوب او الى غيره من (Add new) ولا ننسى امكانية التعديل على أي حقل من زر (modify).
والان ننتقل الى الخيار الثاني وهو قدح المنافذ (Port Triggering) ويستخدم هذا الخيار لبعض انواع التطبيقات التي لا يكفيها تبادل البيانات بشكل طبيعي وانما تحتاج معاملة خاصة ولا يمكنها العمل مع ال(NAT) الطبيعي مثل المؤتمر الفيديوي (video conference) والعاب الانترنت والمكالمات الهاتفية عبر الانترنت (Internet Telephony) وعند النقر على هذا التبويب تظهر النافذة التالية:



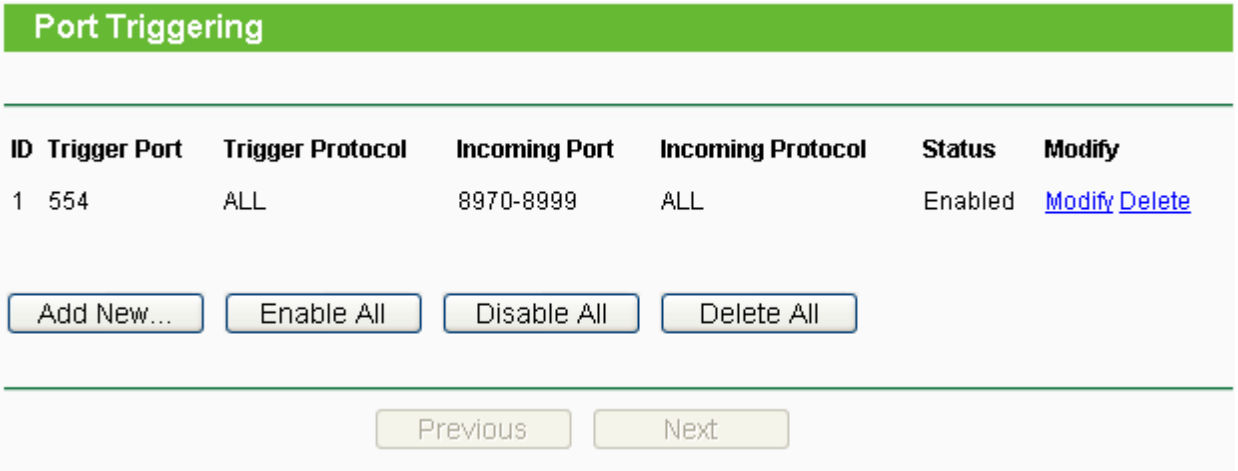
وايضاً كما في التبويب السابق نلاحظ جدول للمعلومات التي يفترض إدخالها وكما يلي:

- (Trigger port): المنفذ الخارجي الذي تخرج عليه البيانات والذي عند الاتصال به سيقدح القاعدة التي سنضبطها.
- (Trigger Protocol): بروتوكول القدح وهو اما (TCP, UDP, ALL) حسب نوع الخدمة المراد قدحها.
- (Incoming ports): المنافذ الداخلة وهي المنفذ او المنافذ التي يأتي من خلالها الاستجابة لطلب الحاسبة ضمن الشبكة لخدمة من نوع خاص تقدح المنفذ ويمكن ادخال خمس مجاميع من المنافذ شرط ان لا تتقاطع فيما بينها.
- (Incoming Protocol) : وهو البروتوكول القادم الذي قد يكون (TCP, UDP, ALL).
- (Status): الحالة وقد تكون تمكين (enable) او منع (disable).
- (modify): تعديل ننقر عليه حين نريد تعديل مواصفات منفذ القدح الذي تم خزنه سابقاً.

والان لضبط اعدادات منفذ قدح جديد ننقر على (Add new) لتظهر النافذة التالية:



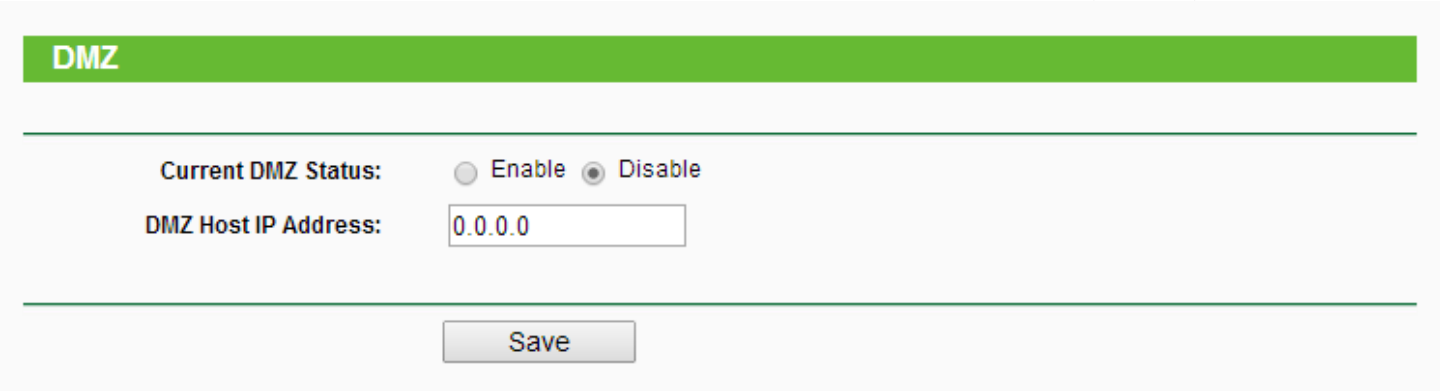
ويتم ضبط بقية الحقول كما شرحنا سابقاً والان بعد اكمال الضبط ننقر على (save) لتظهر نافذة مشابهة للتالي:



ولكن ما الذي سيحصل بعد اكمال الاعدادات؟

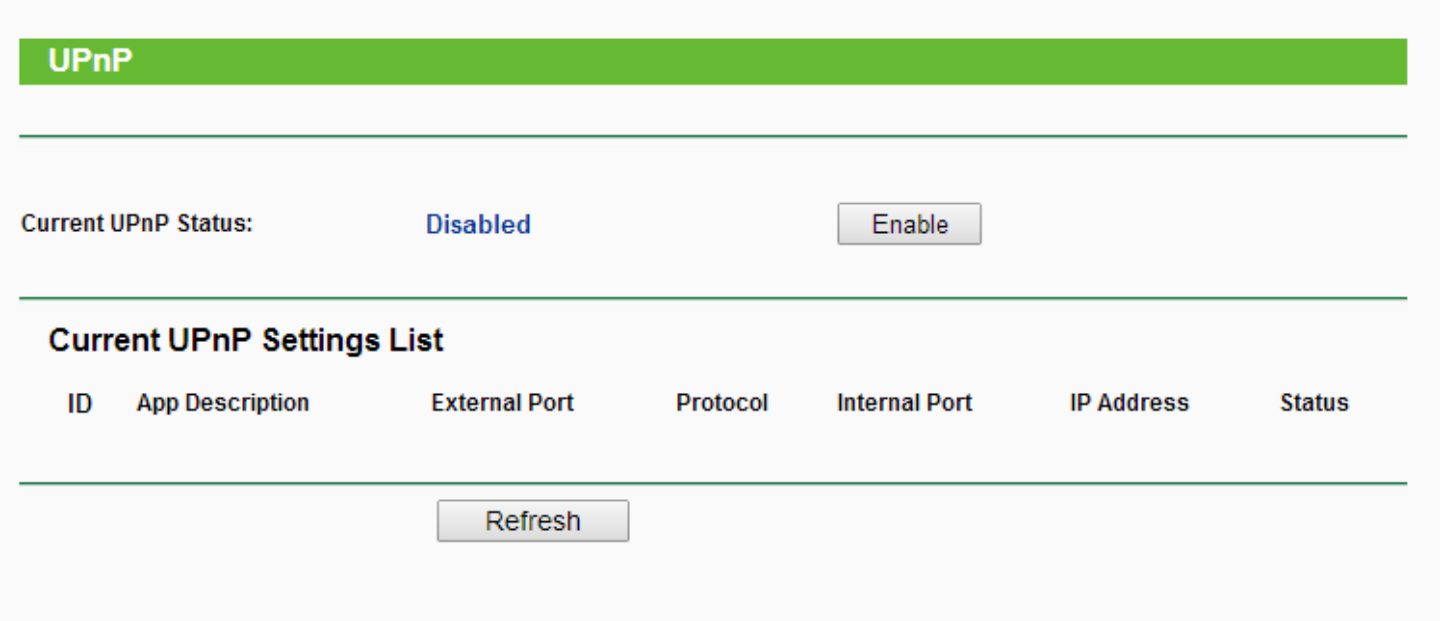
حين يقوم أحد الحواسيب في الشبكة المحلية بطلب بيانات معينة باستخدام منفذ القدح المدخل في الاعدادات وهو في مثالنا أعلاه (554) سيقوم الراوتر بتسجيل هذا الطلب وارساله عبر المنفذ المطلوب واستقبال الاستجابة بشكل خاص على أحد منافذ الدخول (Incoming ports) وعبر استخدام بروتوكول الدخول (incoming protocol) المناسب ليوصل المعلومات المناسبة الى الحاسوب الذي طلبها بشكل خاص وبالتالي ستحصل الحاسبة التي طلبت (Traffic) خاص على معاملة خاصة عبر هذه الخدمة.

- **(Demilitarized Zone DMZ): ومعناها المنطقة منزوعة السلاح أي المنطقة المعرضة للخطر والمكشوفة للأنترنت بشكل صريح وهي ميزة وخاصية نسندها الى أي حاسوب يتطلب منه اجراء مكالمات فيديوية او العاب انترنت او تقديم خدمة كخادم (server) بعنوانه الصريح وبلا جدار ناري وبلا (DHCP) وهنا يجب تعطيل خاصية ال (DHCP) للحاسوب المراد جعله (DMZ) واسناد عنوان (IP) خاص به (Reserved) كما تعلمنا سابقاً ضمن اعدادات ال (DHCP) وعند النقر على هذا التبويب تظهر النافذة التالية:**

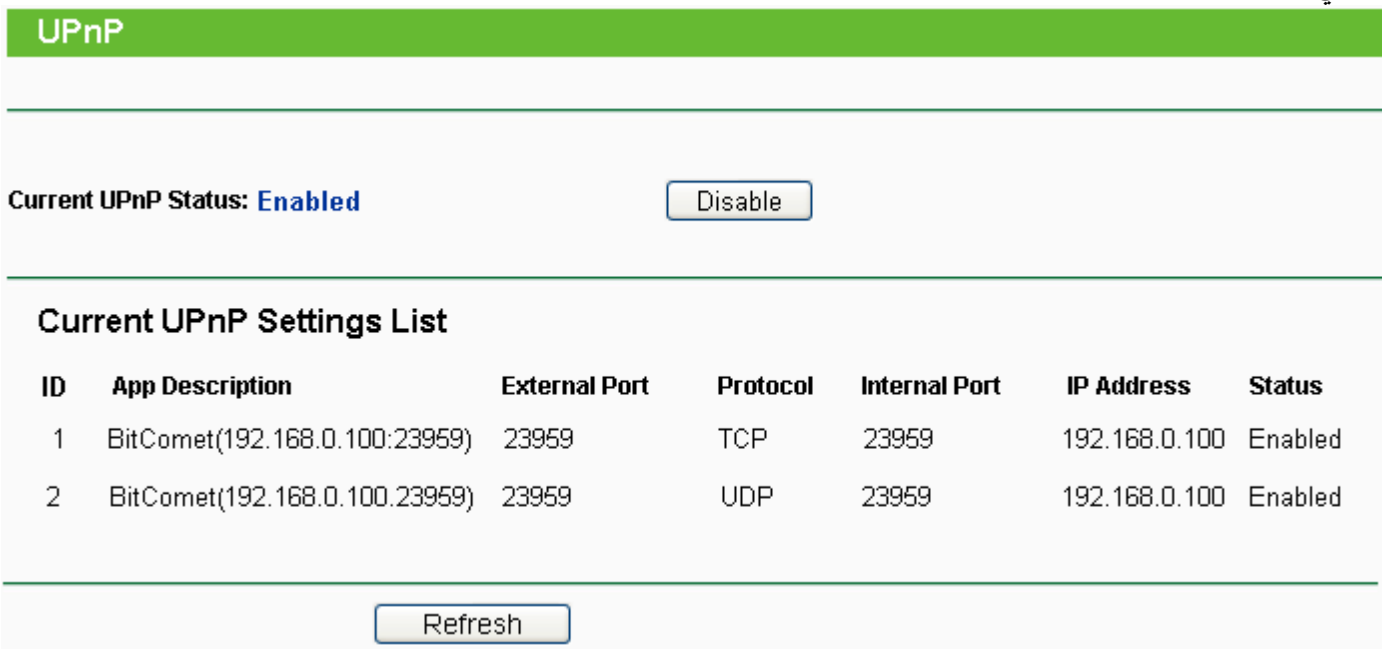


فنقوم بإضافة عنوان الحاسوب المراد كشفه للأنترنت والنقر على تمكين (enable) ثم (save) وهكذا.

- **(uPnP): وهي اختصار ل (Universal Plug and Play) أي الإضافة واللعب العالمية وهي تقنية تسمح للحواسيب التي تفعلها بالدخول عن بعد الى اعدادات ومحتويات حواسيب شخصية أخرى ونحتاج مثل هذه الخاصية عند العمل ببرامج التورينت (torrent) او برامج المحادثة المباشرة مثل السكايب (Skype) ولا تحتاج منا أي اعدادات فقط نقوم بتفعيلها وسيقوم الراوتر تلقائياً بكشف اعدادات أي تطبيق يحتاجها فيفعلها له وبالمواصفات التي تطلبها الحواسيب على طرفي الاتصال. عند النقر على تبويب (UPnP) تظهر النافذة التالية:**



ننقر على (enable) ونتركها وبعد فترة من الزمن وحين ندخل الى اعدادات الراوتر ونفتح هذا التبويب نجد شكل مشابه للتالي:

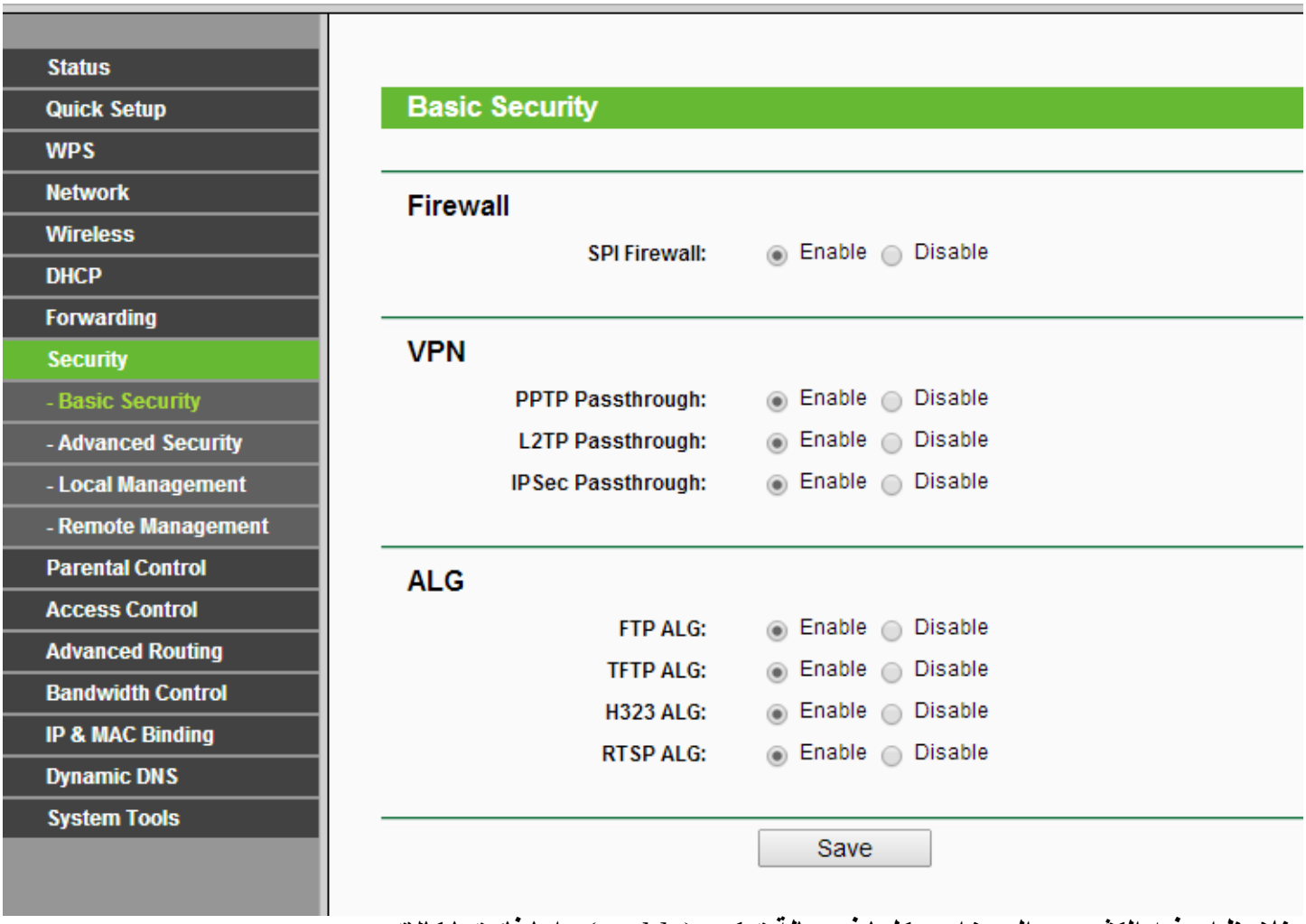


بمعنى ان هناك تطبيقين اسمهما كلاهما (BitComet) يقومان بالاتصال عبر المنفذ (23959) وأحدهما ببروتوكول (UDP) والأخر (TCP) مع الحاسوب الذي عنوانه الحالي (192.168.0.100) وحالتهما التفعيل (enable).
وهكذا نكون قد أنهينا الحديث عن تبويب التقديم الى الامام (forwarding) على امل ان نلتقيكم بدرس جديد مع تبويب اخر.

الجزء الثامن من دورة إدارة الشبكة المنزلية

وصلنا الى التبويب الأكثر أهمية في اعداد الشبكة المنزلية والمحلية وهو الأمنية (security) والذي عند النقر عليه تظهر النافذة التالية:

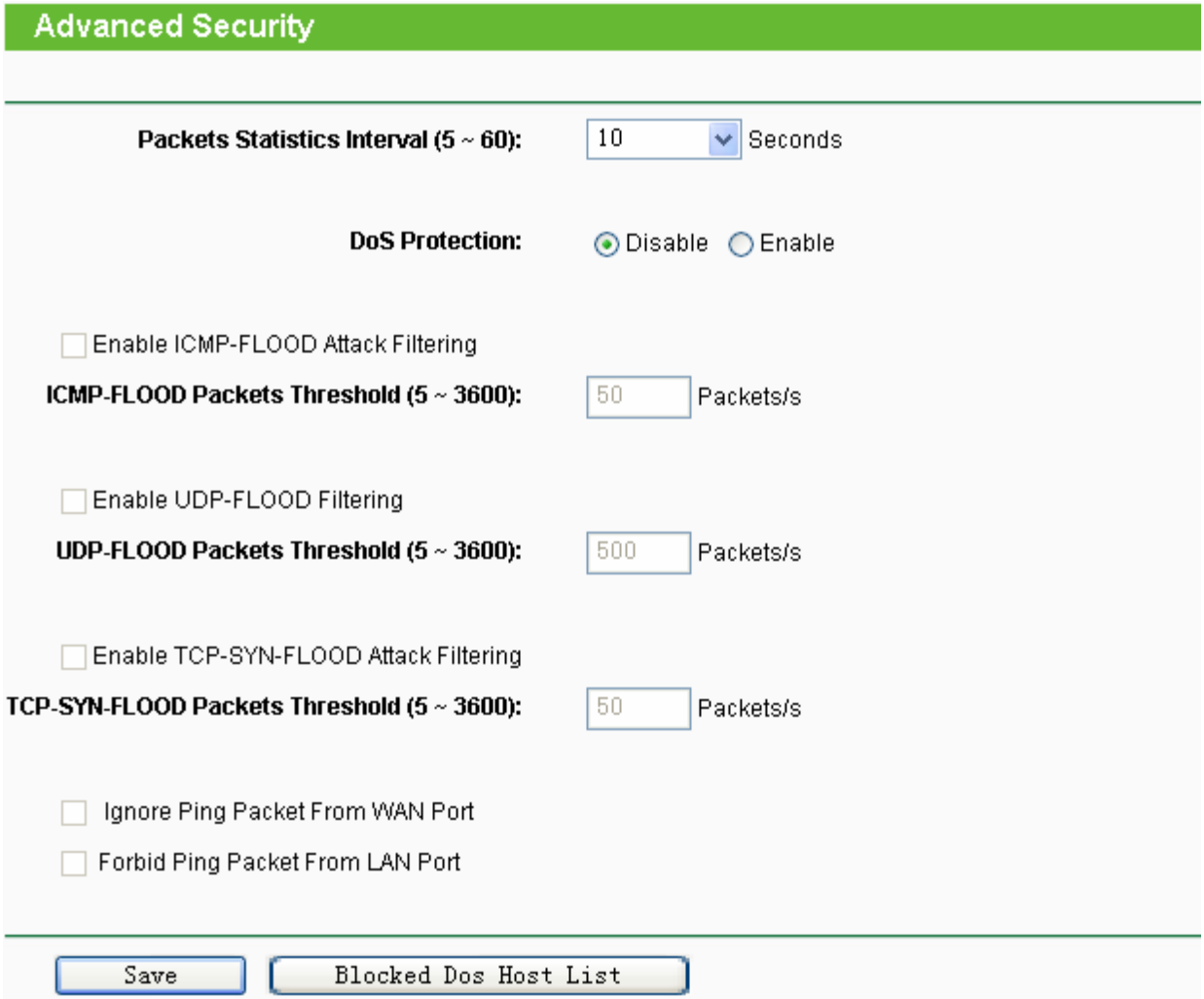
نبدأ بالتبويب الأول وهو الأمنية الأولية (basic security) والذي عند النقر عليه تظهر الخيارات التالية:



ونلاحظ ان فيه الكثير من المميزات وكلها في حالة تمكين (enable) واما فائدتها كالاتي:

- **الجدار الناري (firewall) وهو عبارة عن برمجيات تقف بين الشبكة الداخلية والشبكة الخارجية (الانترنت) وتمنع الدخول الغير مسموح به الى الشبكة الداخلية او محاولة التلاعب بمحتوياتها او الوصول المتعمد لغرض اختراق الحواسيب ضمن الشبكة الداخلية ويفضل طبعاً تمكين (enable) الجدار الناري دائماً.**
- **الجدار الناري المستخدم هنا هو من نوع (SPI firewall) بمعنى الجدار الناري الفاحص للبيانات كاملة (Stateful Packet Inspection) ويفيد في منع هجمات المخترقين على الحواسيب والسيرفرات في الشبكة الداخلية ويفضل تمكينه.**
- **الشبكة الخاصة الافتراضية (Virtual Private Network VPN) وهي عبارة عن اعدادات تسمح بخلق شبكة خاصة بين الأطراف المتباعدة لشركة واحدة او مؤسسة متعددة الفروع ولها تفاصيل كثيرة لا يسع المقام لذكرها ولكن ما يهمنا ان من تطبيقاتها هو التراسل من نقطة الى نقطة عبر نفق افتراضي (Point to Point Tunnel Protocol PPTP) و بروتوكول نفق الطبقة الثانية (Layer Two Tunneling Protocol L2TP) و امنية بروتوكول الانترنت (Internet Protocol Security IPSec) وكل منها له وظيفة خاصة سبق الحديث عنها في دروس أخرى ويفضل ان تكون جميعها في حالة تمكين (enable).**
- **بوابة طبقة التطبيقات (Application Layer Algorithm ALG) وهي البوابة التي تسمح بفلترة مخرجات ال (Network Address Translation NAT) لكافة التطبيقات ويفضل جعلها في حالة تمكين (enable) ايضاً ولكل التطبيقات.**

والان ننتقل الى التبويب الثاني وهو تبويب الأمنية المتقدمة (advanced security) والذي عند النقر عليه تظهر النافذة التالية:

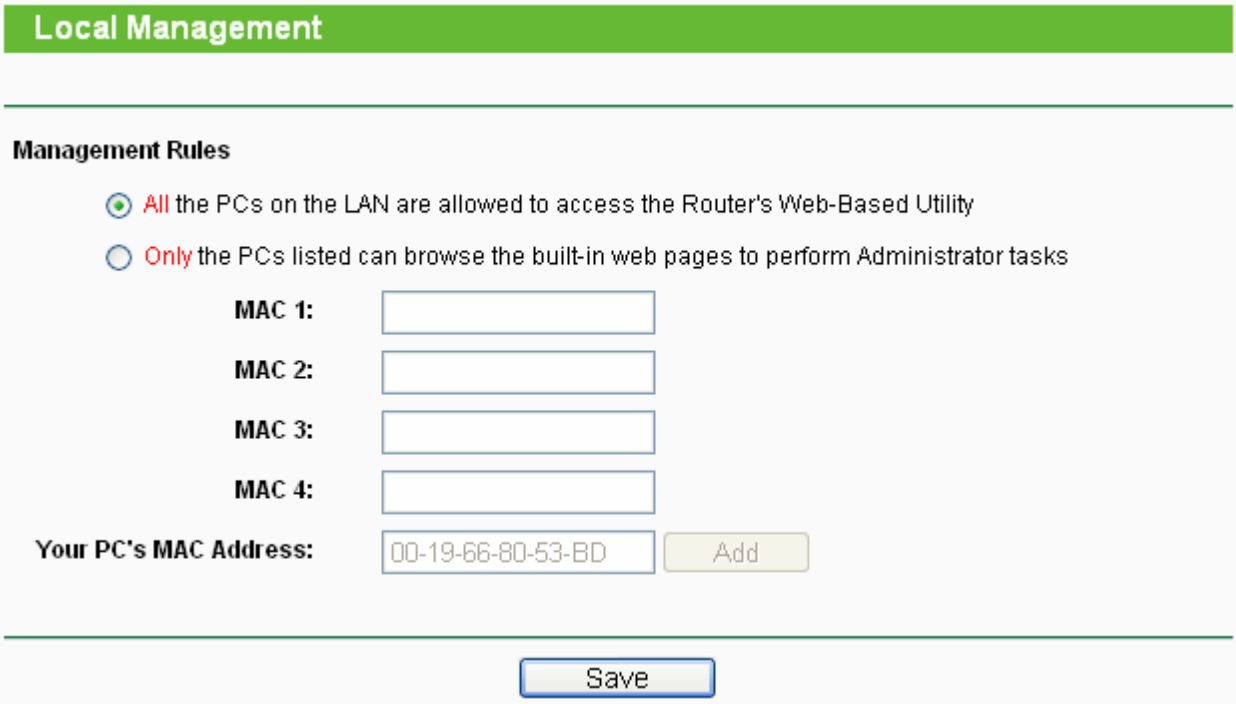


هنا نلاحظ ان كافة الخيارات غير مفعلة والسبب ان تفعيلها يتم فقط في حالة كون الشبكة الداخلية تضم معلومات مهمة ومستهدفة من قبل القراصنة المحترفين لذا يفضل عدم تفعيلها الا في الحالات الاستثنائية القصوى حين تحس كمدير للشبكة المنزلية او المحلية ان البيانات الداخلية لديك مهمة وان اختراقها او تسربها سيتسبب بأضرار خطيرة والا فترك هذه الخيارات افضل لأن كل منها يعمل على اثقال كاهل الراوتر بعبء إضافي مما يسبب تباطؤ عمله والتلكؤ وكثرة الأخطاء فيه وطبعاً كما في كل تبويب ونافذة عند اكمال التغييرات نقوم بحفظها بالنقر على (save).

ملاحظة: عند النقر على زر (blocked DoS host list) تظهر قائمة الأجهزة التي حاولت اختراق الشبكة باستخدام هجوم ال (Denial of Service DoS) وتم كشفها وفلترتها (منع دخولها).

ملاحظة: القيم الموجودة اصلاً هي القيم الافتراضية (default) التي يفضل تركها كما هي في حالة تفعيل هذه الخيارات.

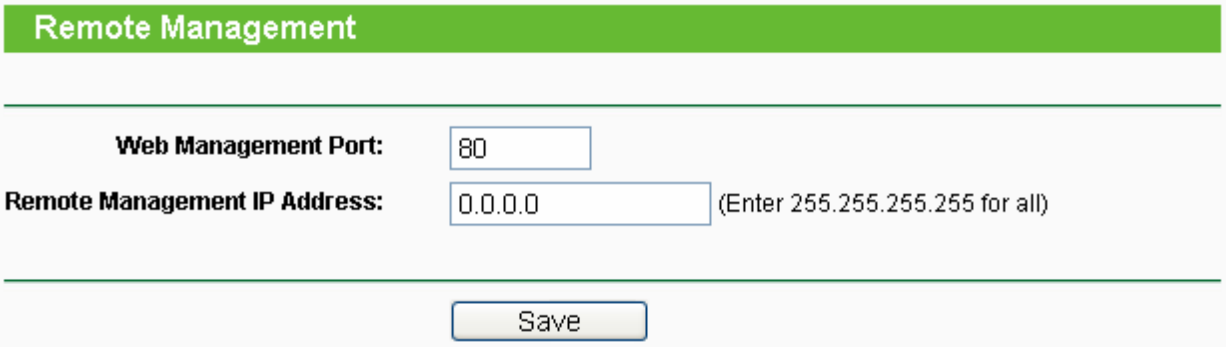
والان نصل الى التبويب الثالث وهو الخاص بالإدارة المحلية (local management) والذي عند النقر عليه تظهر الخيارات التالية:



يتركز دور هذا التبويب على إعطاء سماحية وصلاحية التحكم في الراوتر لكل الحواسيب في الشبكة الداخلية في حالة النقر على (All…..) او منح صلاحية الوصول الى هذه الصفحة من الاعدادات عبر متصفح الانترنت لحاسوب واحد او اكثر فقط في الشبكة وذلك باختيار (only…..) حيث نقوم هنا بإدخال العناوين الفيزيائية (MAC addresses) للحاسوب او الحواسيب التي نريد ان نسمح لها بالدخول الى اعدادات الراوتر وتغييرها وقد يسأل سائل هنا ويقول ان الوصول الى الراوتر مرتبط بمعرفة اسم المستخدم وكلمة المرور فما الحاجة الى هذا الخيار الإضافي للأمان؟

وللجواب على ذلك يجب ان نتذكر حقيقة ان كل اسم مستخدم وكلمة مرور هو عرضة للاختراق والتعرف عليه بشتى الطرق ولذا تصبح هذه الخاصية جدار حماية اخر ووسيلة امان للشبكة تضاف الى بقية الوسائل الأخرى من اسم مستخدم وكلمة مرور وتشفير وغيرها ولذا يفضل ان نختار الخيار الثاني (only….) ونضيف فقط العناوين الفيزيائية للحاسوب او الحواسيب التي نثق بها وبمستخدميها لعدم التلاعب بالشبكة واعداداتها. واخيراً ننقر على الحفظ (save).

والان نصل الى التبويب الأخير في صفحة الأمنية الخاصة بجهاز ال (TP-link) والتي تخص الإدارة عن بعد (Remote management**) والتي عند النقر عليها تظهر الخيارات التالية:**



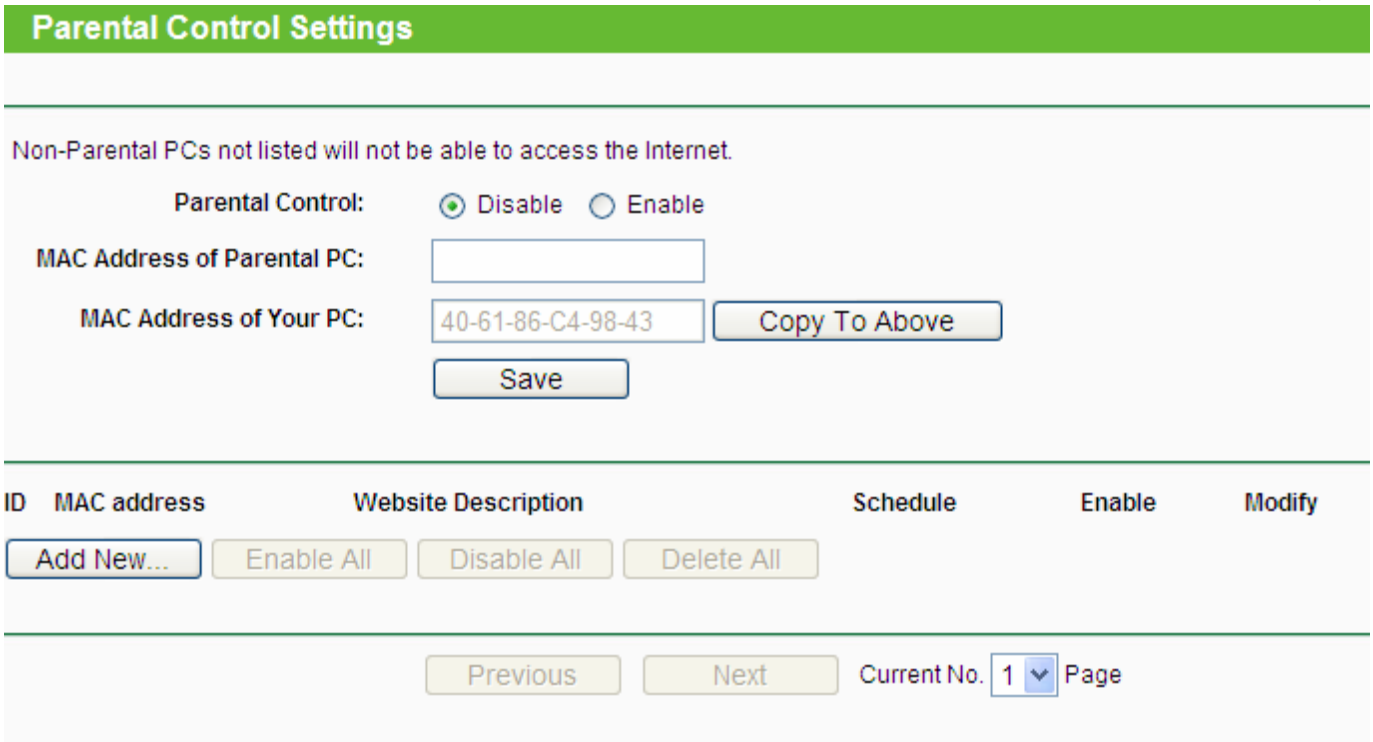
هذا التبويب يركز على التحكم بقابلية الوصول الى الراوتر عن بعد أي من خلال الانترنت وليس من خلال الشبكة المحلية وتتمثل خياراته في ضبط منفذ الإدارة الذي يمكن من خلاله الوصول عن بعد عبر بروتوكول ال (HTTP) والذي يكون عادة هو المنفذ ٨٠ ولكن لزيادة الأمنية يجب تغييره ان كنا ننوي الدخول الى الراوتر عن بعد لضبط اعداداته او الاطلاع على احصائيات الحواسيب المرتبطة به.

والان الخيار الأهم في درس اليوم وهو العنوان المنطقي (IP address) الذي نستطيع من خلاله الوصول عن بعد الى الراوتر المحلي او المنزلي ويكون معطل في الوضع الطبيعي بالعنوان (0.0.0.0) ولتفعيله نقوم بكتابة العنوان الحقيقي (Real WAN IP address**) ثم نقطتين (colon) ثم عنوان المنفذ الذي كتبناه في الأعلى فمثلاً لو كان عنوان ال (IP address) الخاص بمنفذ الوان للشبكة المحلية هو (123.123.12.12) فنقوم بكتابة هذا العنوان هنا وللدخول الى الموقع عن بعد نكتب**

في متصفح الانترنت (123.123.12.12:8080) مثلاً لو كان عنوان المنفذ هو (8080) واما اذا اردنا ان يكون لأي شخص القابلية على الوصول الى الراوتر فنكتب العنوان (255.255.255.255) والذي يعني ان الجميع يستطيع الدخول للراوتر عن بعد وبعد ادخال تلك المعلومات في شريط العنوان في المتصفح والنقر على انتر يطلب منا اسم المستخدم وكلمة المرور للراوتر ويفضل ان تكون كلمة المرور قوية لتصعب عملية الاختراق. واخيراً ننقر على الحفظ (save).

الجزء التاسع من دورة إدارة الشبكات المنزلية:

وصلنا اليوم الى شرح تبويب التحكم الابوي (parental control) والذي يعنى بالسيطرة على الوصول الى مواقع معينة في أوقات معينة والتحكم في فعاليات الأطفال على الانترنت لأن من البديهي ان تركهم بدون رقابة وتحكم قد يؤدي الى عواقب وخيمة تؤدي الى ضياعهم وضياع اخلاقهم في هذا العالم الغامض مترامي الأطراف وعند النقر على هذا التبويب تظهر النافذة التالية:

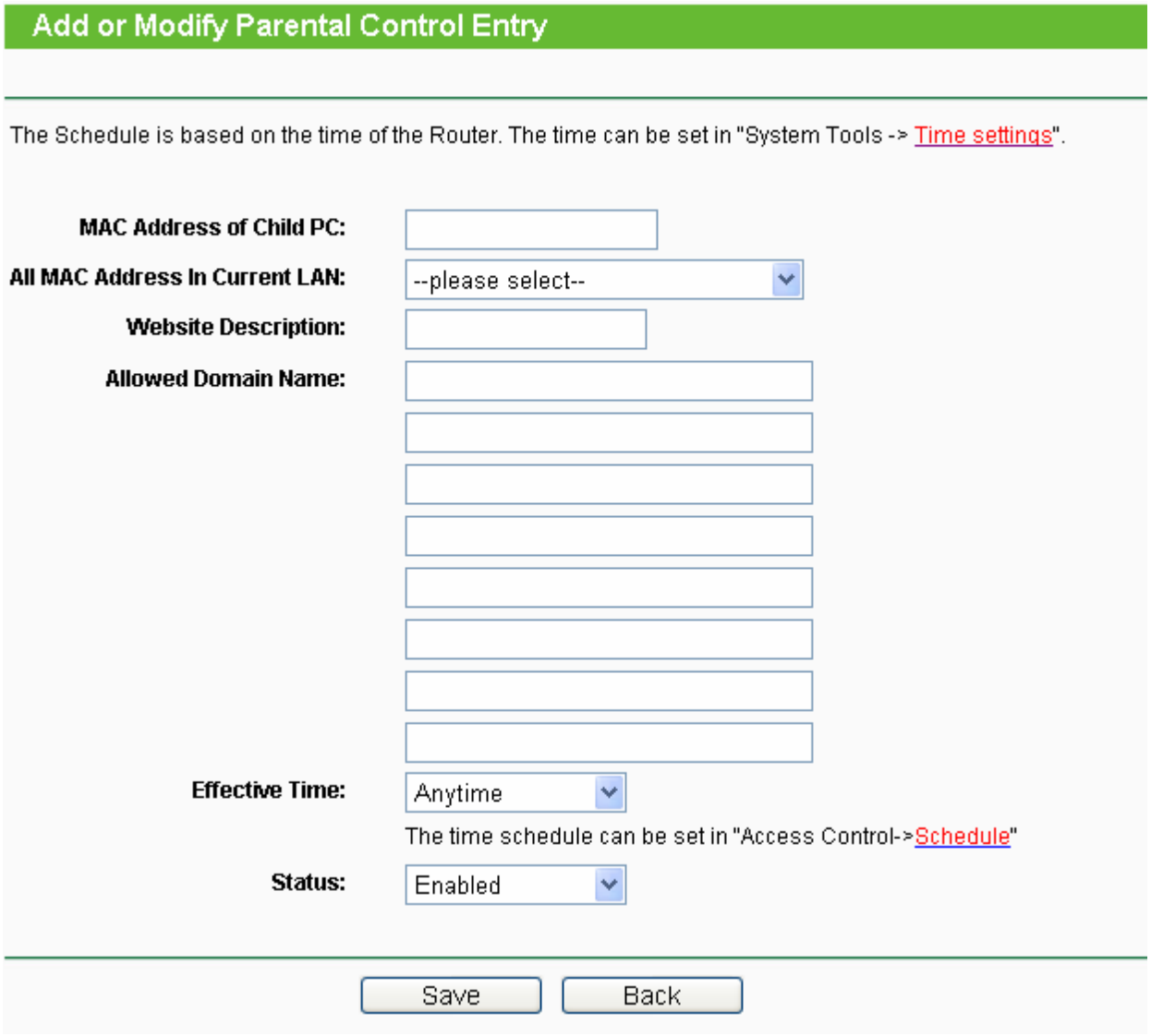


هنا نلاحظ ان الحالة الطبيعية للجهاز تعطيل (disable) التحكم الابوي ويمكننا تمكينها (enable) بالنقر على الدائرة بالقرب من كلمة التمكين (enable) لنبدأ ضبط بقية الاعدادات.

اول شيء يجب ضبطه هو ادخال العنوان الفيزيائي لحاسبة الاب (الحاسبة التي يفترض ان تسيطر على الشبكة المنزلية او المحلية وتفرض القيود على بقية الحاسبات) وهنا يمكن ادخال العنوان الفيزيائي (MAC address) يدوياً او نسخه من الحقل الأسفل منه والذي يحتوي العنوان الفيزيائي للحاسوب الحالي (MAC address of your computer) ويمكن مباشرة نسخه الى الحقل العلوي بالنقر على زر (copy to above) أي النسخ الى الأعلى ثم النقر على (save) لحفظ التغييرات.

والان لحد الان نحن لم نفرض أي قيود ولم نسيطر على أي تصفح فأين يجب ان نبدأ؟

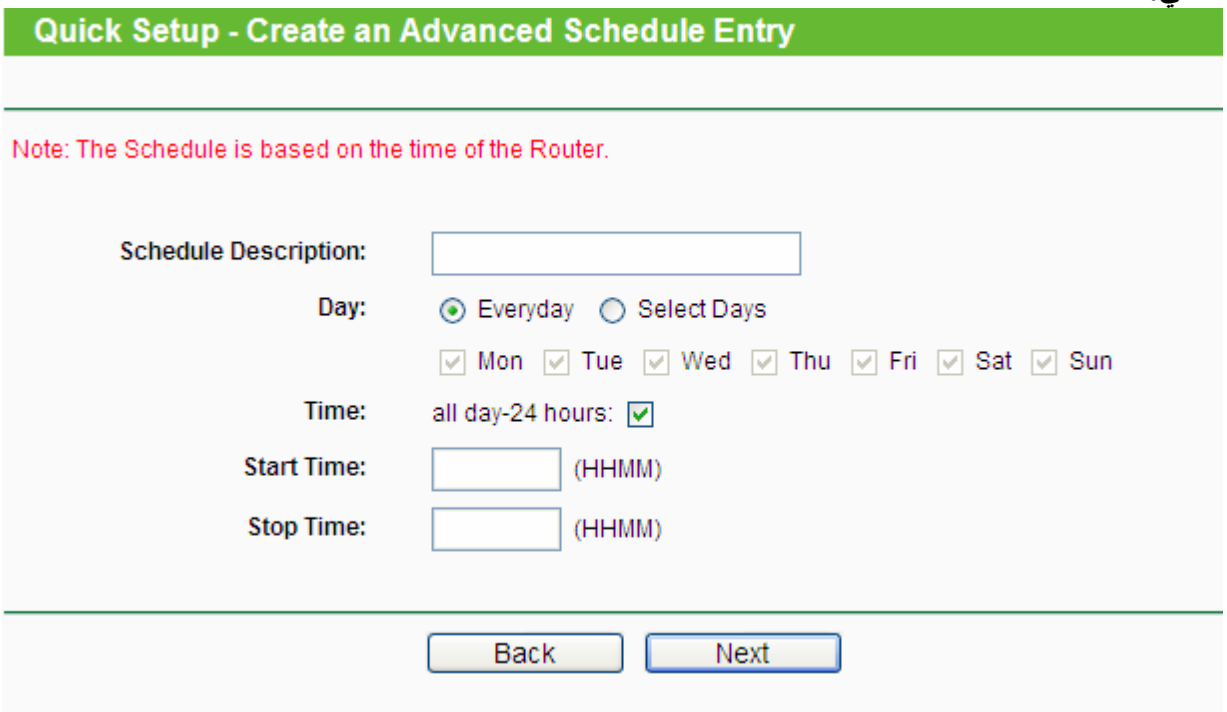
يبدأ عملنا بالنقر على زر إضافة جديد (Add new) لتظهر النافذة ادناه والخاصة بأول حاسبة نريد التحكم في استخدامها للأنترنت وكما يلي:



هنا في اول حقل نقوم بإدخال العنوان الفيزيائي للحاسوب الذي نريد ان نطبق عليه السيطرة والتحكم الابوي ونستطيع معرفة العنوان الفيزيائي للحاسوب المعني من الذهاب الى تبويب (DHCP) ثم الى (DHCP client list) حيث تظهر لنا نافذة مشابهة للتالي:

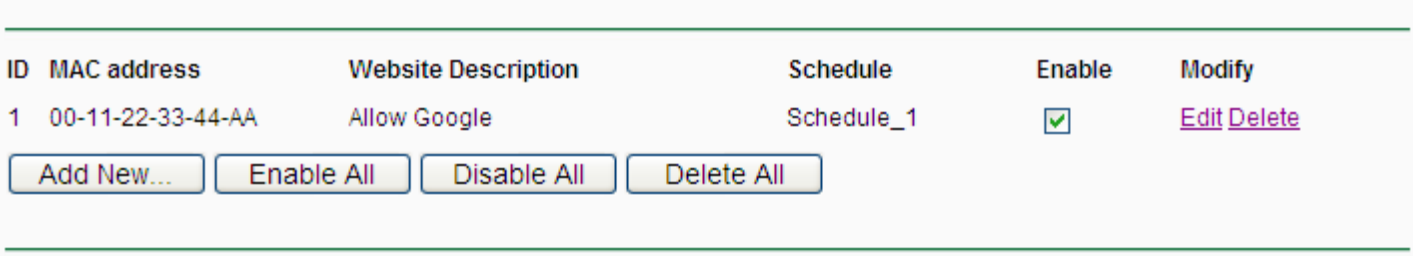
وهنا نرى اسم الحاسوب (client name) والعنوان الفيزيائي المقابل له (MAC address) ونستطيع رؤية كافة العناوين الفيزيائية من القائمة المنسدلة في النافذة قبل السابقة تحت عنوان (All MAC addresses in the current LAN) ونختار منها العنوان المراد التحكم به ثم نعطي وصف للمواقع التي نريد التحكم في الوصول لها في شريط (website description) ثم نقوم بكتابة عناوين المواقع المسموح بتصفحها كاملة او جزئية أي اننا نستطيع كتابة (www.google.com) او نكتب فقط (google) ثم نختار الوقت الذي نريد السماح للحاسوب المعني بالتصفح خلاله من القائمة المنسدلة في خيار (effective time) حيث ان هناك عدة جداول زمنية متاحة وان لم يعجبك أي منها ولم يتوافق مع

ما تصبو اليه فيمكن ضبط جدول زمني خاص بك بالنقر على تبويب (schedule) والذي عند النقر عليه تظهر نافذة مشابهة للتالي:



وهنا نستطيع إعطاء وصف للجدول (schedule description) وتحديد الوقت المراد للتحكم كل يوم (everyday) او أيام محددة (select days) وكذلك الوقت بالساعات من وقت البدء (Start time) ووقت النهاية (stop time).
وبعد الانتهاء من ضبط الجدول ننقر على (next) ثم نعود الى واجهة السيطرة الابوية وندخل الى الزمن الفعال (Effective time) فنجد ان الوصف الجديد الذي اضفناه قد أصبح ضمن الخيارات المتاحة فنختاره واخيراً ننقر على تمكين (enable) لهذه الاعدادات ونحفظ التغييرات بالنقر على (save) وفي ادناه مثال عملي لما تم شرحه:
مثال: إذا أردنا ان نجعل الحاسوب الذي عنوانه الفيزيائي (00-11-22-33-44-AA) يدخل الى موقع الكوكل في أيام السبت فقط ومن خلال حاسوب مدير الشبكة الذي عنوانه الفيزيائي هو (00-11-22-33-44-BB) فنقوم بفعل التالي:

١- ندخل الى تبويب التحكم الابوي ونكتب عنوان حاسوب مدير الشبكة في اول حقل ونحفظ التغييرات.
٢- ندخل على تبويب التحكم بالوصول (access control) ومنه الى تبويب الجداول ونقوم بإعطاء اسم للجدول واختيار يوم السبت فقط ونسمي الجدول (schedule_1) ونحفظ التغييرات.
٣- الان نعود الى تبويب التحكم الابوي ونقوم بالنقر على (add new) وندخل المعلومات المطلوبة كما تم شرحها وحفظ التغييرات لتظهر نافذة مشابهة للتالي:



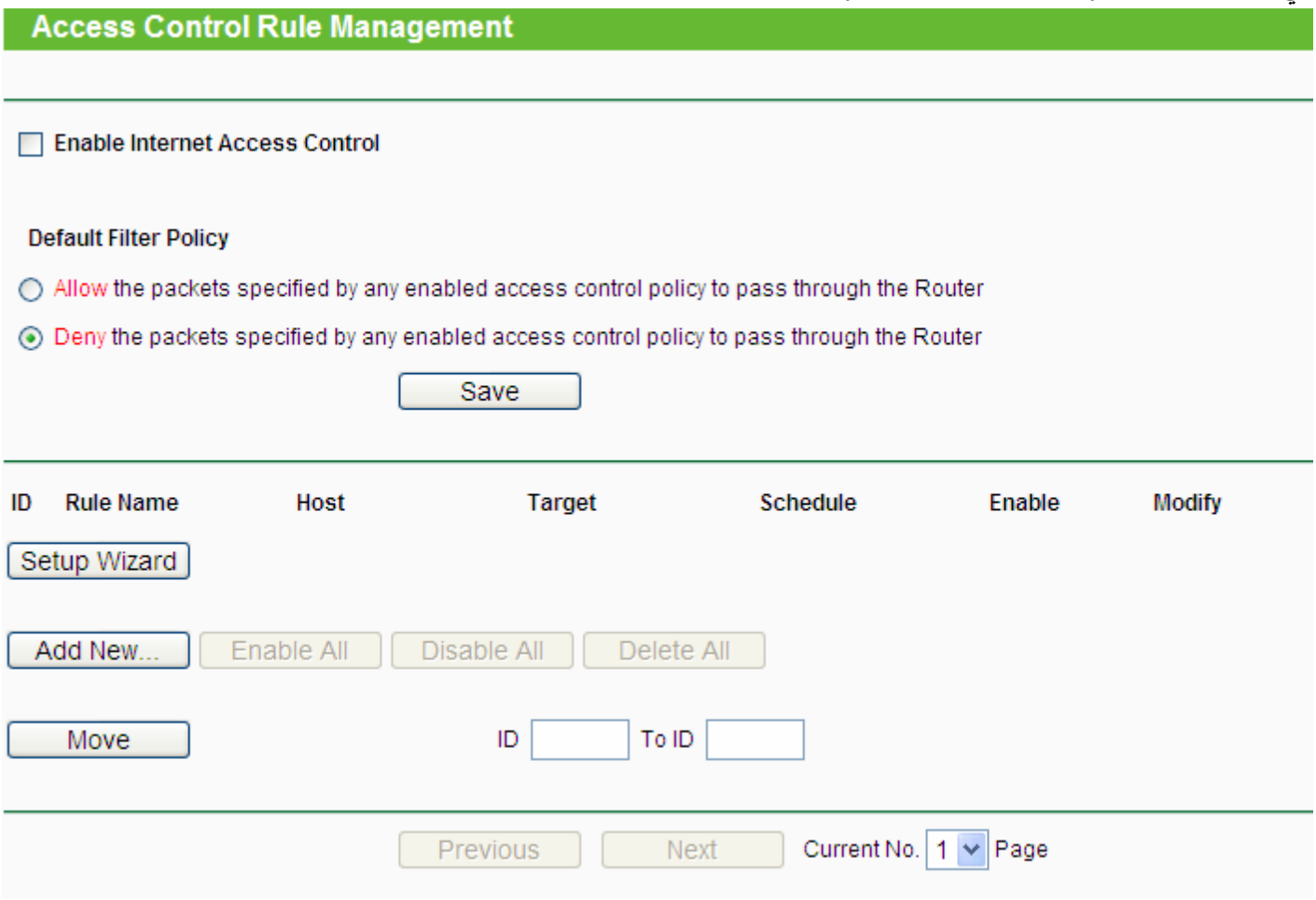
وطبعاً كما في كل النوافذ فأن تمكين الكل (enable all) وتعطيل الكل (disable all) وحذف الكل (delete all) هي خيارات متاحة دائماً.

الجزء العاشر من دورة إدارة الشبكات المنزلية

التحكم بالوصول (access control)

يمكننا هذا الخيار من التحكم بالوصول الى أي موقع او حاسوب او أي جهاز اخر داخل وخارج الشبكة من خلال ضبط مجموعة من الاعدادات وكما يلي:
عند النقر على هذا التبويب تظهر عدة خيارات هي:

الخيار الأول هو القاعدة (rule) او القانون او المقياس الذي يتم على أساسه السماح او المنع من الوصول الى موقع معين في الشبكة او خارجها وعند النقر عليه تظهر الخيارات التالية:

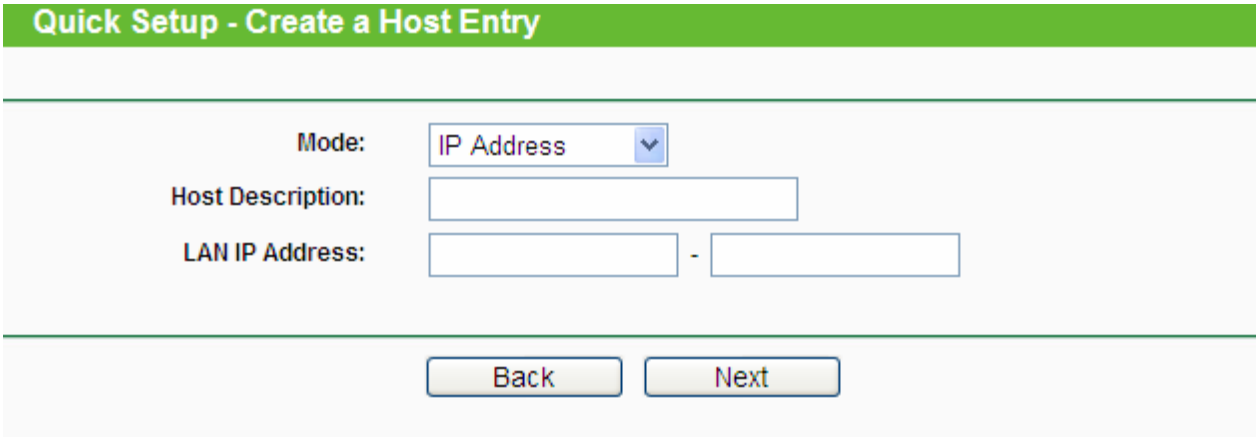


هنا نجد مجموعة من الخيارات أهمها:

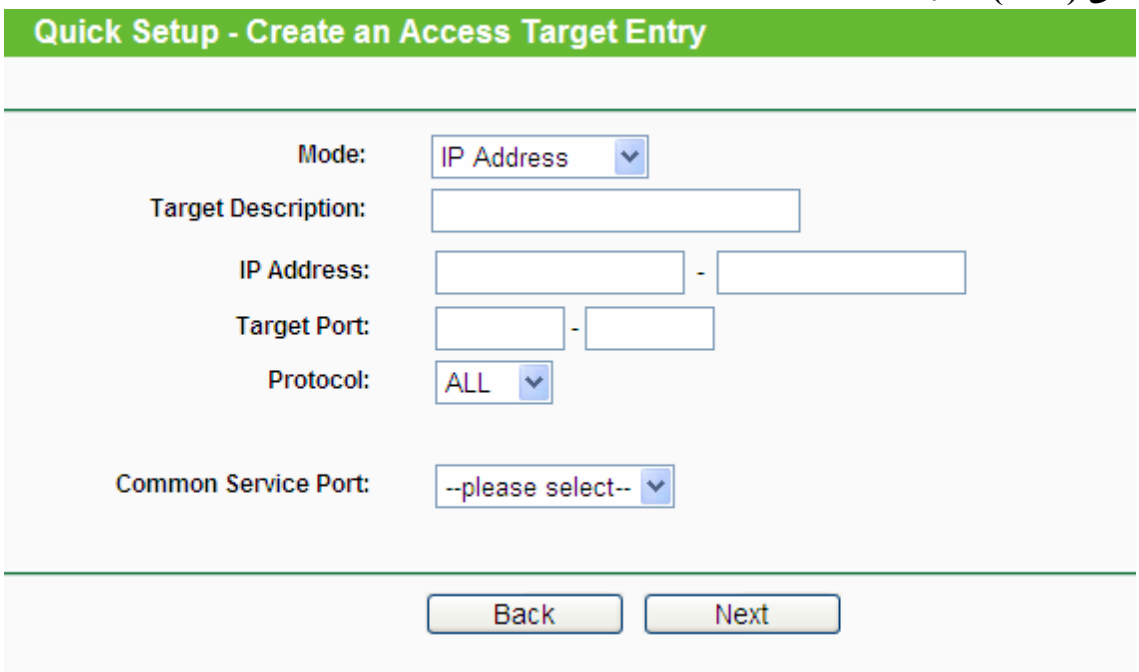
- **تمكين التحكم بالوصول الى الانترنت (enable internet access control) ويجب تفعيل هذا الخيار ان اردنا ان نسمح بالتحكم بالوصول بالنقر بداخل المربع بجواره.**
- **(allow, deny) وتعني السماح او المنع للبيانات التي سنجدد مصدرها وهدفها في هذه القاعدة فأن اردنا لنوع معين من المرور (Traffic) العبور عبر الراوتر نضغط على (allow) وان اردنا منع نوع معين من المواقع او البيانات من العبور عبر الراوتر نضغط على (deny).**
- **بعد أي تغيير يجب الحفظ (save).**
- **والان توجد طريقتين لأضافة قاعدة للتحكم بالوصول اما اتباع الدليل التعريفي (setup wizard) او إضافة جديد وضبط كافة الخيارات يدوياً.**
- **وكالعادة تتواجد ازرار حذف الكل وتمكين الكل وتعطيل الكل كما شرحناها سابقاً.**

والان نأتي الى الطريقتين الواجب اتباع احدهما لضبط قاعدة التحكم بالوصول:

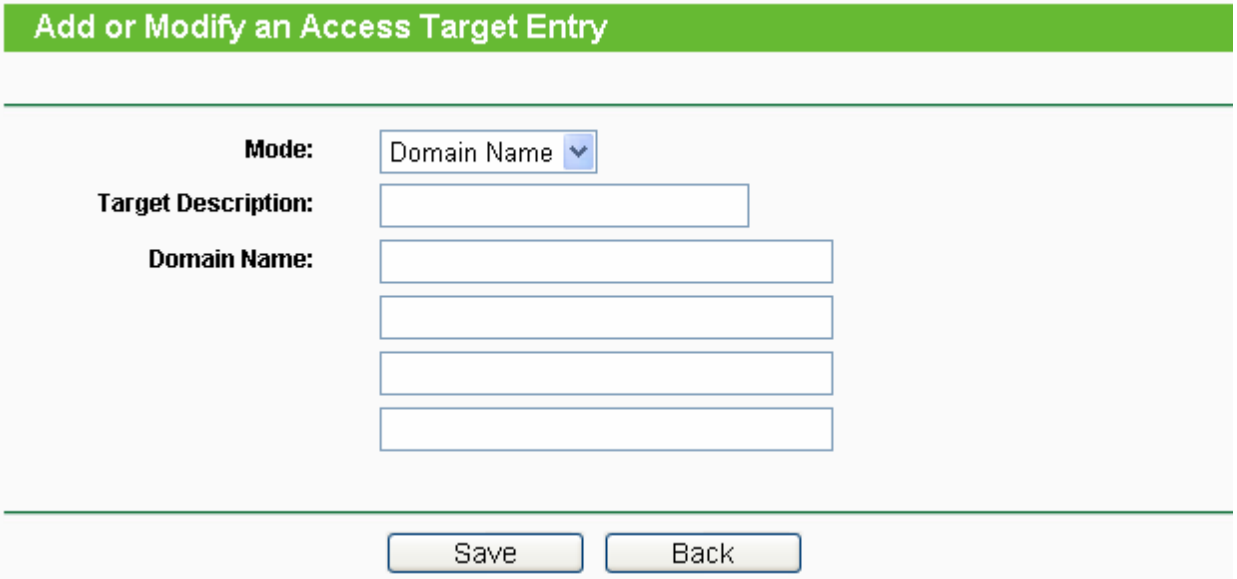
الطريقة الأولى (setup wizard): والتي عند النقر عليها تظهر النافذة التالية:



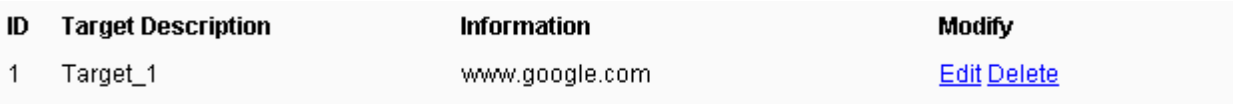
هنا نقوم بضبط نمط (mode) **التحكم هل هو بأستخدام ال** (IP address) **او** (MAC address) **ونعطي وصل للحواسيب المراد التحكم في الوصول لها** (host description) **ونعطي العنوان حسب الاختيار في حقل** (LAN IP address) **ثم ننقر على** (next) **لتظهر النافذة التالية:**



وهنا نحدد نمط (mode) **العناصر المراد الحكم في الوصول لها وهل نعرفها من عنوانها ال** (IP address) **او اسم الموقع** (domain name) **ونحدد وصف لتلك المواقع** (target description) **وحيز عناوين ال** (IP address) **اذا كانت مجموعة من العناوين لموقع واحد او مجموعة مواقع ثم نحدد المنفذ** (port) **المستخدم من قبل ذلك الموقع وهنا نحن نعرف من الدروس السابقة التطبيقات والبروتوكولات الشهيرة ورقم المنفذ لكل منها (مثلاً** FTP=21**) ثم نحدد البروتوكول هل هو** (TCP, UDP, ALL) **واخيراً نحدد منفذ الخدمة المراد التحكم بالوصول لها من القائمة المنسدلة للخيار (** common service port**) ثم ننقر على** (next) **لتظهر النافذة التالية:**

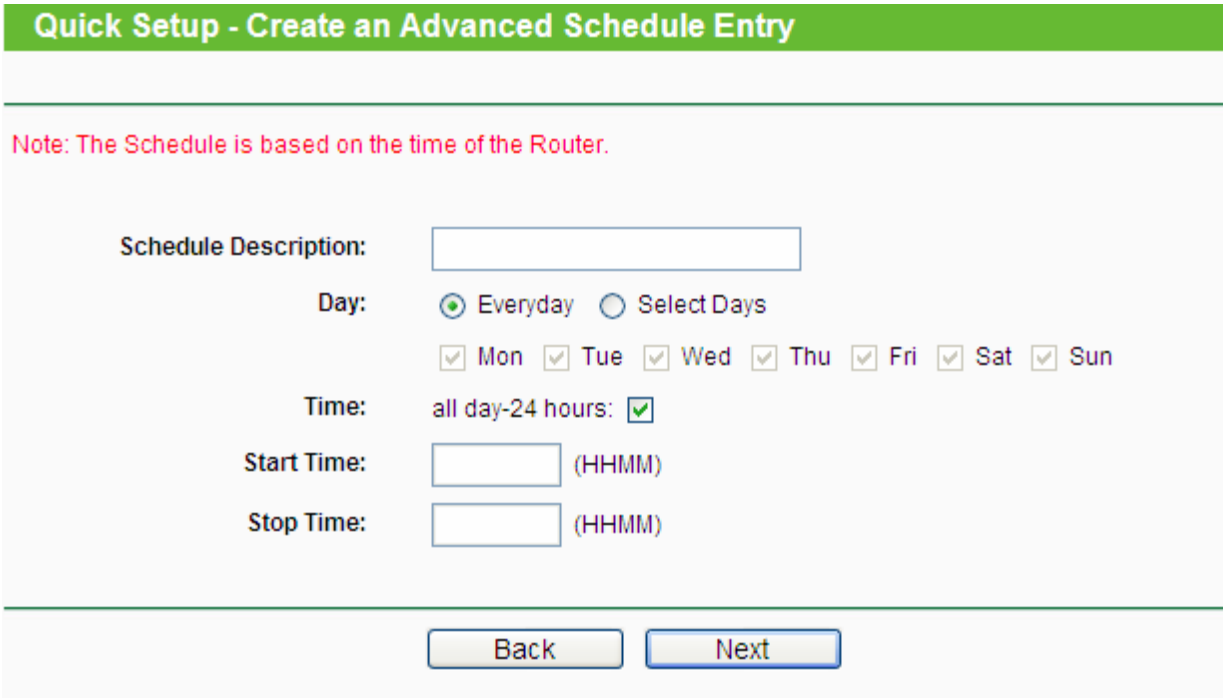


هنا لو اخترنا في النافذة السابقة تعريف الموقع الهدف (target) بدلالة اسم الموقع ستظهر لنا هذه النافذة لتعريف وصف للهدف (target description) أي إعطاء اسم للموقع او المواقع التي نريد تمكينها او حجبها ولتكن مثلاً (bad-sites) ثم ننقر على (save) فمثلاً لو أردنا حجب موقع الكوكل فأننا نكتب في ال (domain name) العنوان التالي (www.google.com) لتظهر النافذة التالية بعد الحفظ واكمال بقية الاعدادات:

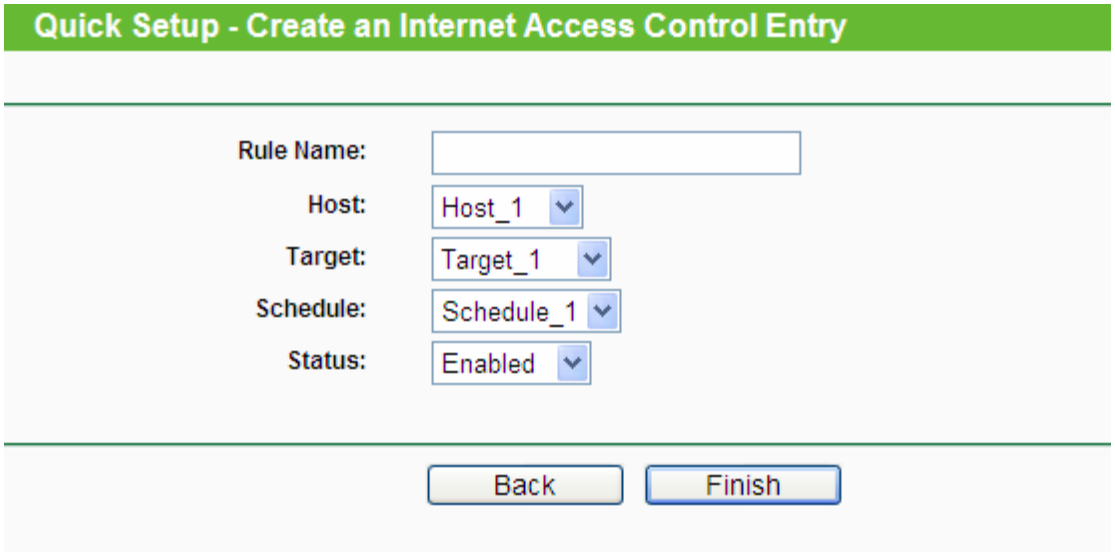


ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

والان ننقر على (next) لتظهر النافذة التالية الخاصة بعمل جدول (schedule) لتنفيذ هذه القاعدة (rule):



نعطي وصف او اسم للجدول في (schedule description) ونحدد اليوم (Day) او الأيام المطلوب تنفيذ هذه القيود فيها ثم نحدد الساعات ضمن اليوم الواحد من موعد البداية (start time) وموعد الانتهاء (stop time) ثم ننقر على (next) لتظهر النافذة التالية:



هذه النافذة الأخيرة في ضبط الاعدادات بحسب الدليل (setup wizard) ونحدد فيها اسم القاعدة المراد تطبيقها (rule name) واسم او وصف الحواسيب المراد تطبيق القاعدة عليها (host) واسم او وصف الموقع او المواقع المراد التحكم في الوصول لها (target) وجدول التنفيذ (schedule) واخيراً الحالة تمكين (enabled) او منع (disabled) واخيراً ننقر على (finish) وهذا كل ما يخص الطريقة الأولى والتي تتكون بأختصار من:

١- تعريف الحواسيب التي تريد تقييد دخولها الى مواقع معينة (host).
٢- تعريف المواقع التي تريد تقييد الوصول اليها (target).
٣- تحديد موعد تنفيذ او جدول تنفيذ هذا التقييد (schedule).
٤- تعريف قاعدة التحكم (rule) وهل هي منع (deny) او سماح (Allow).

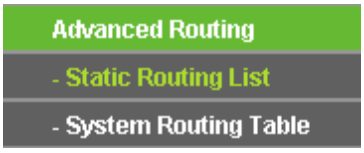
اما بخصوص الطريقة الثانية فقد تم شرحها في مقال سابق تحت عنوان (حجب مواقع معينة باستخدام الراوتر المنزلي (TP-Link router).

الجزء الحادي عشر من دورة إدارة الشبكات المنزلية

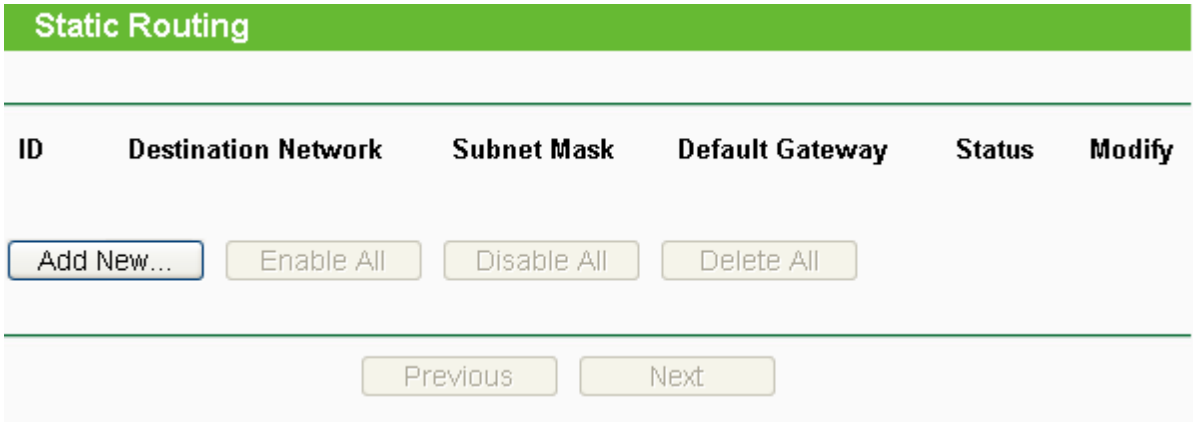
التوجيه المتقدم (Advanced Routing)

كما كرنا سابقاً فأن أجهزة ال (TP-Link) تحتوي الكثير من الوظائف المعطلة والتي لا يكترث لها المستخدمون ربما بسبب صغر الشبكات التي يستخدمونها او قلة الحمل على تلك الأجهزة مما لا يؤدي الى اضعاف الخدمة بسبب عدم ضبط الاعدادات المتقدمة ولكن على كل حال يحتاج المستخدم المحترف الى معرفة وتطبيق كل الخيارات المتاحة وحسب الحاجة ولما كانت هذه الأجهزة تسمى موجهات (routers) رغم كونها تؤدي وظيفية اكثر من ذلك بكثير فأن من اهم خصائصها توفير قابلية التوجيه والتي سندرس كيفية ضبط اعداداتها هنا ان شاء الله فأبقوا معنا:

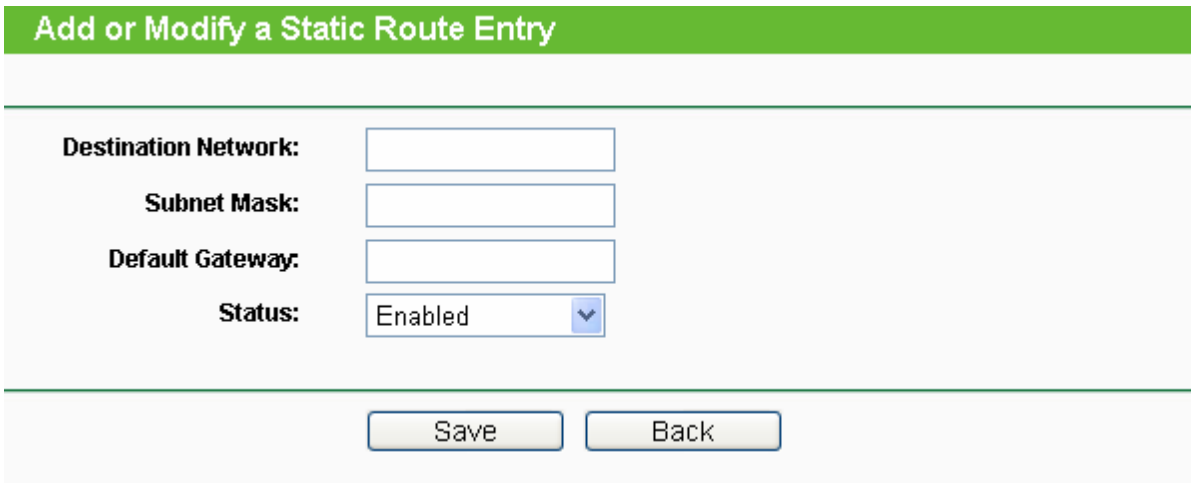
بعد النقر على هذا التبويب ستظهر النافذة التالية:



والان عند النقر على التبويب الخاص بقائمة التوجيه الثابت (static routing list) تظهر النافذة التالية:



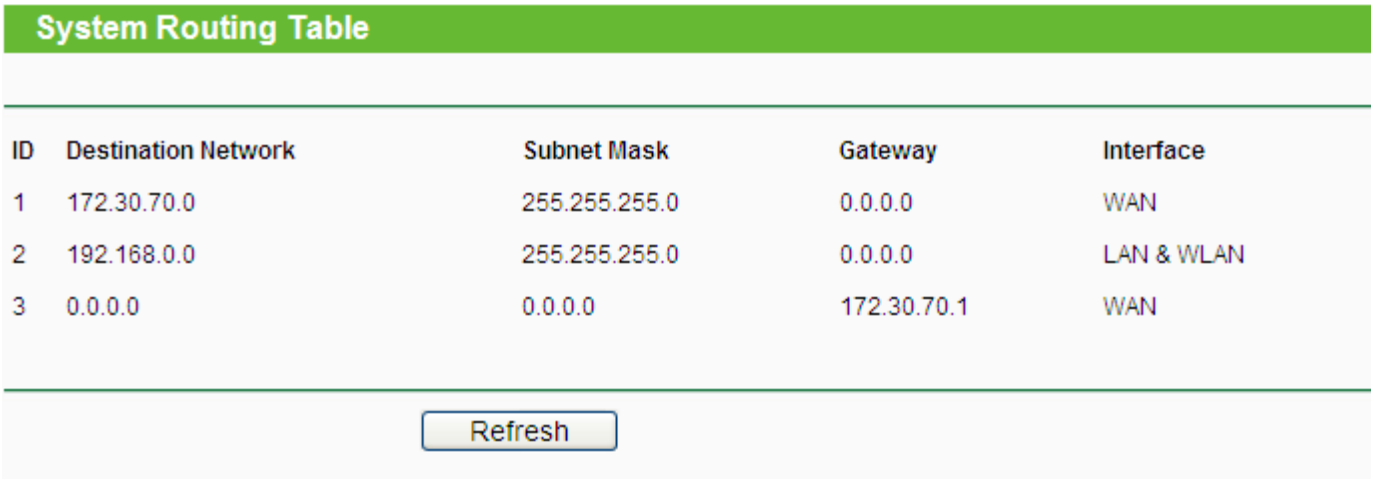
هنا نستطيع إضافة مسارات او وجهات (routes) ثابتة لنوع معين من البيانات او نوع خاص من الأجهزة يتم ضبطها مسبقاً قبل بدء عمل الشبكة لغرض إيصال البيانات الى وجهتها المقصودة عبر مسار محدد مسبقاً (predefined route).
كما هو واضح فأن قائمة المسارات الثابتة تكون فارغة مبدئياً ونستطيع إضافة مسار ثابت جديد بالنقر على (add new) لتظهر النافذة التالية:



والان قبل شرح هذه الخصائص فقط لنتصور ما الذي نريد فعله؟
نحن نريد ان نقول للبيانات الذاهبة الى شبكة معينة عبر منفذ معين ان تتبع مسار معين ومن هنا سنقوم بضبط تلك المعلومات وكما يلي:

- عنوان الشبكة المعنية (destination network) وهو عنوان الشبكة او الحاسوب الذي نريد تخصيص مسار ثابت له.
- قناع الشبكة (Subnet mask) كما هو معلوم في عالم ال (IP address) فأنه لا يمكن استخدامه بشكل صحيح بدون قناع الشبكة الذي يحدد الجزء الخاص بالشبكة (network address) والجزء الخاص بالاجهزة (host address).
- بوابة الشبكة (default gateway) وهو عنوان المنفذ الذي ستعتمده البيانات كمسار ثابت تمر من خلاله الى الوجهة المطلوبة وهو عادة نفس عنوان ال (WAN address) الذي يربط الراوتر بالهوائي الذي يستلم خدمة الانترنت لتوزيعها وفي حالة كون الشبكة سلكية فهو نفس عنوان الجهاز الذي يربط راوترنا بالشبكة العالمية.
- حالة المسار (enable or disable) وتعني التمكين او المنع وقد سبق شرحها في الدروس السابقة وتفيد في حالة وجود مسار محدد نريد تعطيله لهدف ما.
- بقية الاعدادات المعروفة من تمكين الكل (enable all) وتعطيل الكل (disable all) وحذف مسار محدد (delete) او حذف الكل (delete all) متوافرة ايضاً.

جدول توجيه النظام (System Routing Table)
وحين النقر عليه تظهر النافذة المشابهة للتالي:



وهنا ستتوضح الأمور اكثر فالجدول يستخدم فقط للعرض وليس للتعديل وفائدته ان يوضح للمستخدم ان الشبكة الداخلية مثلاً المربوطة على المنفذ (interface) المسمى (LAN & WLAN) يمكن الوصول اليها عبر العنوان (192.168.0.0) وقناع الشبكة من الكلاس (C) وهو (255.255.255.0) وهذا هو العنوان التلقائي المحلي للراوتر والذي نستطيع الوصول اليه من الشبكة المحلية من خلاله وهو (192.168.0.1) واما الشبكة العالمية (الانترنت) فيمكن الوصول اليه عبر منفذ (interface) ال (WAN) والذي عنوانه (172.30.70.0) وبنفس قناع الشبكة السابق وهو عنوان الجهاز الذي يربط راوترنا بالانترنت وطبعاً هذه الأرقام غير ثابتة بل تتبدل من جهاز لأخر وحسب حالة الشبكة.

واخيراً يتضح لنا كيف تتصل الشبكة المحلية بالعالم الخارجي من خلال بوابة الشبكة (gateway) وهي نفس عنوان ال (WAN) والذي يساوي هنا (172.30.70.1).

ملاحظة: قد يسأل سائل هنا ويقول ما الفرق بين عنوان شبكة ال (WAN) الذي ينتهي بصفر وبين عنوان بوابة الشبكة (gateway) والذي ينتهي بواحد؟

الجواب احبتي ان الأول هو عنوان شبكة يعني يشمل عناوين كل الأجهزة التي تتراوح عناوينها بين (172.30.70.1) ولغاية (172.30.70.254) اما الثاني فهو عنوان حاسوب واحد او جهاز واحد وظيفته ربط الشبكة المحلية بالانترنت.

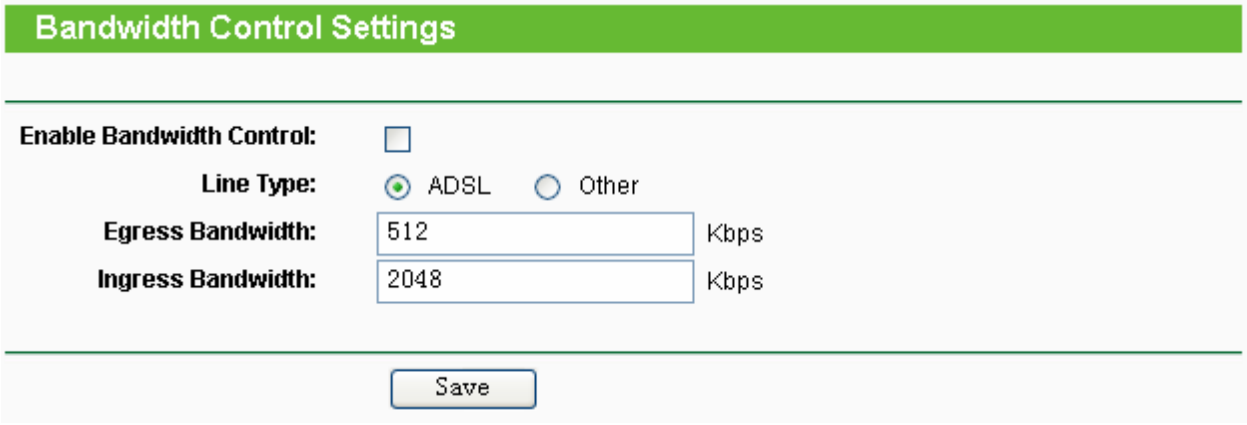
الجزء الثاني عشر من دورة إدارة الشبكات المنزلية

التحكم في عرض النطاق (Bandwidth Control)

قبل البدء ولمن لا يعرف ما هو عرض النطاق فهو مقياس لعدد البتات او البايتات التي يسمح لحاسوب معين او أي جهاز اخر في الشبكة بأرساله او استقبالها في الثانية الواحدة ويقاس عادة بوحدة (bps) بت بالثانية او (Bps) بايت بالثانية وكما هو واضح فأن الفرق بين الاثنين هو فقط في حالة حرف ال (b) حيث ان الحرف الصغير (small b) يرمز الى البت وهو اما (٠ او ١) اما الحرف الكبير (capital B) فيرمز للبايت وهو ثمان بتات وهذه الأمور يعرفها كل مختصي الحاسوب بشكل بديهي.

الان عند النقر على تبويب التحكم في عرض النطاق تظهر الخيارات التالية:

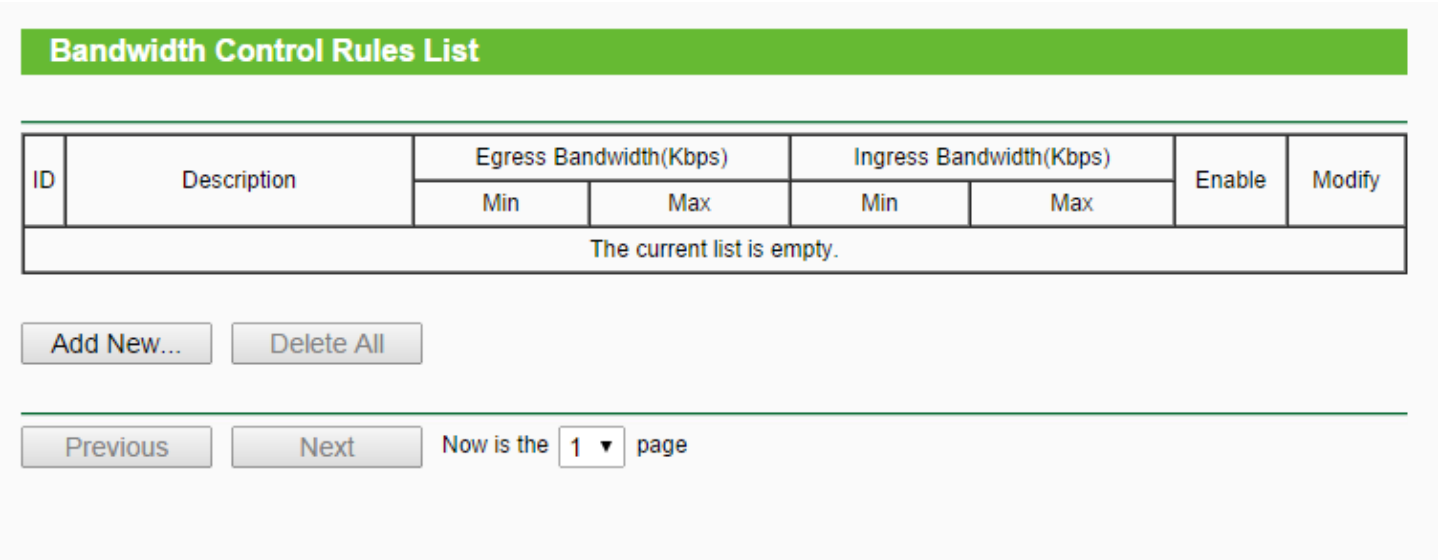
والان تظهر لنا في الجانب الأيمن من نافذة متصفح الانترنت الذي نستخدمه لضبط الاعدادات الخيارات التالية الخاصة بإعدادات التحكم:



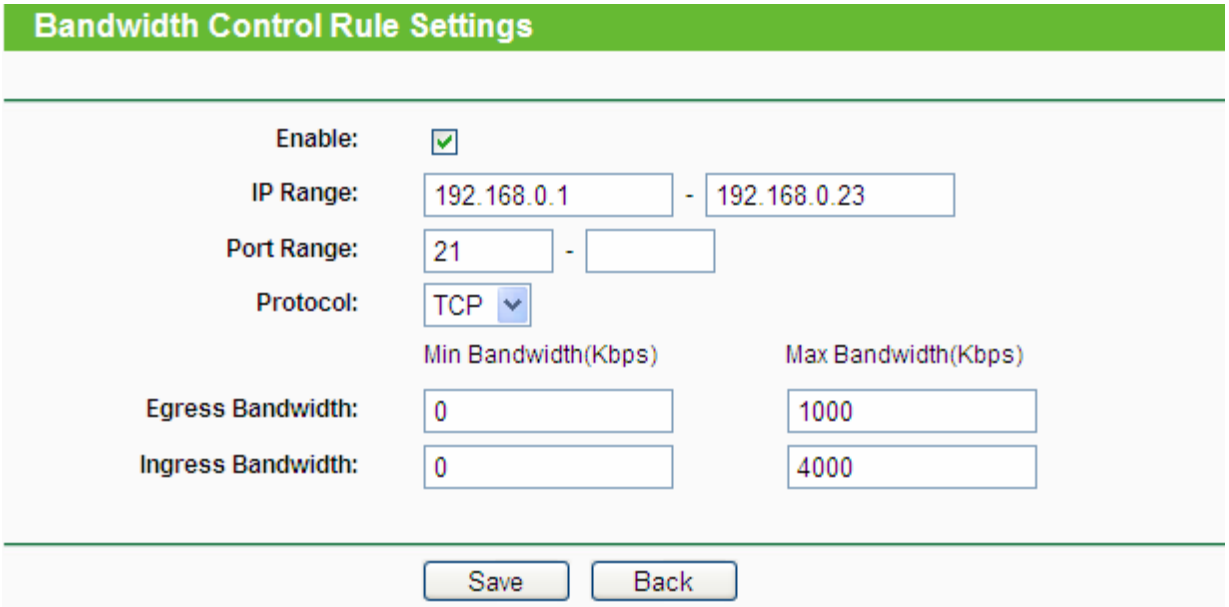
اول تلك الخيارات هو تمكين (enable ….) التحكم بعرض النطاق ويجب تفعيل هذا الخيار ان اردنا ضبط بقية الاعدادات وبعدها نجد نوع خط الانترنت الذي تعمل عليه وهل هو (ADSL) او نوع اخر يتم تحديده حسب نوع الخدمة التي انت مشترك فيها ويمكن سؤال مزود الخدمة عن هذه التفاصيل في حالة عدم معرفتها واخيراً نصل الى الخيارات الأكثر أهمية وهي تحديد عرض نطاق الإخراج (upload)عبر منفذ ال (WAN) وهي (Egress Bandwidth) وكذلك نحدد عرض نطاق الادخال (download) عبر منفذ الشبكة العالمية (WAN port) والمسمى (Ingress Bandwidth). واخيراً ننقر على الحفظ (save).

ملاحظة: هنا يفضل ترك الأرقام على حالها بدون تغيير لضمان مرور اكبر مقدار من البيانات في الثانية الواحدة فنحن لا نريد تقييد شبكتنا بقيود اكثر مما قيدها مزود الخدمة اصلاً ولكن هذه القيود تستخدم في بعض الأحيان للتحكم في مرور الشبكة في حالة كون الاشتراك يعتمد على حجم ال (upload and download) فهنا يجب تقييد المستخدمين بعرض نطاق محدود لتقليل الكلفة الكلية للاشتراك.

الان نصل الى قائمة القيود (rules list) والتي عند النقر عليها تظهر النافذة التالية:



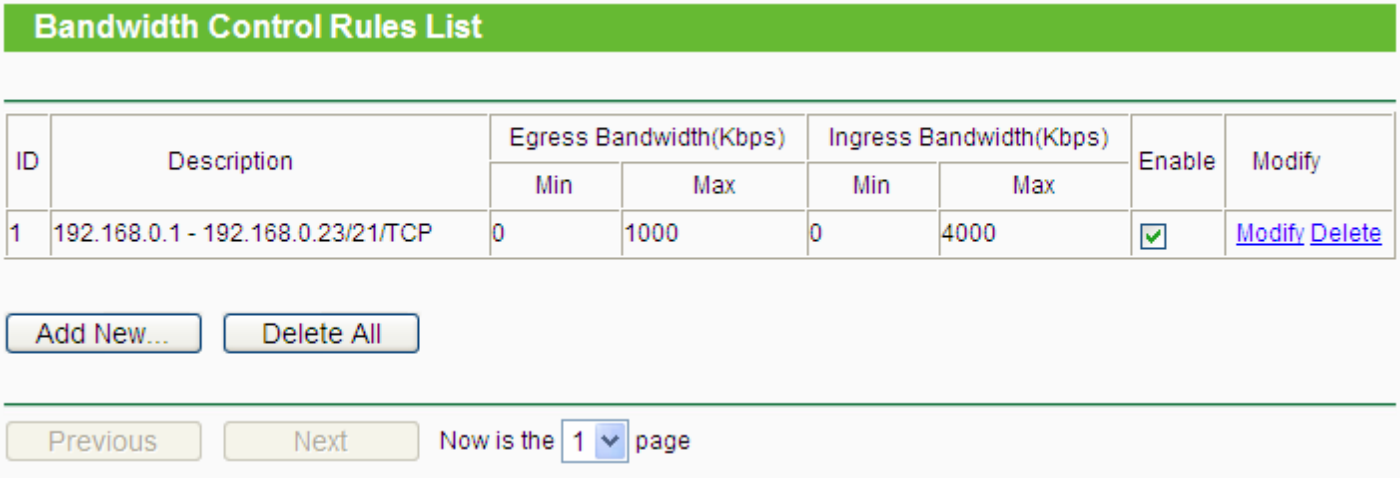
والتي تعني انها فارغة لم يخصص فيها أي شيء لحد الان ولبدء تقييد الحواسيب ننقر على إضافة جديد (Add new) لتظهر النافذة التالية:



وهنا نجد ان خيار التفعيل (enable) مفعل مسبقاً ونقوم بأدخال حيز العناوين (IP range) الذي نريد التحكم به الان وكذلك حيز المنافذ (ports) ونوع البروتوكولات المستخدمة (TCP, UDP, ALL) واخيراً نحدد الحد الأدنى والحد الأعلى للتصعيد والتنزيل حيث ان (min, Egress) تعني اقل سرعة مسموحة في التصعيد و(Max, Egress) هي اكثر سرعة مسموحة للتصعيد وهكذا بالنسبة للتنزيل (download). واخيراً لا ننسى النقر على (save).

ملاحظة: هنا يمكننا حصر مجموعة من الحواسيب والأجهزة الذكية المرتبطة بالشبكة لتقييد حركة البيانات فيها وليس كل الحواسيب ويعتمد ذلك على المدى الذي حددناه لل (IP addresses) فلو اننا قيدنا بعض الحواسيب ببعض العناوين فعندها نستطيع تقييد مرور هذه الحواسيب فقط وليس كل الشبكة وهذا الأمور يتطلب منا مراجعة الدروس السابقة بخصوص فقرة ال (address reservation) ضمن تبويب ال (DHCP).

والان بعد ان قمنا بملء الخيارات كلها ستظهر لنا نافذة قائمة القيود كما يلي:



ونجد فيها وصف (description) للحواسيب نسبة الى حيز عناوينها وكذلك بقية المواصفات من الحدود الدنيا والعليا للتصعيد والتنزيل وحالة التمكين (enable) واخيراً قابلية التعديل (modify) بحذف او تعديل أي قائمة قيود وكذلك الازرار المعتادة من حذف الكل (delete all) وغيرها.

ملاحظة أخيرة:

يتساءل البعض عن سبب كل هذا الاهتمام بجهاز ال (TP-link) لدرجة ان احدهم استهزأ بوجود دورة حول هذا الجهاز اصلاً وفي الرد على هذا التساؤل أقول ان الدورة للمبتدئين في عالم الشبكات حصراً وربما يستفيد منها بعض المحترفين ايضاً ولكن المقصود الأكبر منها المبتدئين ليعرفوا المفاهيم الأساسية للتحكم في الشبكات وواجبات مدير الشبكة حتى اذا تقدموا قليلاً في عالم سيسكو ومايكروسوفت وجونيبر وغيرها من عمالقة الشبكات اصبحوا قادرين على الخوض في غمار تلك

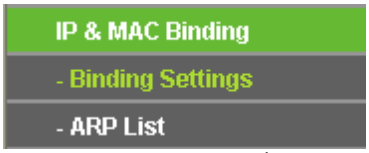
الكورسات بثقة ومعرفة ما يريدون الوصول اليه بسهولة ويسر وعندها سيكون لديهم قابلية طرح الأسئلة الصحيحة في الوقت المناسب مثل (كيف يمكن التحكم في عرض نطاق الشبكة باستخدام ايعازات سيسكو) او (ما هي الاداة او الرول المناسبة في الويندوز سيرفر للتحكم في عرض نطاق الارسال والاستقبال للمستخدمين للشبكة المحلية وهكذا).

الجزء الثالث عشر من دورة إدارة الشبكات المنزلية:

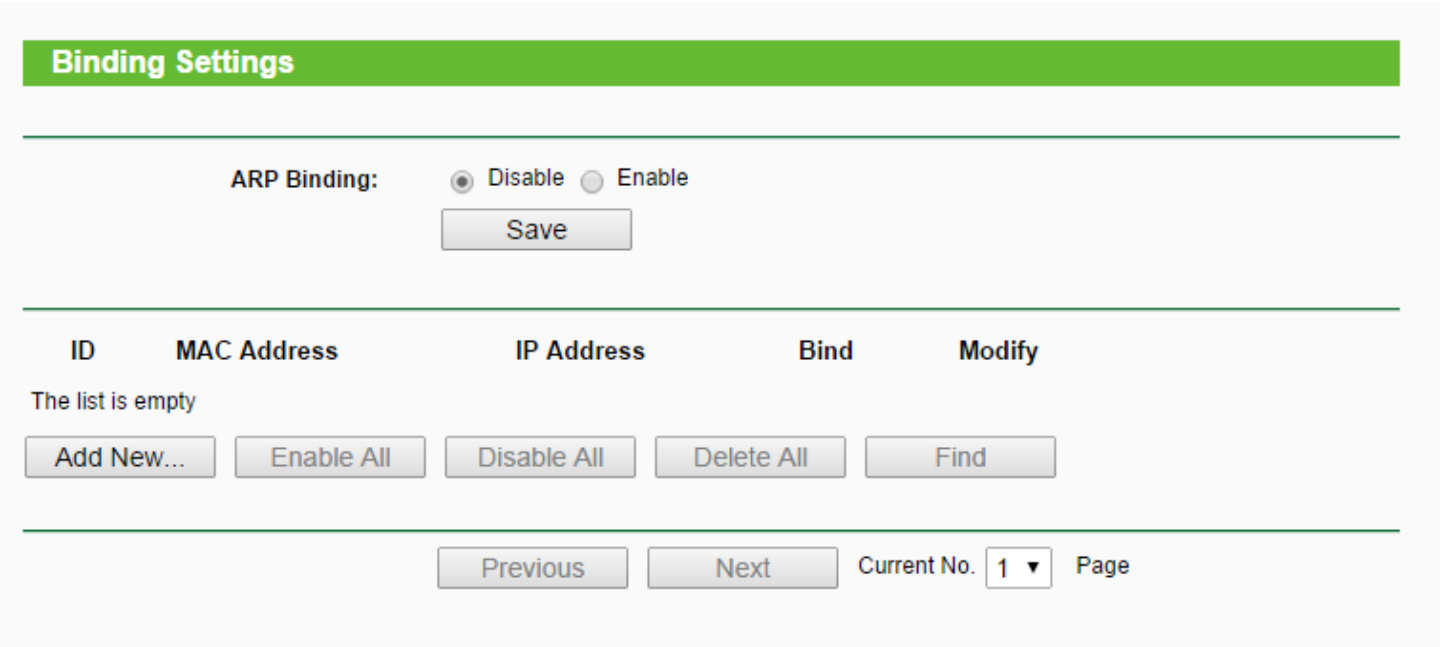
ربط العناوين المنطقية بالعناوين الفيزيائية (IP & MAC binding)

ويفيد هذا الخيار في ربط وتقييد حواسيب معينة لها عنوان فيزيائي معين (MAC address) بعنوان منطقي (IP address) معين والفائدة من ذلك هو ما ذكرناه في الدرس السابق الخاص بالتحكم بعرض النطاق (Bandwidth control) حيث اننا نستطيع التحكم في عرض نطاق أي جهاز من خلال عنوانه المنطقي ولأن العنوان المنطقي (IP) يتغير كل عدة ساعات (بسبب سيرفر ال DHCP) فأن ربطه بعنوان فيزيائي ثابت يعني الغاء خاصية التغيير التلقائي للعناوين المنطقية وتثبيتها لكل حاسوب ويتم ذلك كما يلي:

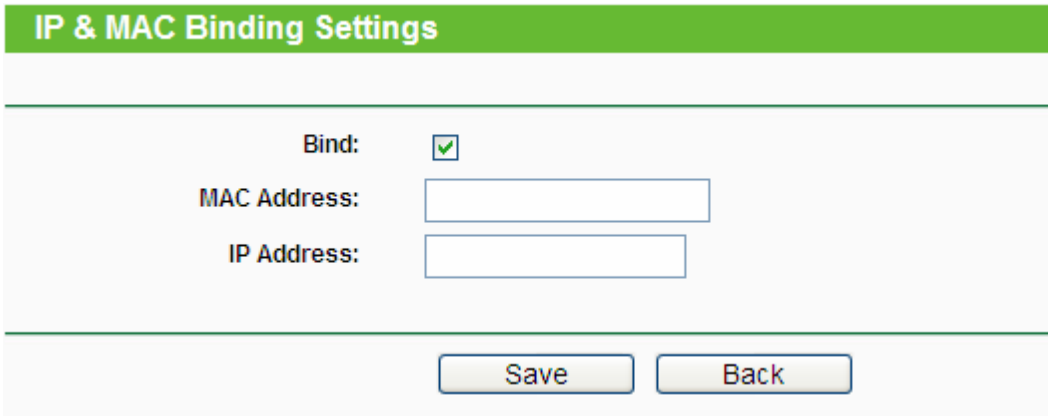
عند النقر على هذا التبويب تظهر الخيارات التالية:



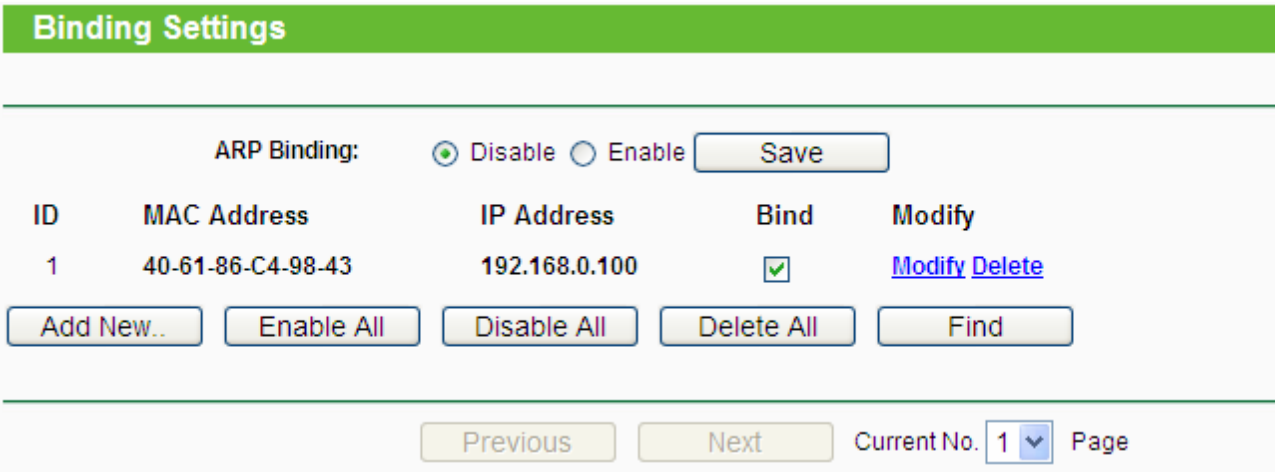
الخيار الأول هو اعدادات التقييد (binding settings) ويضم الأمور التالية:



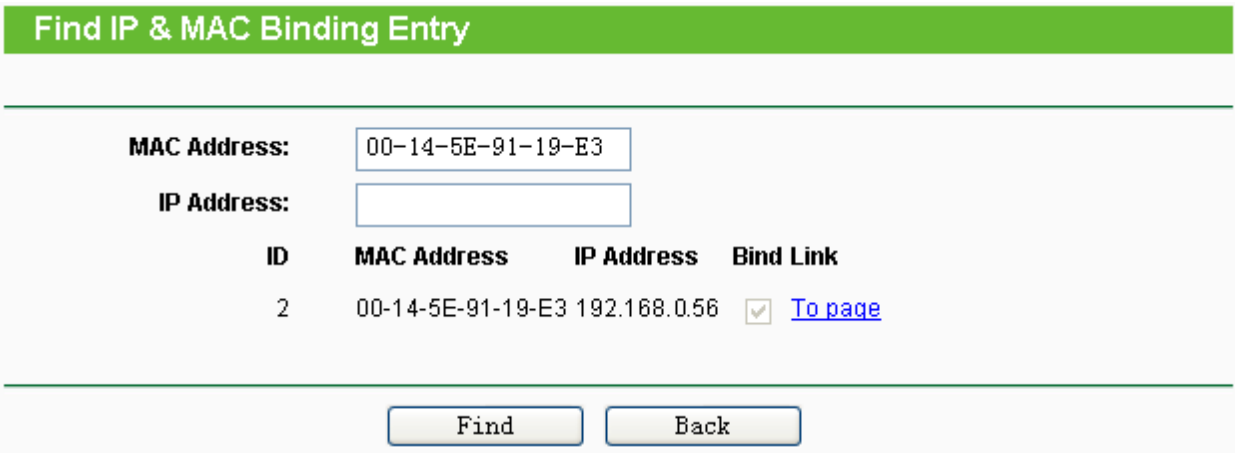
ولبدء العمل بهذا الخيار يجب تفعيل خيار التمكين (enable) وحفظ ذلك (save) ثم البدء بإضافة القيود واحداً تلو الاخر من زر (add new) لتظهر النافذة التالية:



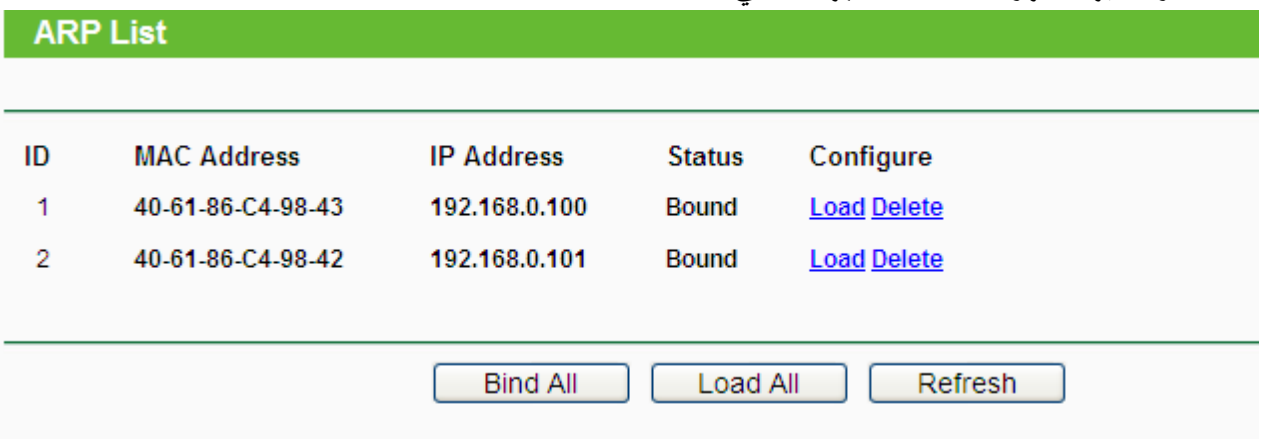
نكتب العنوان المنطقي والفيزيائي (IP & MAC) المراد ربطها وتقييد أحدهما للأخر معاً ثم نفعل خيار التقييد (bind) وننقر على الحفظ (save) لتظهر النافذة بعد ذلك بالشكل التالي:



نقوم بتكرار عملية التمكين (enable) وحفظ ذلك (save) ونرى ان هناك الكثير من الخيارات المألوفة بالنسبة لنا مثل تمكين الكل (Enable all) وتعطيل الكل (disable all) وحذف الكل (delete all) ومربع التحديد لخيار التقييد (bind) والذي عند النقر بداخله لوضع علامة الصح فها يعني تفعيل التقييد والا فالتقييد غير مفعل واخيراً زر إيجاد قيد معين محفوظ مسبقاً (find) والذي عند النقر عليه تظهر النافذة التالية:



نقوم بإدخال أي من ال(IP or MAC) التي نعرفها ونريد معرفة العنوان الاخر المقيد بها فيظهر العنوان الاخر كما في أعلاه.
الخيار الاخر من خيارات هذا التبويب هو قائمة بروتوكول دقة العناوين (Address Resolution Protocol ARP) والتي عند النقر عليها تظهر النافذة المشابهة للتالي:

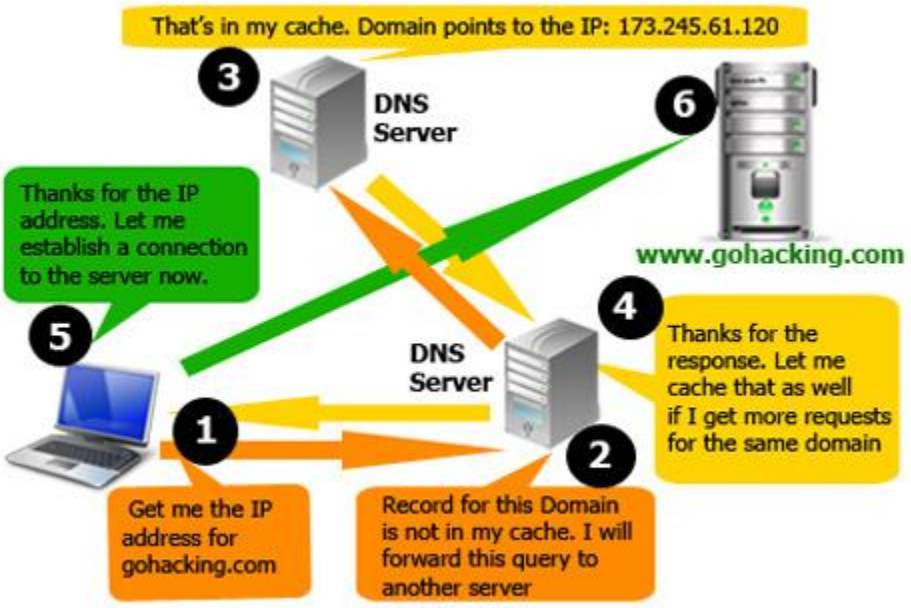


ومن هنا نستطيع تقييد الكل او تحميل الكل (load all) ونقصد بالتحميل للكل هنا قيام الراوتر بتحميل كل القيود التي قمنا بتفعيلها الى هذه القائمة أي اضافتها هنا ان لم تكن قد أضيفت مسبقاً ويتوفر لدينا خيارات الحذف والتحميل للقيود المفردة كذلك امام كل حقل في الجدول.

الدرس الرابع عشر من دورة إدارة الشبكات المنزلية:

نظام أسماء النطاق الديناميكي (Dynamic Domain Name System DDNS)

قبل البدء في شرح درس اليوم لابد من التطرق بشكل مختصر الى فائدة ال (DNS) والفرق بينه وبين (DDNS) فهيا بنا:
ال (DNS) او نظام أسماء النطاق هو تطبيق او برنامج يعمل في الطبقة السابعة طبقة التطبيقات (Application Layer) من مكدس الشبكات ويكون كجهاز مستقل او كوظيفة في جهاز معين ضمن مجموعة وظائف أخرى وراوترنا الذي نعمل عليه (TP-Link) يوفر هذه الخدمة نوعاً ما كما يوفرها الويندوز سيرفر واغلب ان لم يكن كل الراوترات والسيرفرات في عالم الشبكات ووظيفته الرئيسية هي تحويل الأسماء المقروءة بشرياً الى أسماء مقروءة حاسوبياً وبالعكس أي تحويل العنوان (www.google.com) الى شيء مشابه ل (10.23.234.22) وبمصطلحات الحاسوب تحويل ال (URL) الى (IP) وبالعكس كما في الصورة ادناه:

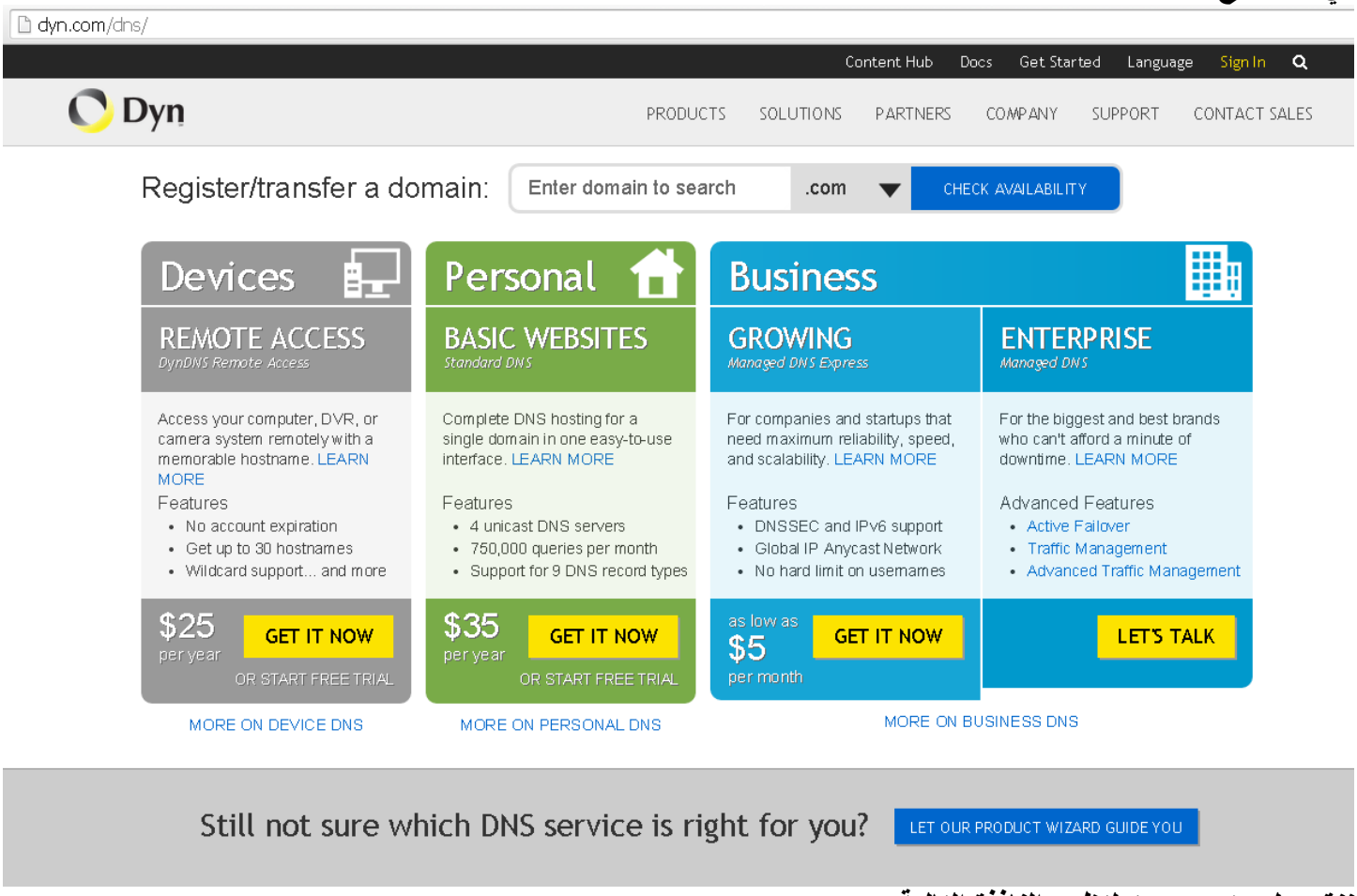


والان ما الفرق بين ال (DNS) وال (DDNS)؟
يستخدم الأول بشكل رئيسي مع عناوين ال (IP) الحقيقية الثابتة للمواقع الكبيرة والمؤسسات العملاقة ولكن لما كانت عناوين ال (IP) للجيل الحالي قد نفدت فقد بدأت حلول ال (Private IP) بالظهور الامر الذي أدى الى التغير المستمر للعنوان (IP)الخاص بالحاسوب او السيرفر مما يتطلب وجود حل ديناميكي يتابع تغير ال (IP) الخاص بأي عنوان (URL) واليكم السيناريو الموجود حالياً:
قام الشخص (س) بأنشاء موقع انترنت في حاسوبه الشخصي المربوط ضمن شبكة محلية وقد حصل على (IP) من النوع الخاص المتغير (Dynamic Private IP) وبعد ان قام بنشر موقعه وقام ال (local DNS) المحلي بتسجيل ال (URL) وال (IP) المقابل له بدأ الناس بكتابه عنوان الموقع في متصفحاتهم وبدأ ال (DNS) بأخذهم الى الموقع المطلوب ولكن بعد مرور وقت معين تغير ال (IP) الخاص بحاسوب الشخص (س) فبدأ الناس بالشكوى من عدم ظهور الموقع المطلوب!
نعم انه سيناريو شائع بالنسبة للمبتدئين في مجال المواقع وقد قامت المؤسسات المعنية بهذا بتبسيط الموضوع وانشاء ال (DDNS) وهو خدمة محدثة للخدمة القديمة تأخذ على عاتقها المتابعة للعناوين المتغيرة وتحديث جداولها الرابطة بين (URL & IP) بشكل دوري لتضمن ان الجداول الخاصة بها صحيحة تماماً وللموضوع تفاصيل كثيرة لها مكان اخر لشرحها ان شاء الله تعالى.
والان نبدأ درسنا لهذا اليوم:
يوفر راوتر ال (TP-Link) خدمة ال (DDNS) والتي تسمح للحواسيب المرتبطة به ان تستضيف مواقع انترنت او سيرفرات ال (FTP) او سيرفرات البريد الالكتروني التي لها اسم نطاق (Domain Name) ثابت وعنوان (IP) ديناميكي متغير مع

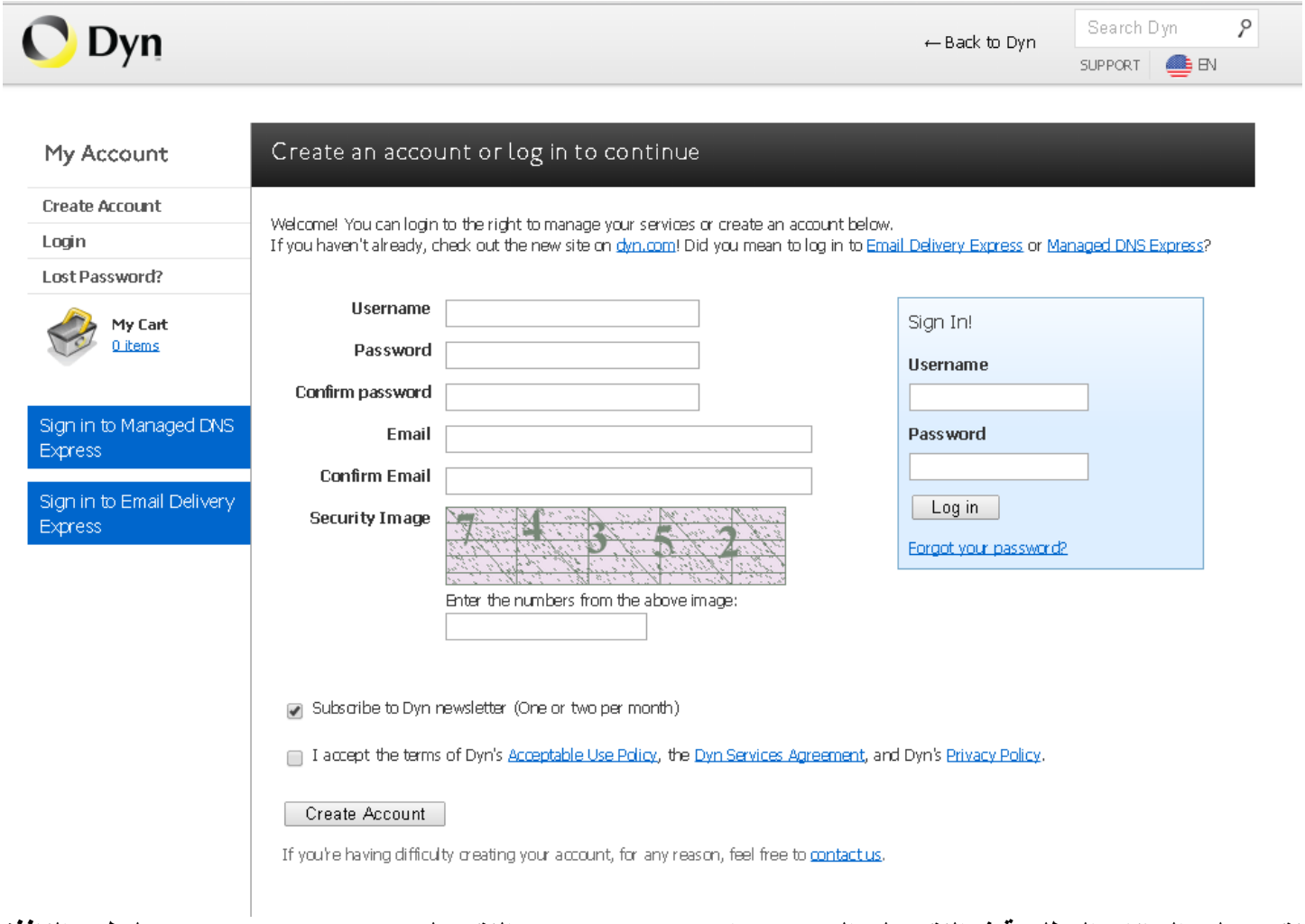
إمكانية وصول الأصدقاء الى سيرفرك الشخصي او موقعك الالكتروني بكتابة عنوانه ال (URL) مهما تغير ال (IP) الخاص بحاسوبك.

قبل البدء بتفعيل هذه الخاصية لا بد من التسجيل في احد المواقع التالية:

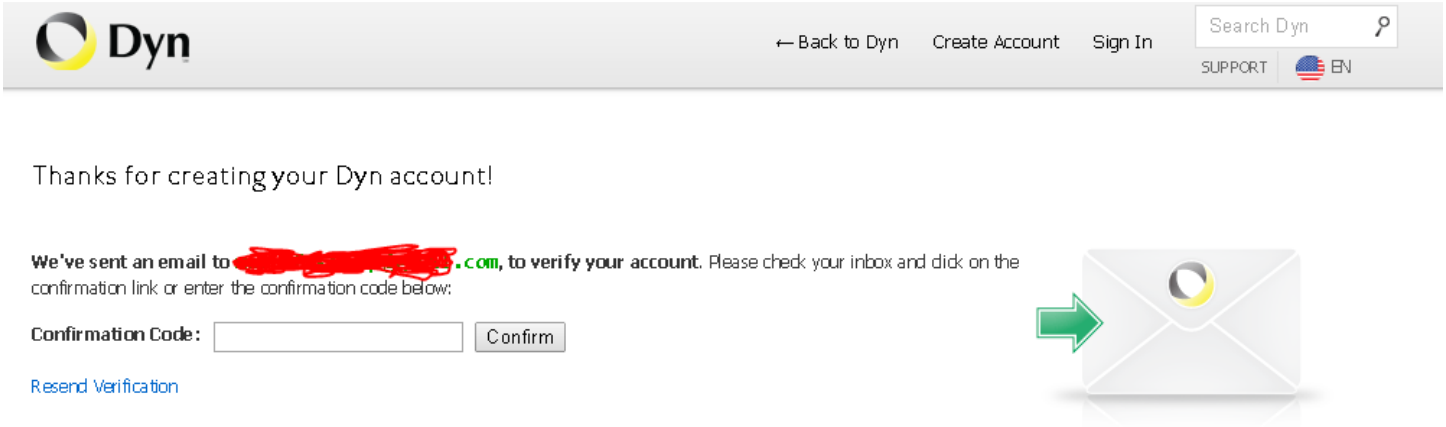
(www.comexe.cn) او (www.dyndns) او (www.no-ip.com) والتي بعد اكتمال التسجيل فيها سيتم اعطائك كلمة مرور او مفتاح للولوج وسنأخذ الموقع الثاني كمثال لكيفية التسجيل حيث انه عند النقر على رابطه تفتح لنا النافذة التالية في المتصفح:



ننقر على (sign in) لتظهر النافذة التالية:



نقوم بملء البيانات المطلوبة ثم النقر على المربع بجوار (I accept….) والنقر على زر (create account) لتظهر النافذة التالية:



هنا يخبرنا بأنه قد قام بأرسال كود التفعيل الى عنوان بريدنا الالكتروني الذي ادخلناه قبل قليل ولإكمال التسجيل يجب الذهاب الى البريد الالكتروني ونسخ الكود من هناك الى المربع المؤشر في النافذة أعلاه وبعد وضع الكود هنا ننقر على (confirm) لتظهر النافذة التالية:

Congratulations! Your Account Is Now Active!

Account [redacted] has been confirmed and activated. Please explore the following options to get started.

most popular!

Features	DynDNS Pro	Dyn Standard DNS	Managed DNS Express
	$25.00/yr	$35.00/yr	$5.00/mo STARTING PRICE
	CONTINUE	CONTINUE	CONTINUE
Hostnames/DNS Records	25	75	25+
Domain name	Choose from one of ours	Custom Domain	DNS hosting from 2+ domains
Access to phone technical support	✔	✔	✔
Number of Users	1	1	100+
Data Centers	5 Unicast	5 Unicast	17 Anycast
Logs	Update history (24 hr.)	Update history (24 hr.)	Comprehensive change logs
SOAP/REST API	-	-	✔
	CONTINUE	CONTINUE	CONTINUE

Just starting out with Dynamic DNS? We offer a 14-day trial of DynDNS Pro!

هنا يطلب منا اختيار نوع الحساب الذي نريد الاشتراك فيه بحسب الإمكانيات المتوفرة والمبالغ المالية التي نستطيع دفعها وتبقى هنا المسألة خاضعة لخصوصية كل شخص اما انا فسأنقر على عبارة (14-days trial) أي البقاء بحساب تجريبي مجاني لمدة ١٤ يوم لتظهر النافذة التالية:

Remote Access Free Trial

Try out our basic Dynamic DNS
& remote access service for 14 days.

START THE TRIAL

Dyn » Managed DNS, Outsourced DNS & Anycast DNS » Remote Access Free Trial

- Traffic Management
  - Managed DNS
  - Managed DNS Express
  - Standard DNS
  - Remote Access
  - Compare Features
  - Secondary DNS
- Domain Registration
- Managed DNS Case Studies
- Managed DNS Whitepapers & eBooks
- Support
- Contact Sales

What is it?

Looking to access your computer, DVR, webcam or camera system remotely without having to remember a confusing (and ever changing) IP address? Check out our free 14 day trial of Remote Access, a great option for those who need Dynamic DNS and remote access capabilities without any bells, whistles or fireworks.

What does it do?

Remote Access allows you to assign an easy to remember hostname (such as yourname.dyndns.org) to your location's IP address. By installing an update

One low yearly subscription

After the 14 day trial ends, Remote Access has a low subscription rate of just $25 a year. Sign up for five years and you will get 28% off!

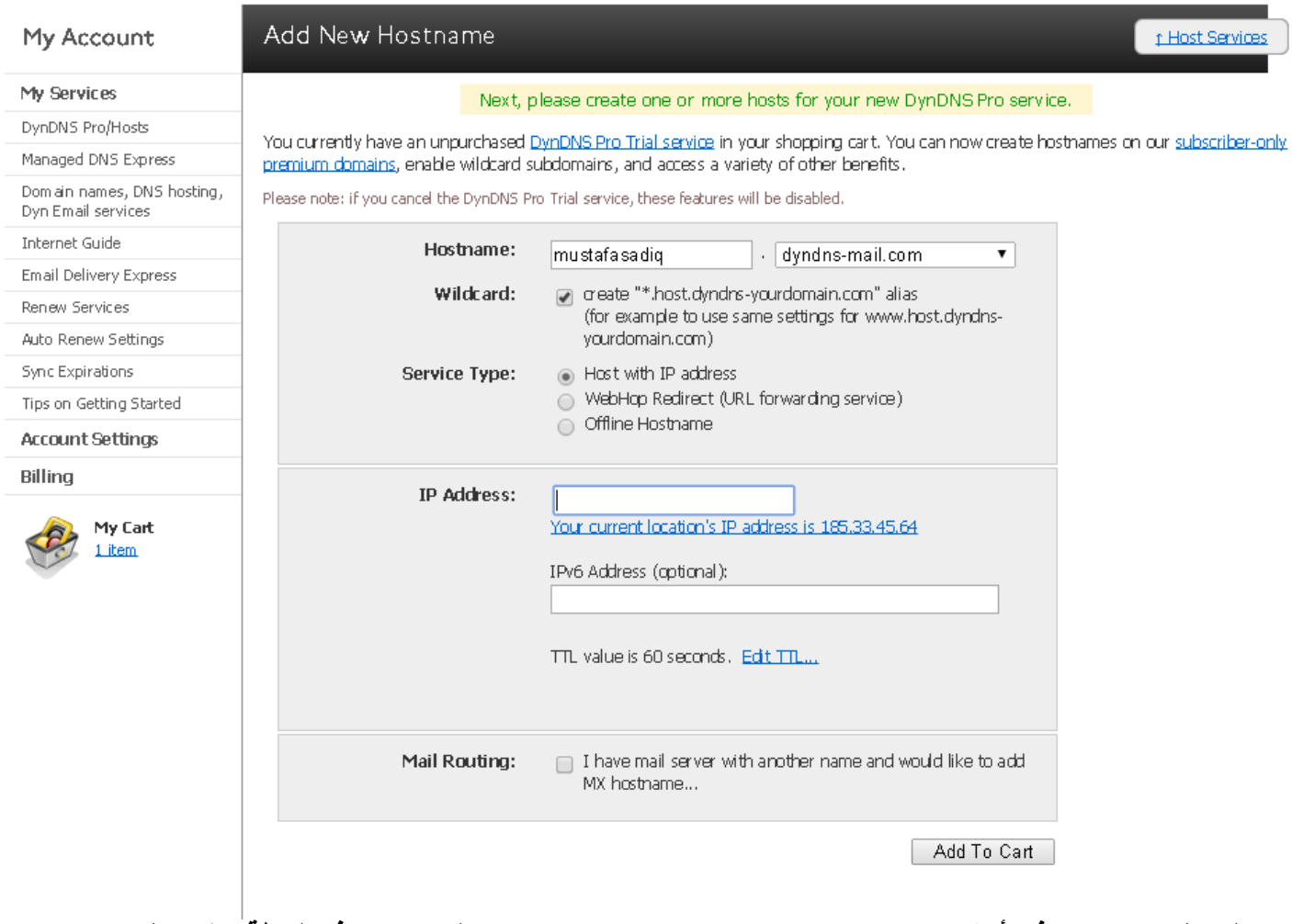
No account expiration

Remote Access subscribers don't have to worry about their account expiring after 30 days of inactivity, a great reason for users to upgrade.

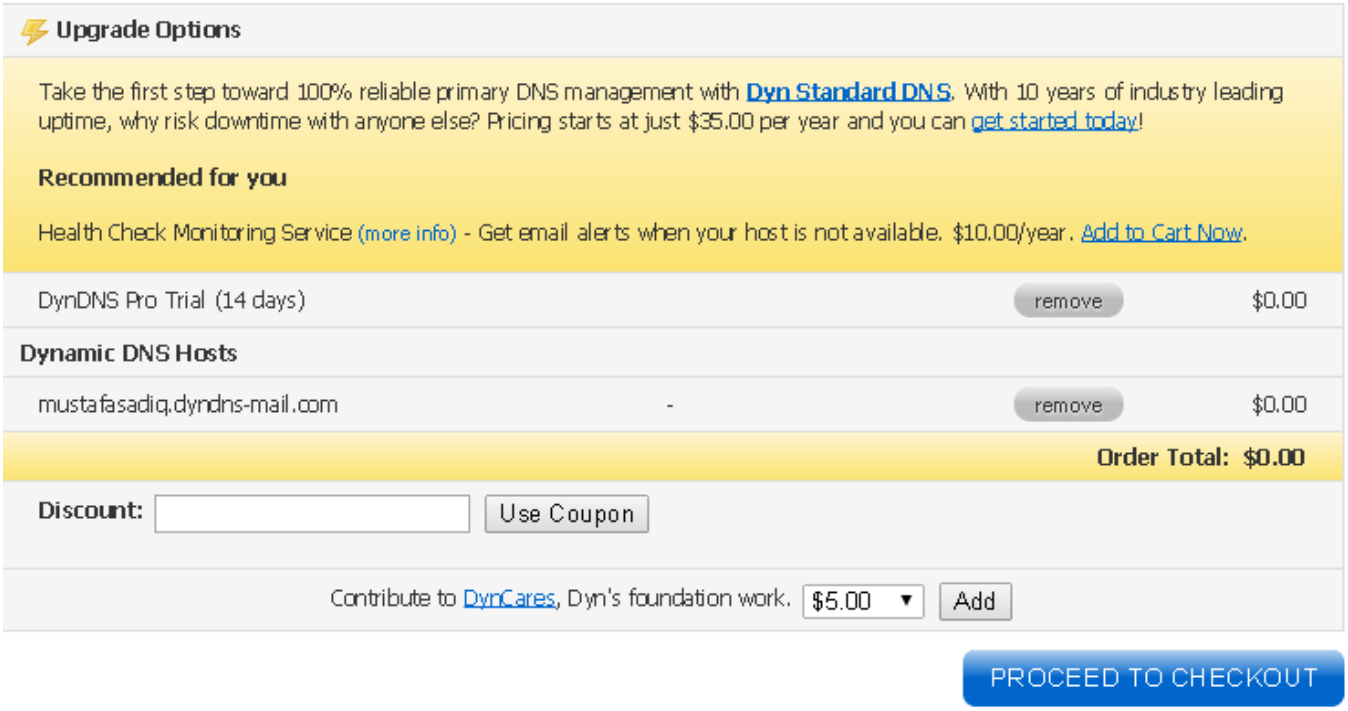
Up to 30 DynDNS hostnames

Whether you need Dynamic DNS for a single location or multiple locations, Remote Access has you covered with up to 30 hostnames

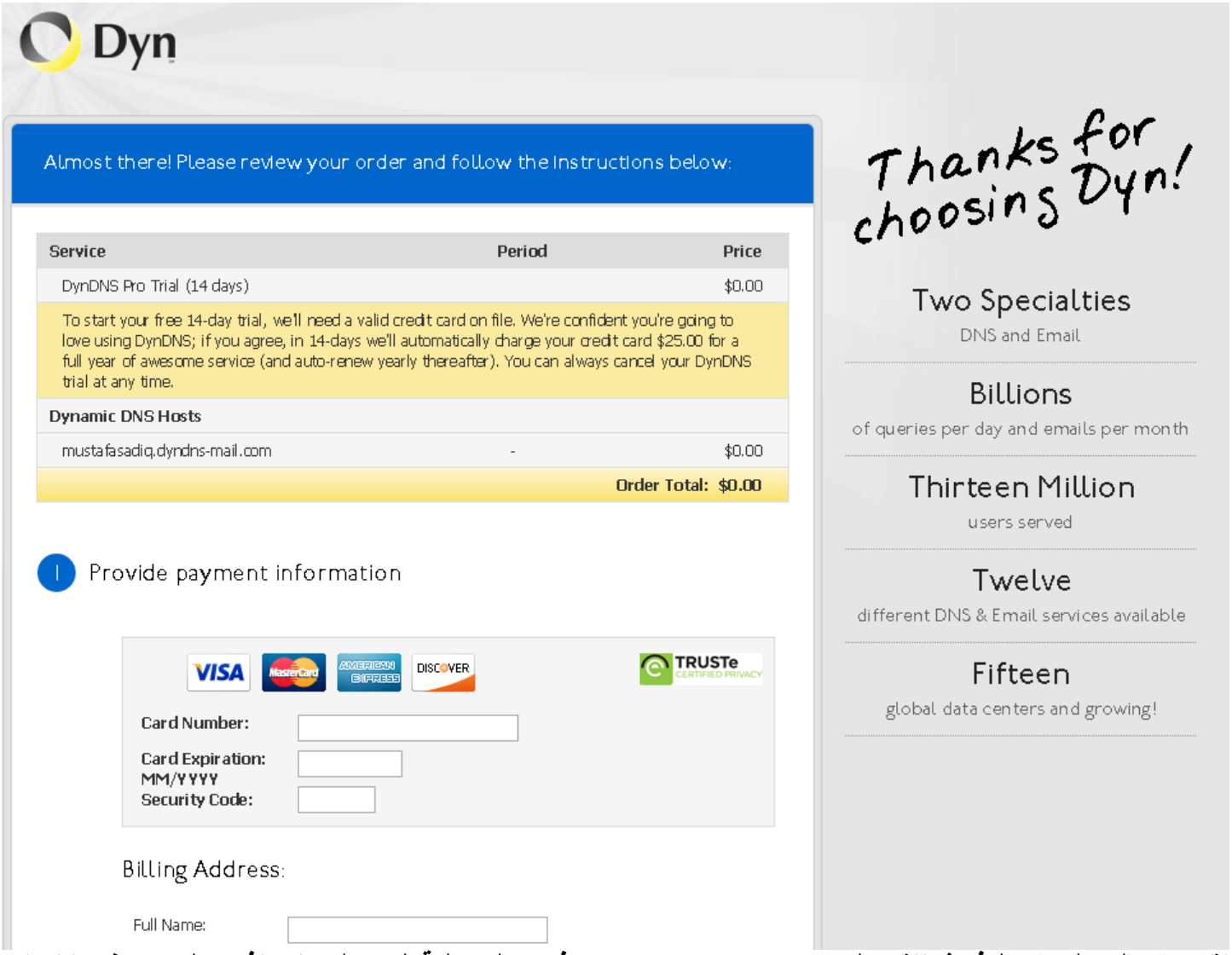
فننقر على (Start the trial) لتظهر النافذة التالية:



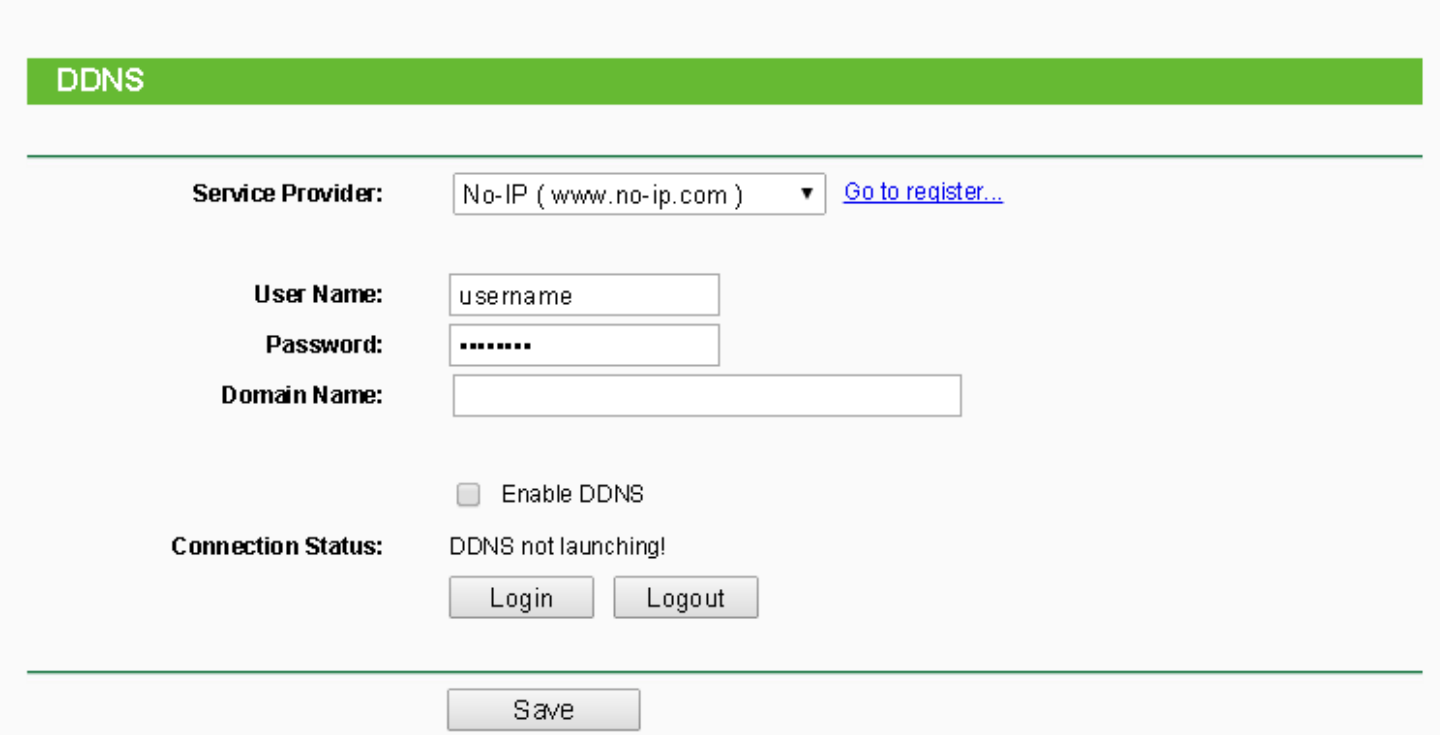
نقوم بملء الخيارات كما في أعلاه ولا ننسى ان نكتب عنوان (IP address) الخاص بنا في لحظة انشاء الحساب ويمكن معرفته بسهولة من استخدام ايعاز (ipconfig/all) في محرك الأوامر (cmd) كما تم شرحه سابقاً ثم ننقر على (Add to Cart) لتظهر النافذة التالية:



نقوم بالنقر على (proceed to checkout) **لتظهر النافذة التالية:**



نقوم بإدخال معلومات الدفع ثم ننقر على (sign up for trial) وهكذا تكتمل عملية التسجيل والان نذهب الى متصفح الانترنت خاصتنا ونفتح واجهة التحكم بال (TP-Link) حيث كنا سابقاً ضمن تبويب (DDNS) والذي عند النقر عليه تظهر النافذة التالية:

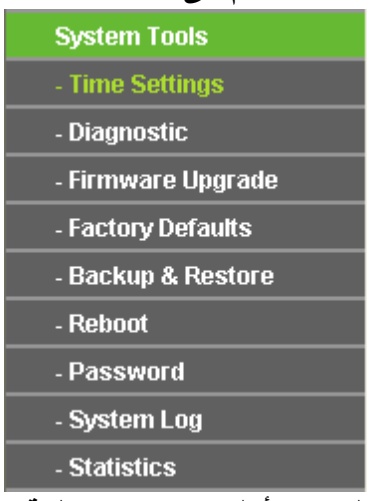


الان من اول مربع خيارات نختار الموقع الذي قمنا بالتسجيل فيه وهو في مثالنا هنا (www.dyndns.com) ويمكن طبعاً التسجيل في أي موقع اخر واختياره هنا والان عند اختياره ستظهر الخيارات التالية:

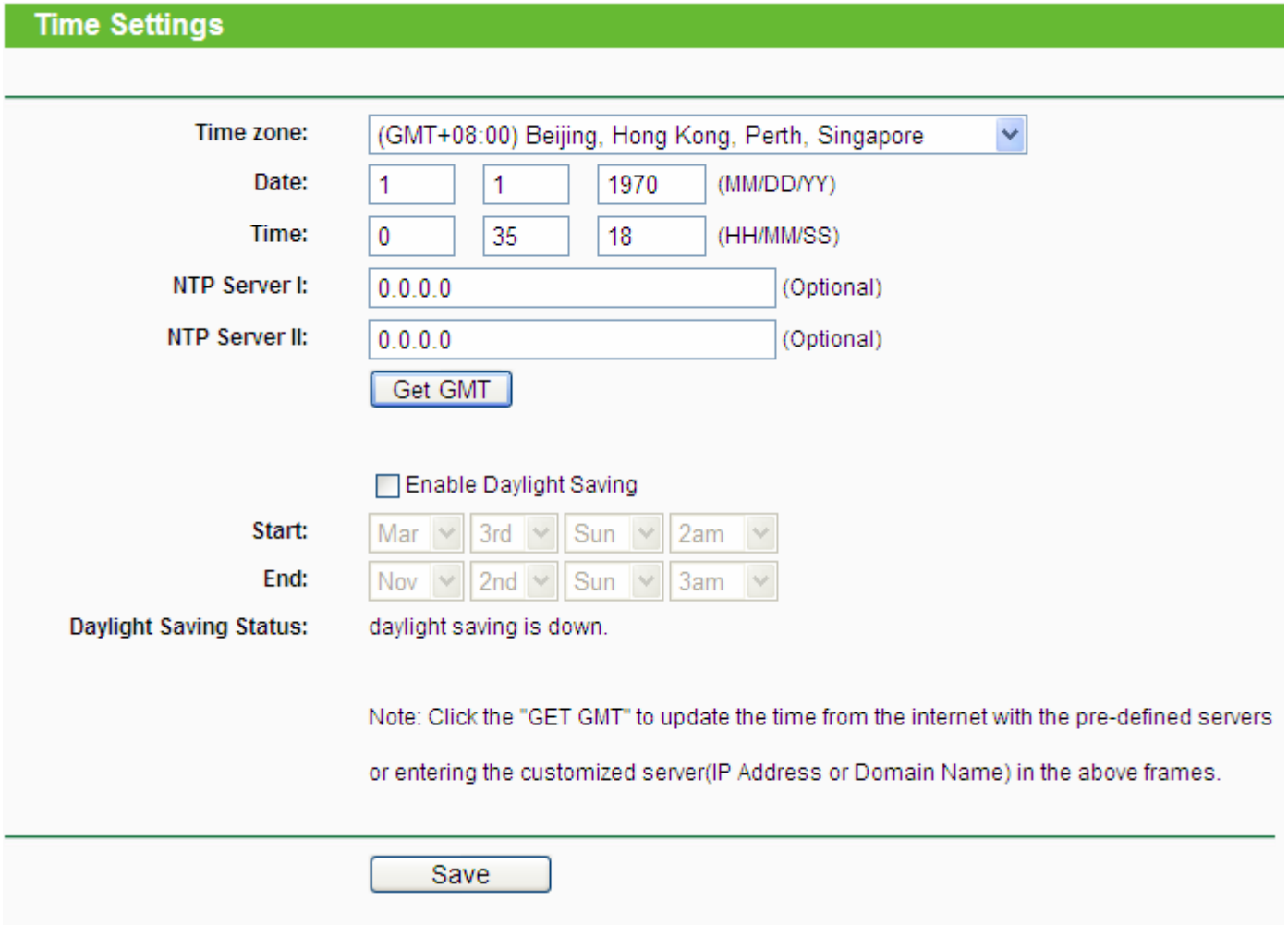
في حالة انشاء حساب اخر ومحاولة الدخول من خلاله نقوم بالنقر على (logout) ثم نقوم بإدخال معلومات الحساب الجديد من اسم المستخدم وكلمة المرور واسم النطاق ثم النقر على (login) من جديد.

الجزء الخامس عشر والأخير من دورة إدارة الشبكة المنزلية والمحلية:

وصلنا اليوم الى التبويب الأخير من تبويبات نظام تشغيل أجهزة ال (TP-link) وهو كما في النافذة ادناه:

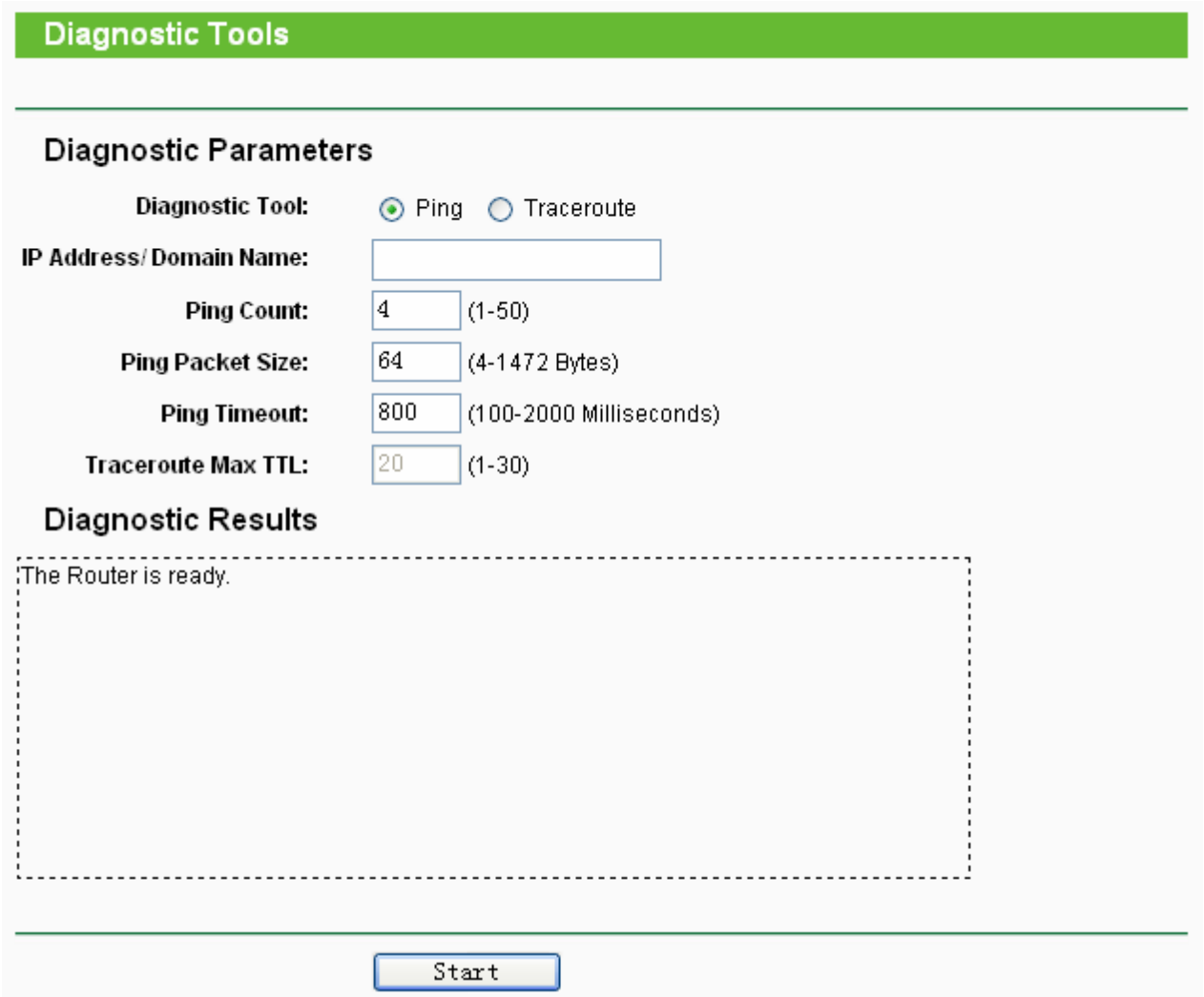


الخيار الأول هو اعدادات الوقت الخاص بالجهاز وعند النقر عليه تظهر النافذة التالية:

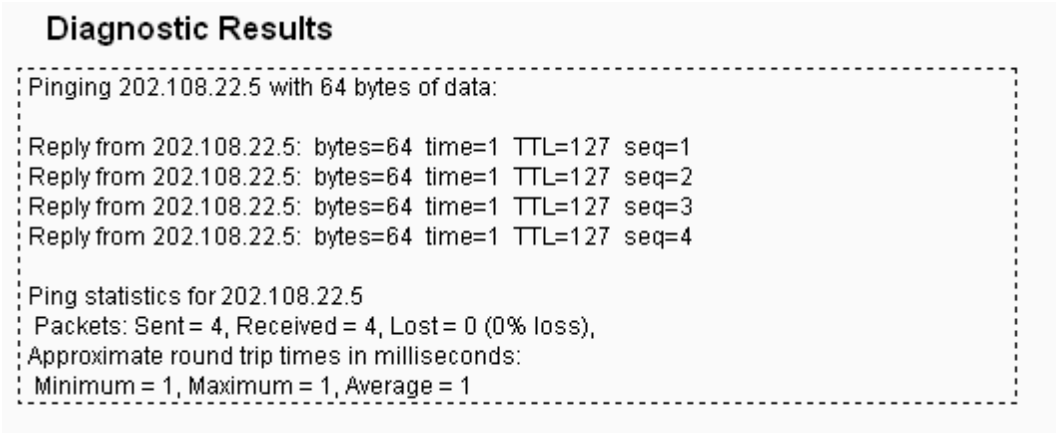


من هذه النافذة يمكن اختيار المنطقة الزمنية (time zone) وحسب البلد الذي تسكنه وكذلك الوقت والتاريخ الحالي (لحظة ضبط اعدادات الوقت) وإمكانية ادخال عنوان (IP address) لسيرفر ال (Network Time Protocol NTP) الأول والثاني وهذا الاجراء اختياري ونستخدمه فقط في حالة معرفة تلك العناوين وبخلافه سيقوم الراوتر بمجرد الاتصال بالانترنت بالحصول على الوقت الافتراضي للشبكة من مزود الخدمة كما يمكننا النقر على زر (GET GMT) للحصول على التوقيت العالمي لغرينتش بمجرد الاتصال بالانترنت ويفضل إبقاء بقية الاعدادات بدون تغيير ولا ننسى النقر على (save) للحفظ.

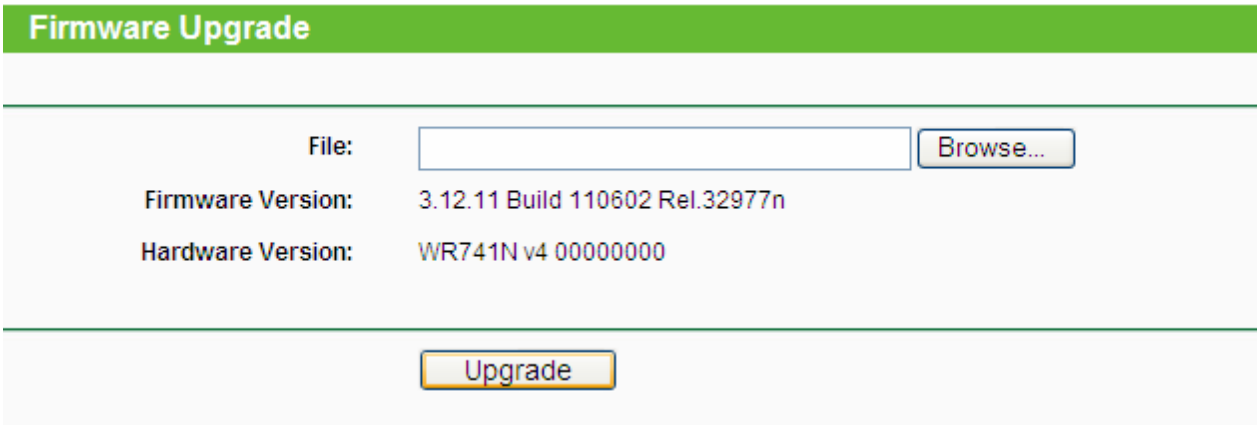
التبويب الاخر خاص بتشخيص مشاكل الجهاز وحالته (diagnose) والذي عند النقر عليه تظهر النافذة التالية:



من هنا نستطيع عمل (ping) او (tracert= traceroute) لأي عنوان (IP address) او موقع ويب وبالاعدادات التي نختارها وننقر بعدها على (start) لفحص وجود اتصال او لا مع موقع معين والبطء وغيرها من المشاكل التي قد تواجه الشبكة المحلية وعادة ما تظهر النتائج كما في ادناه:

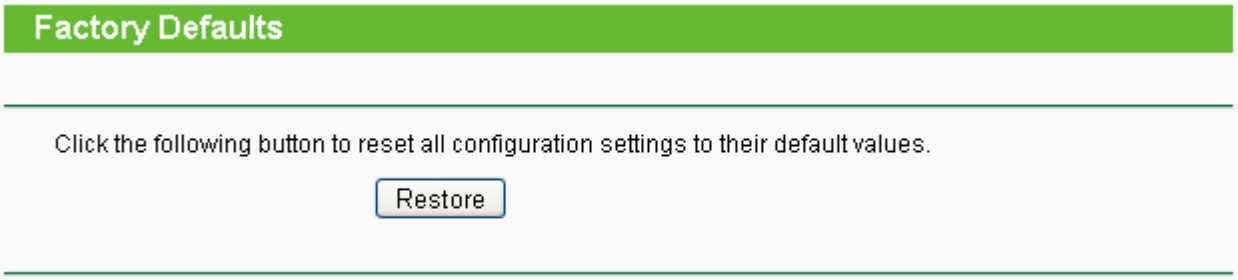


التبويب الاخر يخص تحديث (ترقية) نظام تشغيل الراوتر (Firmware upgrade) حيث عند النقر عليه تظهر النافذة التالية:



ونلاحظ عرض النسخة الحالية من النظام (firmware version) ونسخة الجهاز (hardware version) ولعمل تحديث للجهاز نقوم بالدخول الى موقع الشركة (www.tp-link.com) ونقوم بالبحث عن اسم الجهاز في الموقع لتظهر اخر التحديثات له فنقوم بتنزيلها كملف بأمتداد (.bin) وبعدها نتأكد من عدم انطفاء الكهرباء اثناء الترقية وننقر على (Browse) ونختار الملف الي قمنا بتنزيله من الموقع ثم ننقر على (upgrade) لتبدأ عملية ترقية نظام تشغيل الجهاز وننتظر قليلاً وبعدها سيعاد تشغيل الجهاز بالنظام الجديد.

التبويب الاخر يخص ارجاع الجهاز الى اعدادات المصنع الاصلية (Factory defaults) والذي عند النقر عليه تظهر النافذة التالية:



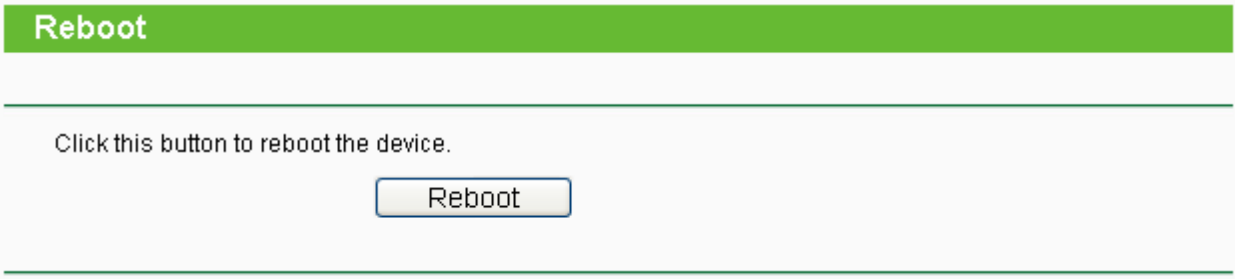
بعد النقر على (Restore) سيرجع العنوان (IP) الأصلي واسم المستخدم وكلمة المرور الاصلية التي كانت موجودة للجهاز قبل ان نقوم بالتعديل عليها وستمحى كل التغييرات التي قمنا بها ويرجع الجهاز الى ضبط المصنع.

التبويب الاخر هو حفظ نسخة احتياطية من اعدادات الجهاز وارجاع الجهاز الى نسخة محفوظة سابقاً (backup and restore) والتي عند النقر عليها تظهر النافذة ادناه:

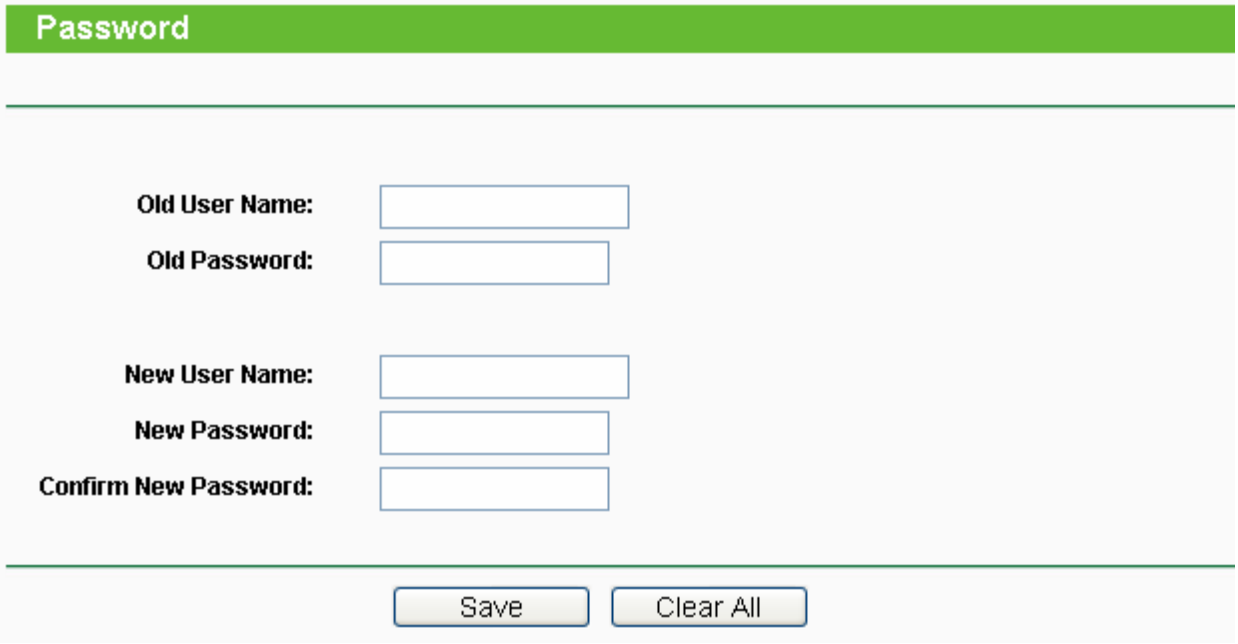
وعند النقر على (backup) يقوم الجهاز بحفظ نسخة (.bin) من الاعدادات الحالية في الحاسوب ويمكن الرجوع اليها في حالة حصول خلل في المستقبل بالنقر على زر (browse) واختيار النسخة المحفوظة او المنزلة من الموقع ثم النقر على (restore) ليرجع الجهاز الى الاعدادات المحفوظة مسبقاً.

ملاحظة: تستغرق عملية الاسترجاع ٢٠ ثانية ويجب الحرص على عدم إطفاء او انطفاء الجهاز اثنائها لأن ذلك سيسبب تلف الجهاز وعدم القدرة على الاستفادة منه بعدها.

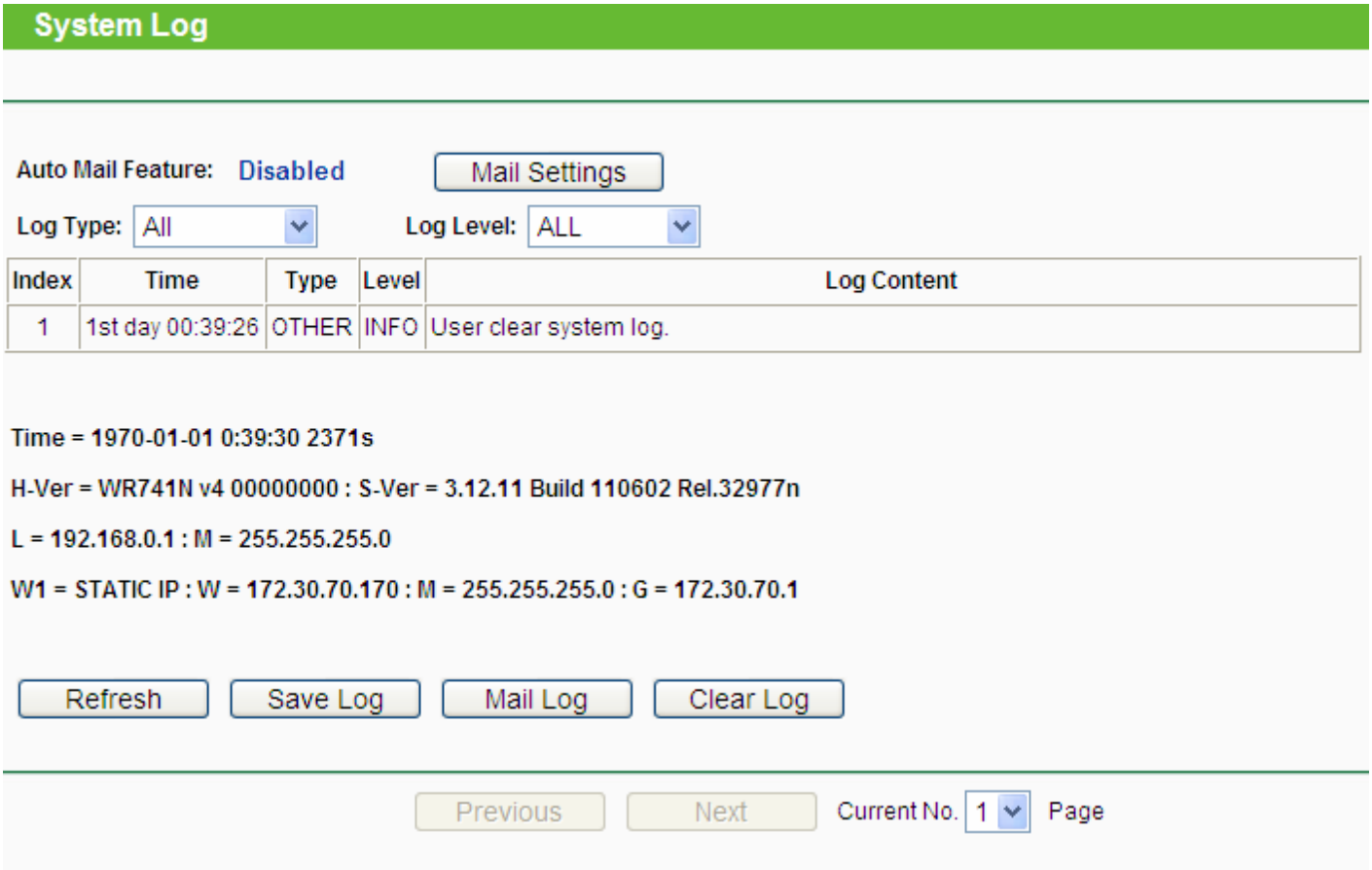
التبويب الاخر من ضمن أدوات النظام هو إعادة التشغيل (reboot) ونستخدمه أحيانا بعد اجراء تعديلات معينة على الجهاز او حين نحس بوجود بطء في الجهاز ونريده ان يعود الى وضعه الطبيعي وعند النقر على هذا التبويب تظهر النافذة التالية:



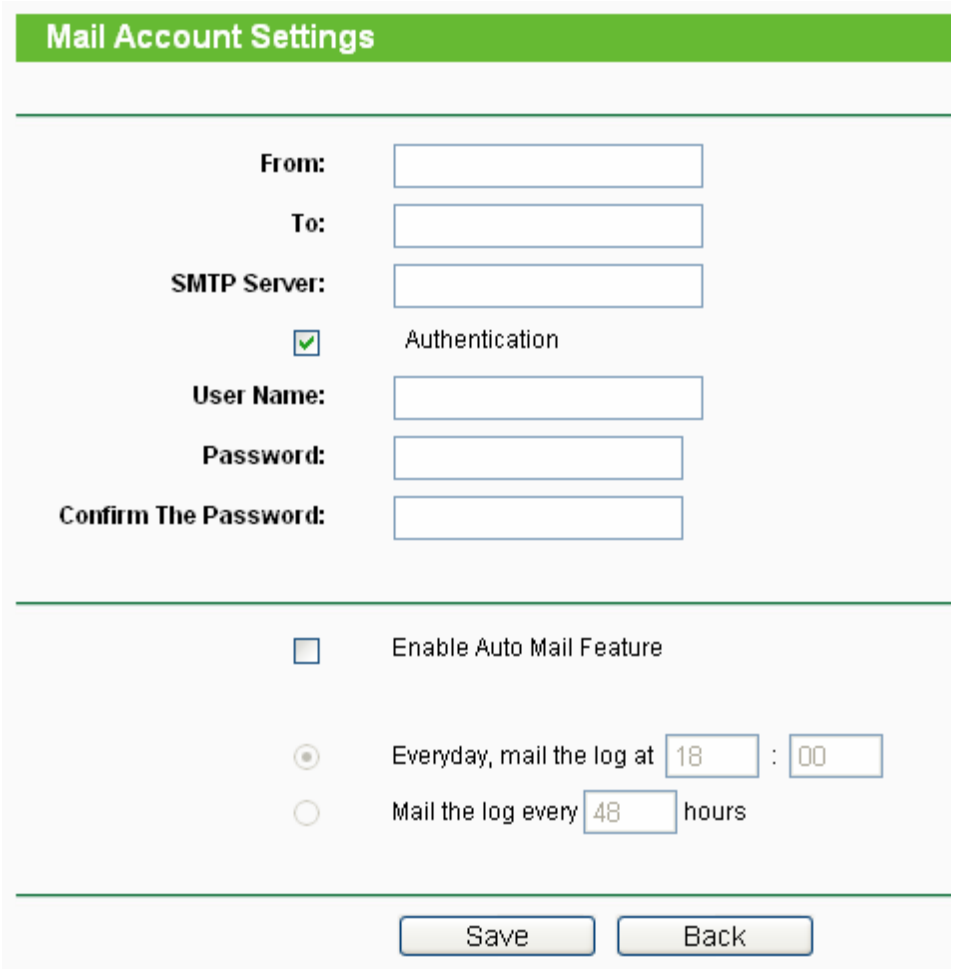
ننقر على (reboot) فيقوم الجهاز بعملية إعادة تشغيل حيث ان بعض الاعدادات لا تتغير الا بعد إعادة التشغيل مثل العنوان (IP address) ان تم تغييره و الترقية والاسترجاع والاعدادات اللاسلكية واعدادات ال (DHCP) وغيرها.
التبويب الاخر خاص بكلمة المرور للراوتر وإمكانية تغييرها وكما في النافذة ادناه:



حيث يمكن ادخال كلمة المرور السابقة (old password) وكذلك اسم المستخدم القديم (old user name) واستبدالهما باسم مستخدم جديد (new user name) وكلمة مرور جديدة (new password) وحفظ التغييرات من زر (save).
ملاحظة: اسم المستخدم الجديد يجب ان لا يزيد عن ١٤ رمز ويجب ان لا يحتوي أي مسافات فارغة وانتبه الى ان كلمة المرور الجديدة يجب ان يتم إدخالها مرتين للتأكيد.
التبويب الاخر هو سجل النظام (system log) والذي عند النقر عليه تظهر النافذة التالية:

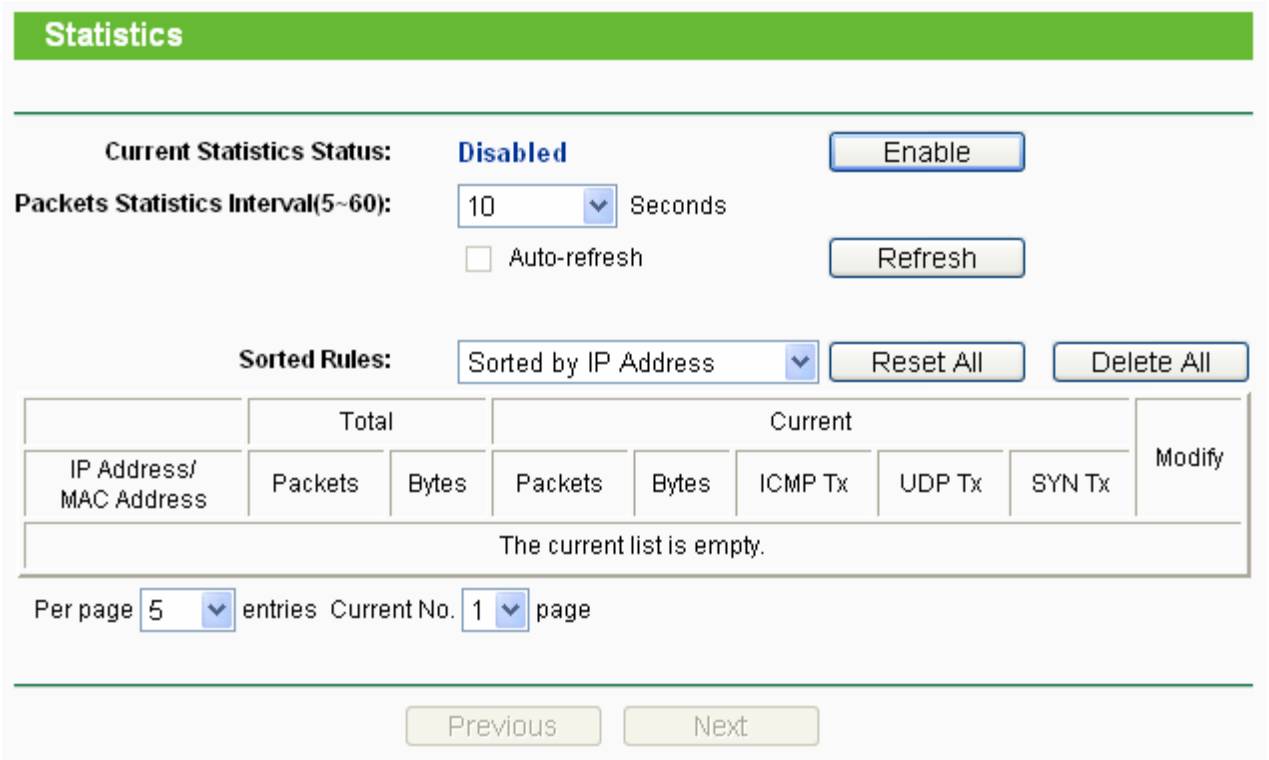


ويفيدنا هذا التبويب في حالة اردنا ان يقوم الراوتر بأرسال نسخة من سجل فعاليات الجهاز الى بريدنا الالكتروني حيث يجب اولاً تفعيل (enable) خاصية ال (auto mail feature) ثم ملء اعدادات البريد (mail settings) والتي عند النقر عليها تظهر النافذة التالية:



وهنا نحدد الرسالة من اين (من صندوق بريد شبكتك الداخلية) والى اين (الى بريدك الالكتروني) وعبر سيرفر (SMTP) الخاص بشبكتك الداخلية وعند اختيار (وضع علامة صح) لخيار تدقيق الدخول (authentication) يجب ادخال اسم المستخدم وهو اسم بريدك الالكتروني للشبكة الداخلية المحلية او المنزلية ان كنت قد فعلت فيها ال (SMTP) مسبقاً وبدون ما بعد ال (@) أي انه لو كان بريدك الالكتروني (mustafa@missan.com) فتقوم بكتابة اسم المستخدم (mustafa) فقط واما كلمة مرور البريد الالكتروني فيتم إدخالها كاملة واما بقية الخيارات فتحدد فيها نوعية المعلومات التي يراد لسجل النظام ان يسجلها ويرسلها بالبريد.

التبويب الأخير في قائمة أدوات النظام هو تبويب الاحصائيات (statistics) والذي عند النقر عليه تظهر النافذة التالية:



هنا تكون الاحصائيات معطلة افتراضياً ويمكن تفعيلها وتمكينها بالنقر على زر (enable) ويمكن إبقاء بقية الاعدادات على حالها وتجدر الإشارة الى ان تمكين الاحصائيات يساهم في تحسين قابلية الجهاز للتصدي لهجوم ال (DoS) ونلاحظ من قائمة الاحصائيات ان الجهاز سيقوم بأحصاء المجموع الكلي للبايتات والبكتات الصادرة والواردة الى كل عنوان (IP and MAC address) ولمختلف أنواع البروتوكولات مثل (ICMP, UDP, SYN) وغيرها من الاحصائيات وحسب نوع الجهاز.
الى هنا ينتهي كتابنا هذا وتبقى دورتنا مفتوحة لأي جديد في عالم الشبكات المحلية وللمزيد حول هذا الموضوع وغيره مما يخص الشبكات والحاسوب والمعلومات العامة تفضلوا بزيارة موقعنا على العنوان التالي:

مدونة مصطفى صادق العلمية

www.mustafasadiq0.wordpress.com

مصطفى صادق لطيف

العراق- ميسان