Készítette: Petróczy Tibor

Routerek általános konfigurációja

Ebben a leírásban az egyik közkedvelt router (Cisco Linksys WRT54G) teljes konfigurációs palettáján haladok végig, személy szerint is ezt az eszközt használom otthoni felhasználás céljából.

Továbbá személyes tapasztalat alapján a Linksys routerek közül kifogástalanul működnek az E és a WRT típusú eszközök, illetve a NetGear és a TP-Link termékek is. (Ez a reklám helye☺)

Vásárlás előtt ajánlom mindenkinek a gyártói oldalakon elérhető router szimulátorokat, amelyekben hellyel-közzel a legtöbb funkciót és vezérlőpultot elérhetjük.

Alapvetően a legtöbb routert helyi hálózaton keresztül, vezetékes kapcsolat esetében tipikusan a helyi hálózat kezdő címével érhetjük el, ezt a router alapkonfigurációját tartalmazó leírásból megtudhatjók, de nyugodtan próbálkozzunk valamelyik IP címmel:

192.168.1.1
192.168.1.2
192.168.2.1
192.168.2.2

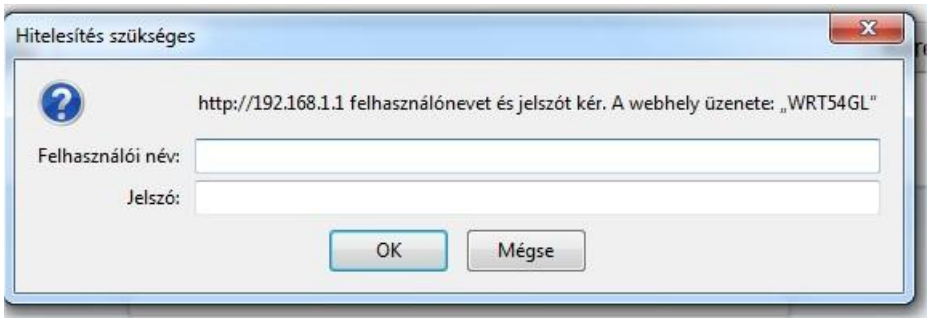
Az routerbe való belépésnél alapvetően arra kell figyelni, hogy nem biztos, hogy alapértelmezetten engedélyezve van a vezeték nélküli hálózaton keresztüli konfiguráció, ezért célszerű vezetékes kapcsolaton keresztül próbálkozni.

Szimulátorok:

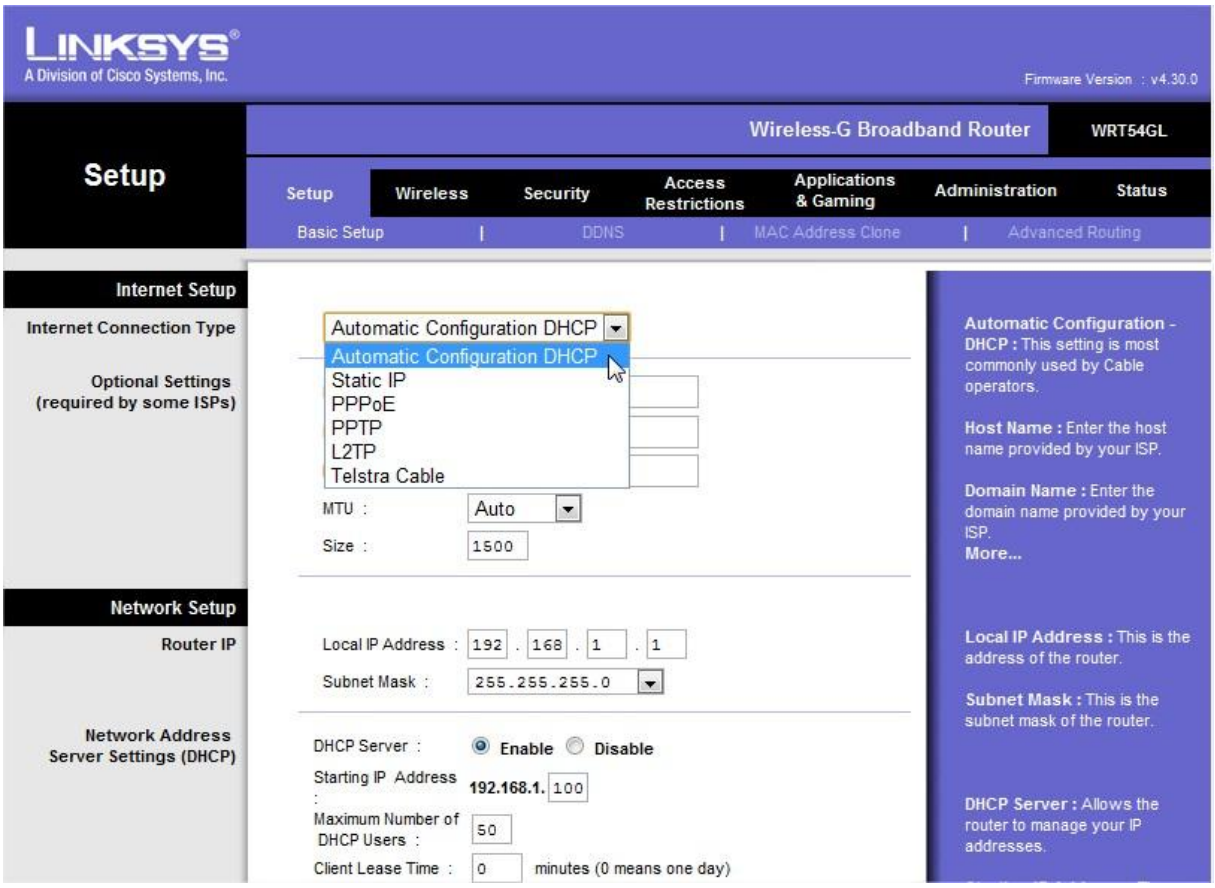
http://ui.linksys.com/
http://www.voiproblem.com/emulators/
http://www.tp-link.com/en/support/emulators/

Linksys WRT54G router konfigurációs leírás

1. Lépjünk be routerünk konfigurációs felületére a 192.168.1.1-es alapértelmezett címen, ahol meg kell adni a router konfigurációhoz szükséges adminisztrátori felhasználó nevet és jelszót, ez alap esetben „admin” – „admin” páros szokott lenni:



2. A router kezdőlapján némi információ látható a routerrel kapcsolatban (jobb felső sarok: telepített firmware verzió), továbbá a konfigurációs menü:



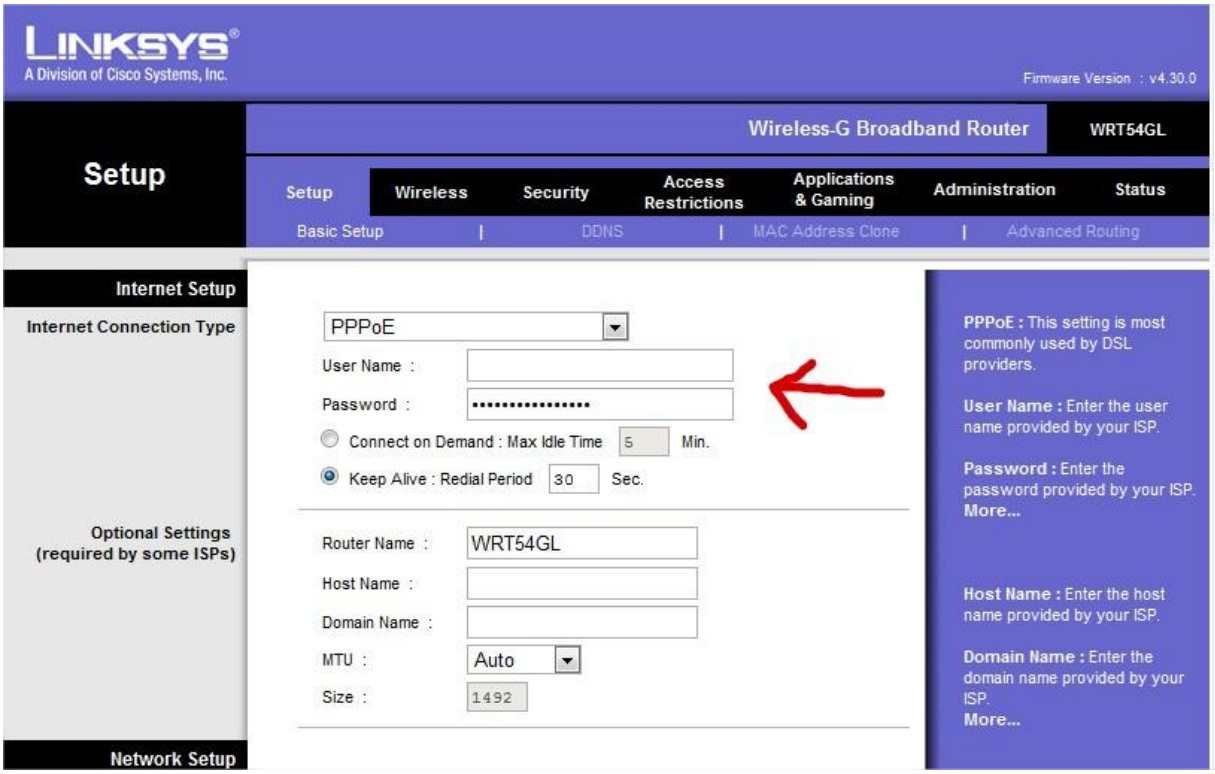
Talán a főoldalon a legfontosabb menüpont a beállítások közül az alap beállítások, ahol a hálózati kapcsolatunkat tudjuk szabályozni mind a külső és belső hálózat felé. Ezt úgy is szokták mondani, hogy a router külső lábához tartozó konfiguráció, amely valójában a külvilág, szolgáltatató (IPS), Internet vagy WAN megnevezésben is előfordul. A belső lába pedig értelemszerűen a belső hálózat (LAN) felé néző pontja.

Ezen a ponton tudjuk a szolgáltatónk álatal biztosított „Internet csatlakozási típus”-t beállítani, ahol a leggyakrabban előforduló az „Automatic Configuration DHCP”, a „PPPoE” és korábban a „Static IP”. Ez a 2 opció minden routerben megtalálható. A többi opció (PPTP, L2TP, Telstra, Bigpond…) router függő szokott lenni.

A 3 alapértelmezett beállítás között a szolgáltatás fajtájától függően beszélhetünk különbségről. Az „Automatic Configuration DHCP” esetében gyakorlatilag nincs szükségünk semmilyen beállításra a szolgáltató felé, mivel ezt ő nyújtja számunkra automatikusan egy általa üzemeltetett DHCP kiszolgáló segíttségével.

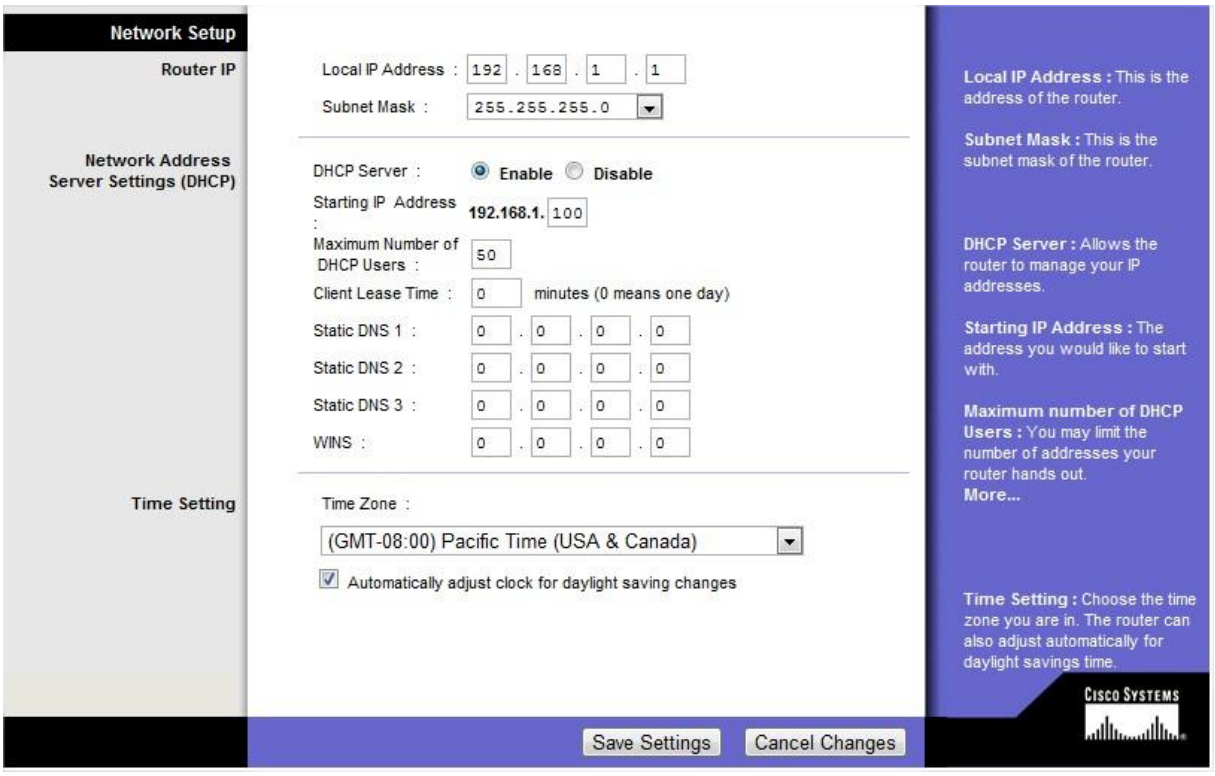
A „Static IP” esetében a szolgáltatóval megkötött szerződéssel egyidejüleg megkapjuk a konfigurációhoz szükséges IP beállításokat, amelyet fixen használunk (ez nem egyenlő a FIX IP cím igénylésével).

Talán a 3. leggyakoribb eset a „PPPoE” kivitelezés, ez a **Point To Point Protocol over Ethernet** mozaikszavát takarja, amely gyakorlatilag a régen használt betárcsázós megoldáshoz hasonlítható, ahol egy felhasználónév és jelszó páros segítségével a szolgáltatónkhoz felcsatlakozunk, és ezután használhatjuk a hálózatot.



Ezen kívül némi technikai beállításra is van lehetőségünk, mennyi legyen a maximális tétlenségi idő, vagy a kapcsolat életbentartásához mekkora legyen az újrahívási idő köz (pl: 30 sec), továbbá opcionális adatokat is megadhatunk (router neve, host név, domain név, MTU – Max Transfer Unit).

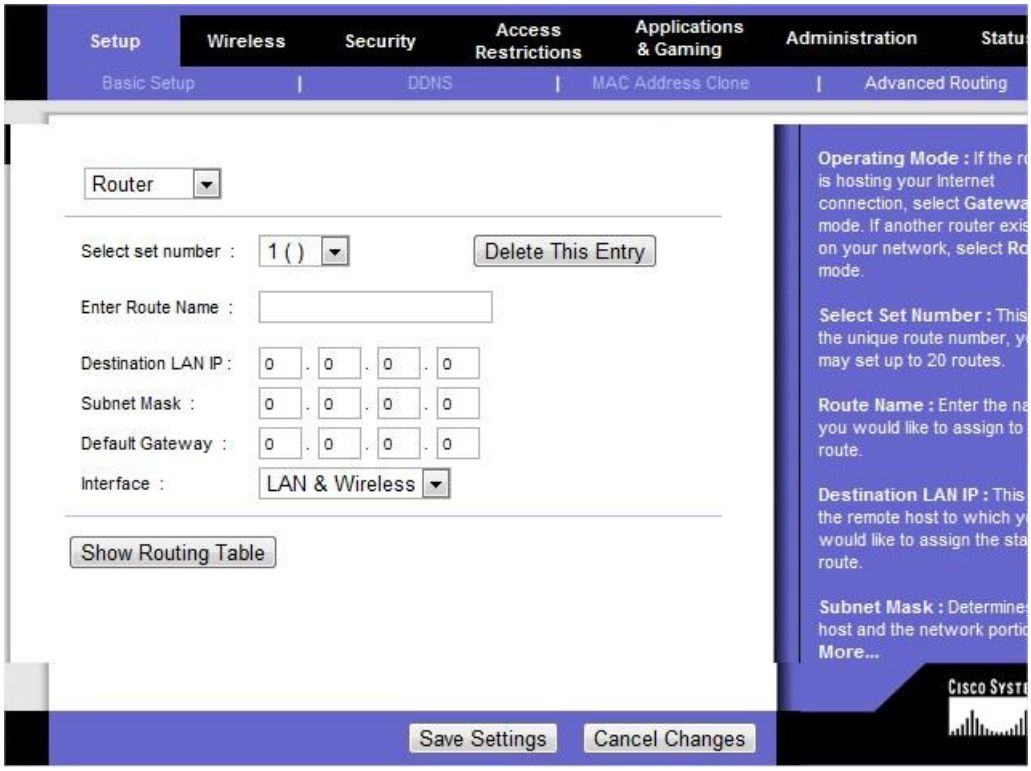
Ezt követően ugyanezen a panelen tudjuk szabályozni a belső hálózat paramétereit, mi legyen a router kezdő címe, és ezzel egyben a belső hálózati cím intervallum, és az ehhez tartozó hálózati netmaszk, illetve ezek mellette a router által biztosított DHCP kiszolgáló (belső hálózat felé) paramétereit tudjuk szabályozni.



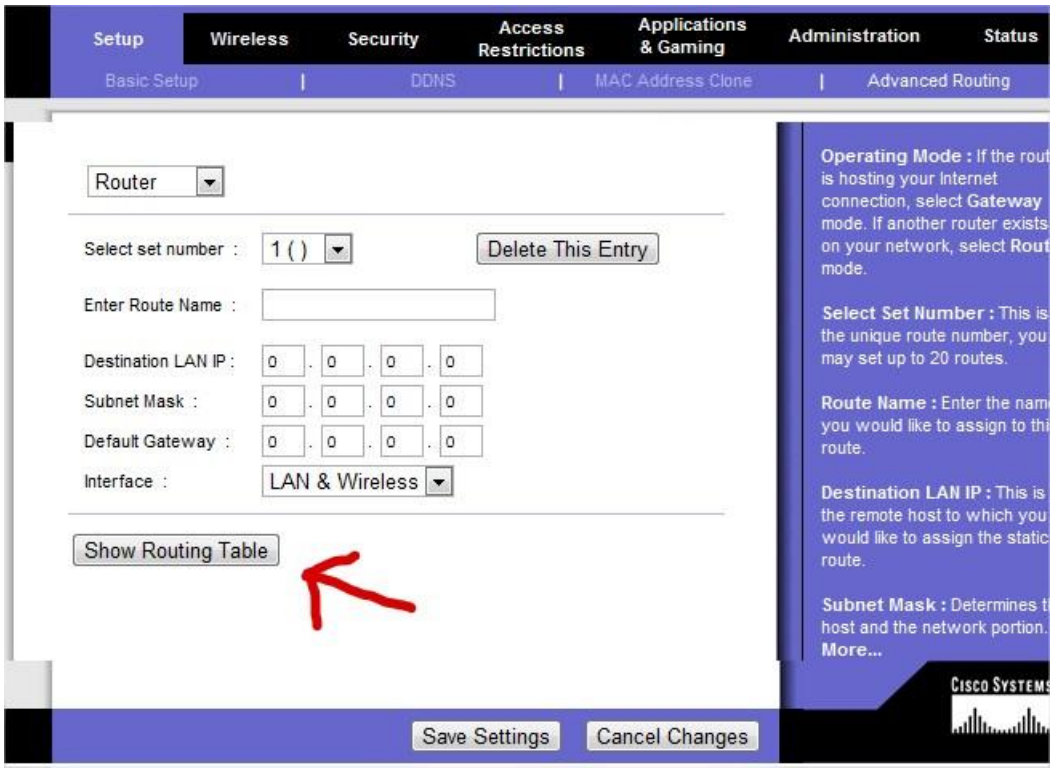
3. Az alapbeállítások után a 2. menüpontot választva „DDNS” (Dynamic DNS) konfigurációs paneljára tudunk lépni, ennek a támogatottság router függő szokott lenni, hogy melyik DDNS szolgáltatást nyújtó oldalak vannak beintegrálva, ezek közül a legnépszerűbb a „DynDNS.org”. Ezen szolgáltatás eléréshéz szükséges egy regisztrációval rendelkeznünk, ahol birtokunkban van egy dinamikus domain név, és a hozzá tartozó felhasználó és jelszó páros. Miért is van erre szükségünk? Ezen opcióval ugymond a routerünket (külső láb) könnyedén elérhetjük az előbb említett dinamikus dns ismeretében és a szolgáltatás beállítását követően, így nincs szükségünk IP címek megjegyzéséhez, főleg abban az esetben ha az Internetet szolgáltató IPS-ünk változtatja időszakosan a külvilág felé néző IP címünket.

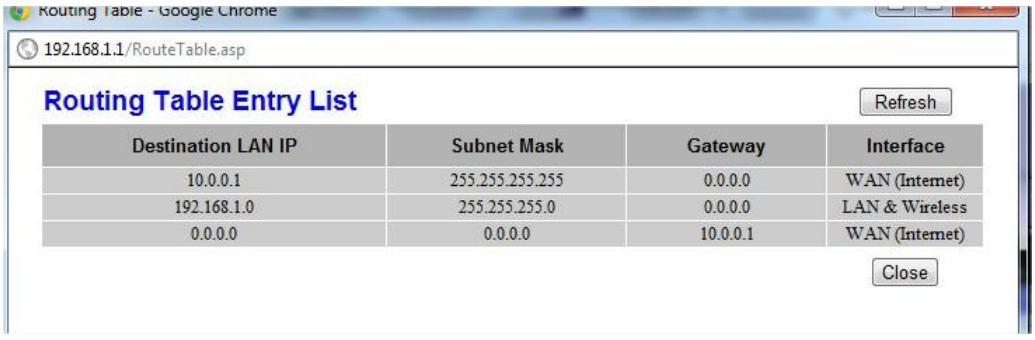
4. A következő panelen az „alapértelmezett” hálózati kártyánk MAC (Media Access Control – fizikai cím) címét tudjunk klónozni a router számára. Erre a funkcióra akkor van szükségünk, ha a szolgáltatónk az előfizetésünket egy adott MAC címhez rendeli, ekkor csak azzal a hálózati kártyával (NIC) tudjunk használni az Internet elérést, viszont a routerek ezen funkciójával elrejtjük (maszkolás) a router MAC címét, és a szolgáltatóhoz rendelt MAC címet klónozzunk a router MAC címére.

5. A következő panel az „Advanced Routing”, amely egy speciálisabb területe a beállításoknak. Itt bizonyos hálózati forgalmakat testreszabhatunk, gyakorlatilag statikus útvonalakat állíthatunk be a routeren keresztül. Több útvonal elkészítésére van lehetőségünk, amelyet csak használat előtt ki kell választanunk.



Aktuális forgalomirányító tábla listázása:





6. Következő lépésként konfiguráljuk a „Wireless” hálózatunkat

Vezetéknélküi hálózat kiépítése az elsődleges cél, amiért felhasználók otthon routert kezdenek el használni, azonban ez a terület az, ami a legtöbb biztonsági kritériumot magával hordozza, ugyanis egy vezetéknélküli kapcsolat esetében, nem korlátozhatjuk a levegőben áramló csomagokat, hogy az mások is ne „láthassák”.

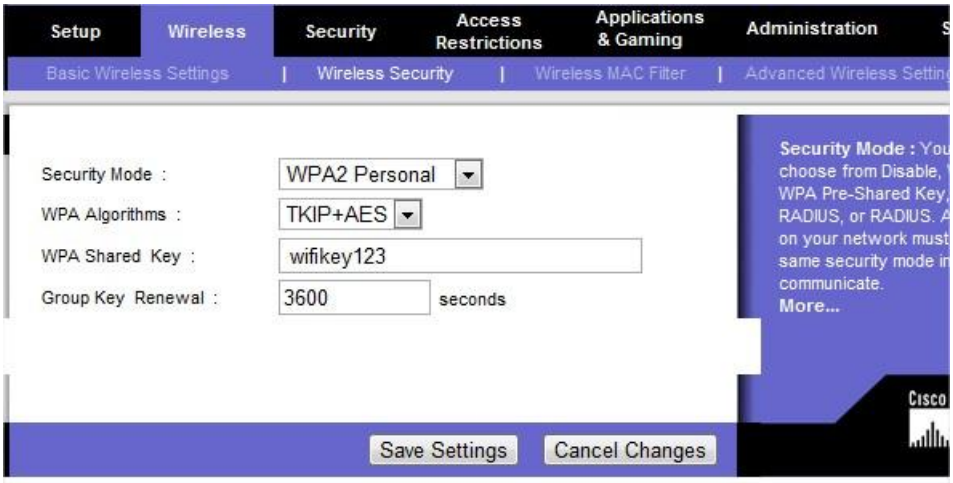
Első körben a vezetéknélküli hálózati módot (Wireless Network Mode) tudjuk szabályozni, ahol a router által támogatott szabványok közül van lehetőségünk választani. Célszerű a „Mixed” módot választanunk, mivel ezzek kiküszöböljük azt a lehetséges hibát, hogy egy WiFi kliens nem támogatná az általanunk preferált hálózati módot, így automatikusan a kliensnek megfelelő módon fog kommunikálni a router.

Továbbá megadhatjuk az „SSID”-t, amellyel azonosítjuk a routerünket a hálózaton.

Kiválaszthatjuk a WiFi csatornáját, ennek akkor van jelentősége, ha a közelben több-több router üzemel, amelyeknek a hatóköre fedheti egymást, így célszerű különböző csatornákon üzemeltetni az eszközöket az esetleges „áthallás” miatt.

Utolsó opcióként az SSID üzentszórását tudjuk beállítani, ennek előnye, hogy könnyedén ki tudjuk választani a wifi klienseken a keresett routert, viszont így egyszerűen mások is láthatják a wifi sugárzást.

Következő menüpontunknak van a legnagyobb jelentősége a vezetéknélküli hálózatok üzemeltetésében, ugyanis itt tudjuk a biztonsági beállításokat megtenni:

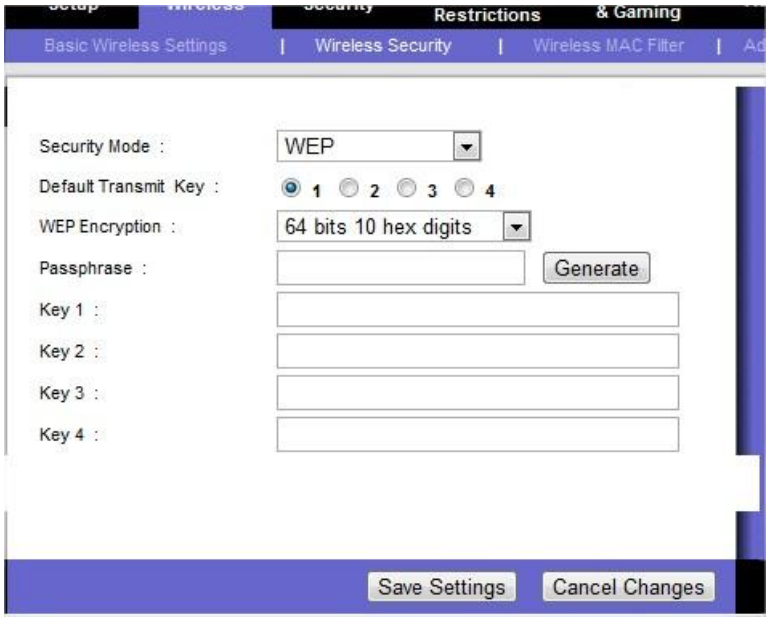


Alapvetően 7 opció közül választhatunk, ezek közül otthoni felhasználásra a „WPA2 Personal" a legbiztonságosabb, viszont tisztába kell lennünk, hogy a titkosítási módok közül melyeket ismerik a wifi kliensek, mert ez gondot okozhat. Az előző képen láthatunk egy általános beállítást otthoni felhasználásra, itt a titkosítási mód „WPA2 Personal", a felhasznált algoritmus „TKIP+AES", az előre beállított jelszó (key) „wifikey123", és a a kulcs megújjítási kérelem pedig 3600 másodpercenként történik.

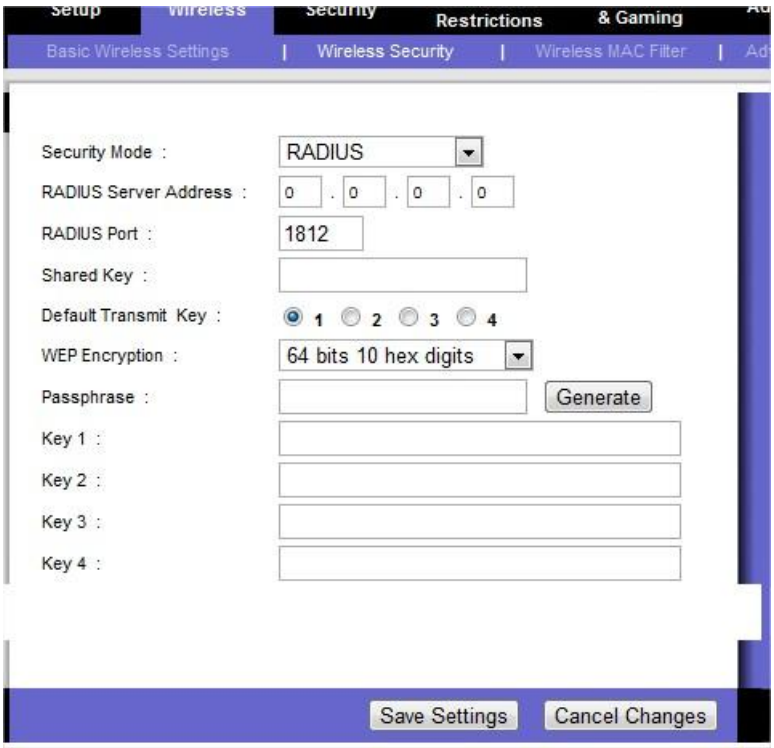
A következő ábárn a választható módokat látjuk:

A biztonsági módok közül a legrégebbi a WEP (Wired Equivalent Privacy) technológia, azonben ezt a titkosítási módszer megfelelő eszközök birtokában pár perc feltörni, ezért erősen ajánlott ennek a nélkülözése. A következő képen a régebben használt WEP mód beállítási paneljét látjuk, ezt csak ismertetés képpen tüntetem fel, viszont a gyakorlati életben már nem „használjuk". Erről a panelről annyit kell tudnunk, hogy beállíthatjuk a használt kulcsot titkosításának mélységét (64, 128bit), továbbá megadhathatunk több kulcsot is, amelyet a routerben opcionálisan választhatunk.

Ezzel szemben a WPA (Wi-Fi Protected Access) és a WPA2 részben más algoritmust használ a titkosításra és a titkosítási metódus is másképpen épül fel. A használt algoritmusok az AES (Advanced Encryption System) sé a TKIP (Tempory Key Integrity Protocol).

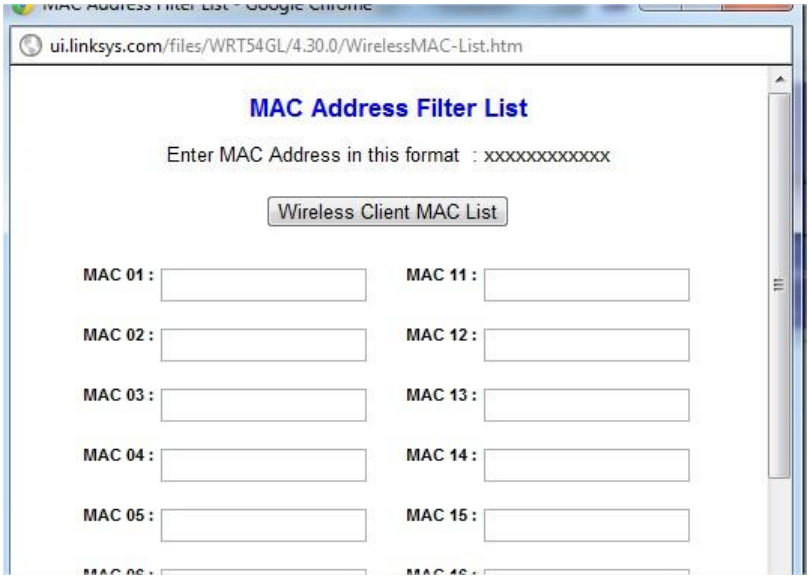


A következő képen egy „RADIUS" konfigurációs panelt látunk, erről a módszerről annyit szükséges tudnunk, hogy az authentikációs folyamatot a routerrel ellentétben egy külső szerver végzi el, ezzel biztonságosabbá tehető a hálózat egy esetleges fizikai hozzáférés esetén is.

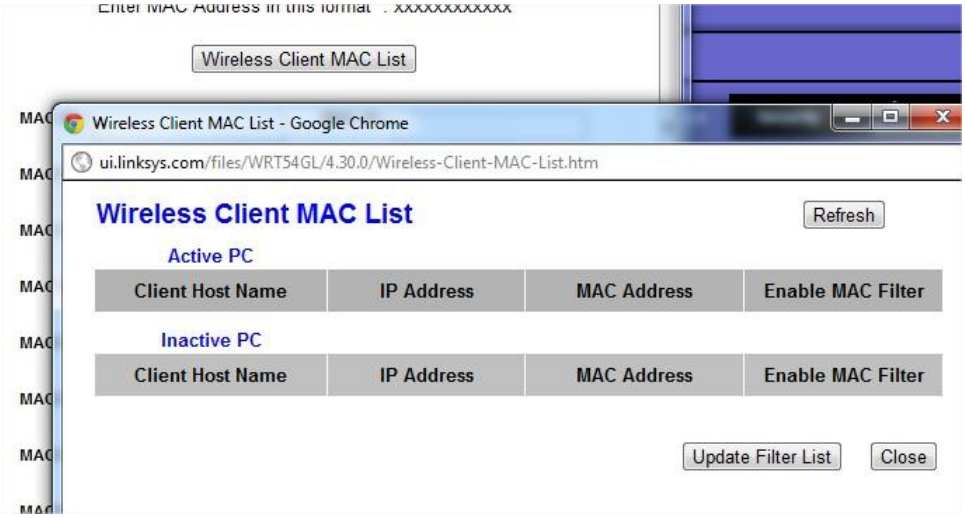


A következő panelen lehetőségünk van MAC cím szűrést beállítani, így csak a megadott MAC címmel rendelkező kliensek tudnak csatlakozni a routerhez. Ez biztonsági szempontból nem mondható jó megoldásnak mivel könnyedén kikerülhető.

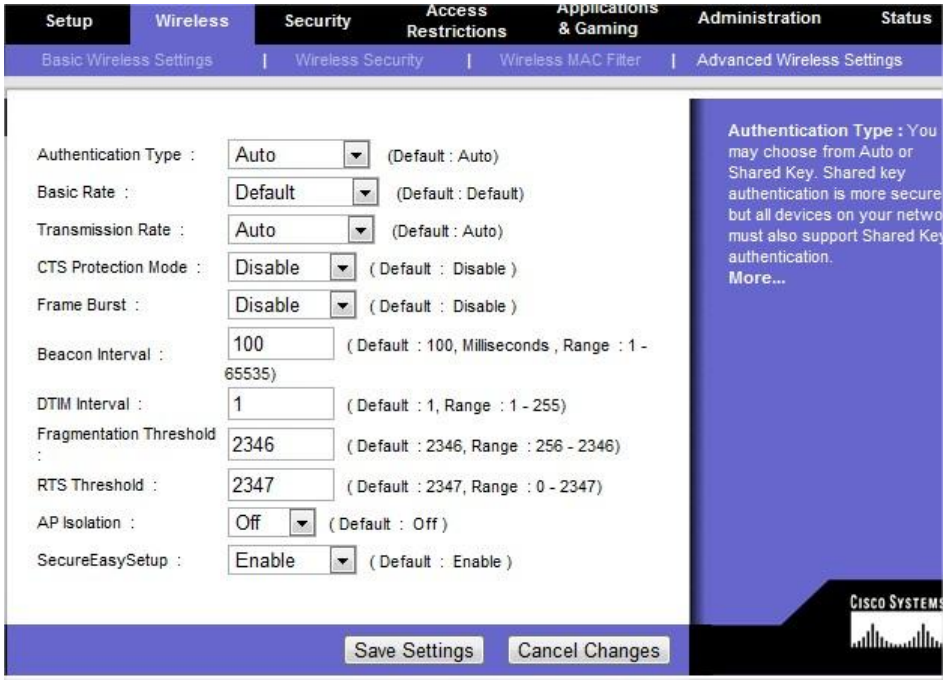
Az „Edit MAC Filter List” gomb megnyomásával kapjuk a következő ablakot, ahol a MAC címeket tudjuk felsorolni a megadott formátumban:



Az érvénybe lépett MAC címek és aktív eszközök listája:



Az utolsó ablak, amely a vezetéknélküli hálózat beállításához tartozik már speciális paraméterek megadását teszi lehetővé:



Authentication Type: ezzel tudjuk a hitelesítési módot beállítani, ez alapértelmezetten az „Auto" funkciót használja. Ez az opció teszi lehetőv a nyílt vagy megosztott kulcs alapú hálózat használatát.

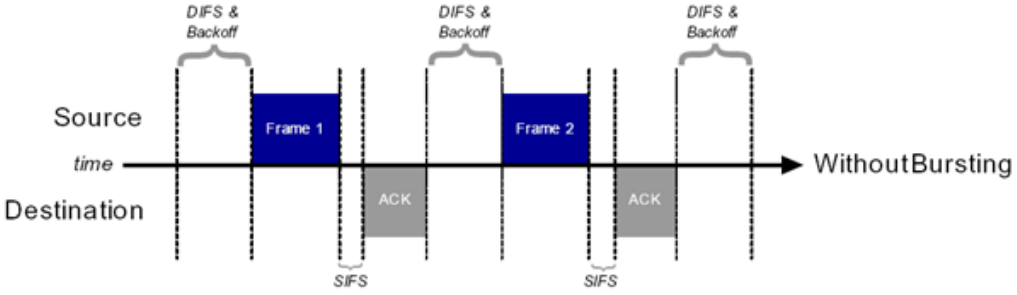
Basic rate: ezzel az alapértelmezett átviteli értéket tudjuk szabályozni, ahol a „Default" érték minden eszköz számára megfelelő, ha viszont régebbi klienseket használunk, akkor a lehető legkisebb értéket kell választanunk.

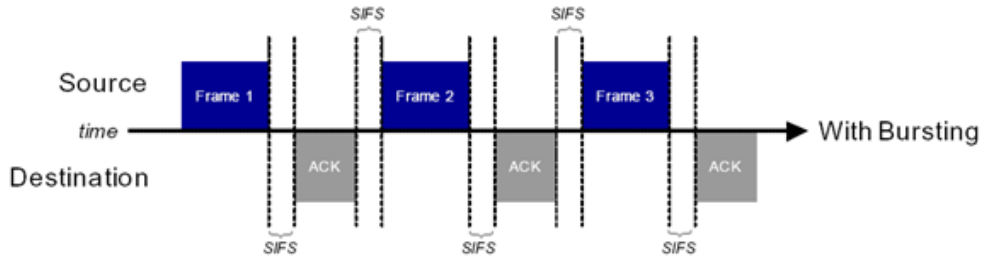
Transmisson Rate: az alapértelmezett átviteli sebességet tudjuk meghatározni.

CTS Protection Mode: CTS=Clear To Send védelmi mód, ez egy biztonsági beállítás, amely alapértelmezetten tiltva van, és így gátoljuk a routerünk működését, mivel túl sok 802.11g-s szabványnak megfelelő eszköz csatlakozik, akkor a 802.11b-s wifi szabvány lép életbe, ha csak a G módot szeretnénk, akkor engedélyeznünk kell.

Frame Burst: alapértelmezetten tiltva van ez a funkció. Ez egy átviteli technika, amely a 802.11e QoS szolgáltatás specifikációja, melynek segítségével növelni tudjuk az átviteli teljesítményt.

Mellékelek két képet, amely szemlélteti ezen technológia használatát és mellőzését:





A technológia lényege hogy a 2. esetben, tehát mikor használunk Frame Burst-öt, akkor a DIFS (Distributed InterFrame Space), vagyis a szükséges várakozási időt nem várja meg a küldős fél.

Beacon Interval: alapjel időköz, a két alapjelsugárzás közötti idő nagysága, ezt nevezhetnénk a vezetéknélküli ügyfelek és a hozzáférési pontok „szívverésének", olyan rádiójel, mely a hálózatot arról értesíti, hogy még aktívak. Az érték 1 és 1000 ezredmásodperc között legyen, te a tényleges érték maximálisan 65535 lehet.

DTIM Interval: Delivery Traffic Indication Message (kézbesítendő adatforgalom jelzésének üzenete), ez egy olyan üzenet, amely a hálózat engergiatakarékos ügyfeleit értesíti arról, hogy nekik szóló információ érkezik, hogy aktiválhassák magukat és fogadni tudják az üzenetet. A kisebb érték azt mutatja, hogy az ügyfelek nem kapcsolhatnak túl sokáig energiatakarékos módba, a magasabb érték azt jelenti, hogy energiatakarékos módba kapcsolhatnak, de sokáig aktívnak kell lenniük, mert több információ összegyűjtve jut el hozzájuk.

Fragmentation Threshold: feldarabolási küszöb, a csomagméret maximális nagysága, melyet meghaladva az útválasztó az adatcsomagokat feldarabolva küldi el. Információ küldésekor általában akkor lép fel probléma, ha a küldött adatok ütköznek a hálózat egyéb adatforgalmával. Ez a küldött információ feldarabolásával javítható lehet. Minél alacsonyabbra állítja a darabolási küszöb értékét, annál kisebb lesz a fel nem darabolandó csomagok mérete. A maximális értéket (2346) használva feldarabolás gyakorlatilag nem történik.

RTS Threshold: az RTS-küszöb (Request To Send) a maximális bájtméret, amelyért az adáskérés, adáskérés törlése (RTS (Request to Send) / CTS (Clear to Send) csatorna állítási mechanizmus működik. Jelentős rádióinterferenciát, vagy nagyszámú vezeték nélküli eszközt egyazon csatornán tartalmazó hálózat esetén az RTS-küszöb csökkentése segíthet csökkenteni a keretveszteséget. Az RTS-küszöb alapértelmezetten 2347 bájt, ami a maximális érték.

AP Isolation: ha esz az opció engedélyezve van, akkor minden wifi eszköz számára létre lesz hozva külön egy virtuális hálózat, így az eszközök nem tudnak kommunikálni egymással. ezt érdemes használni, ha sok vendég vezetéknélküli eszközre lehet számítani.

SecureEasySetup: A SecureEasySetup™ megkönnyíti a vezeték nélküli kliensek csatlakoztatását vezeték nélküli útválasztójához. A SecureEasySetup automatikusan konfigurálja a vezeték nélküli biztonsági beállításokat az útválasztó és a vezeték nélküli kliensek között. A SecureEasySetup folyamat alatt, az útválasztó SecureEasySetup információt közvetít, hogy a vezeték nélküli kliensek végre tudják hajtani a SecureEasySetup folyamatot, és megkapják az új **Network Name** (Hálózatnév) (SSID), módszertípus, titkosítási típus, és jelmondat adatokat a hálózattól.

7. „Security” menüpont beállításai

Ezen „Security” (biztonsági) beállítások a routeren keresztül menő kapcsolatok biztonsági kritériumaira, módjaira és tűzfalszabályaira vonatkozik.

Két menüpont közül tudunk választani az első a „Firewall” (Tűzfal), a második pedig a „VPN” (Virtual Private Network).

Lehetőségünk van az útválasztónk (roter) által nyújtott tűzfal ki és bekapcsolására. A tűzfal szabályok tekintetében 4 opciót tudunk állítani.

Az első opció (Block Anonymous Internet Request) segítségével a hálózatunkat tudjuk elrejteni a külvilág felől, egyszerűen a router tiltja a WAN hálózatból érkező ismeretlen kéréseket (ide tartozik a ping is).

A második opció engedélyezésével a kivülről érkező multicast forgalmat tudjuk tiltani (ezt az ISP-től kaphatjuk).

A harmadik opció segítségével a hálózati címfordítást tudjuk tiltani (ezt nem célszerű engedélyznünk), ezáltal a helyi szerverinket nem tudjuk kivülről elérni.

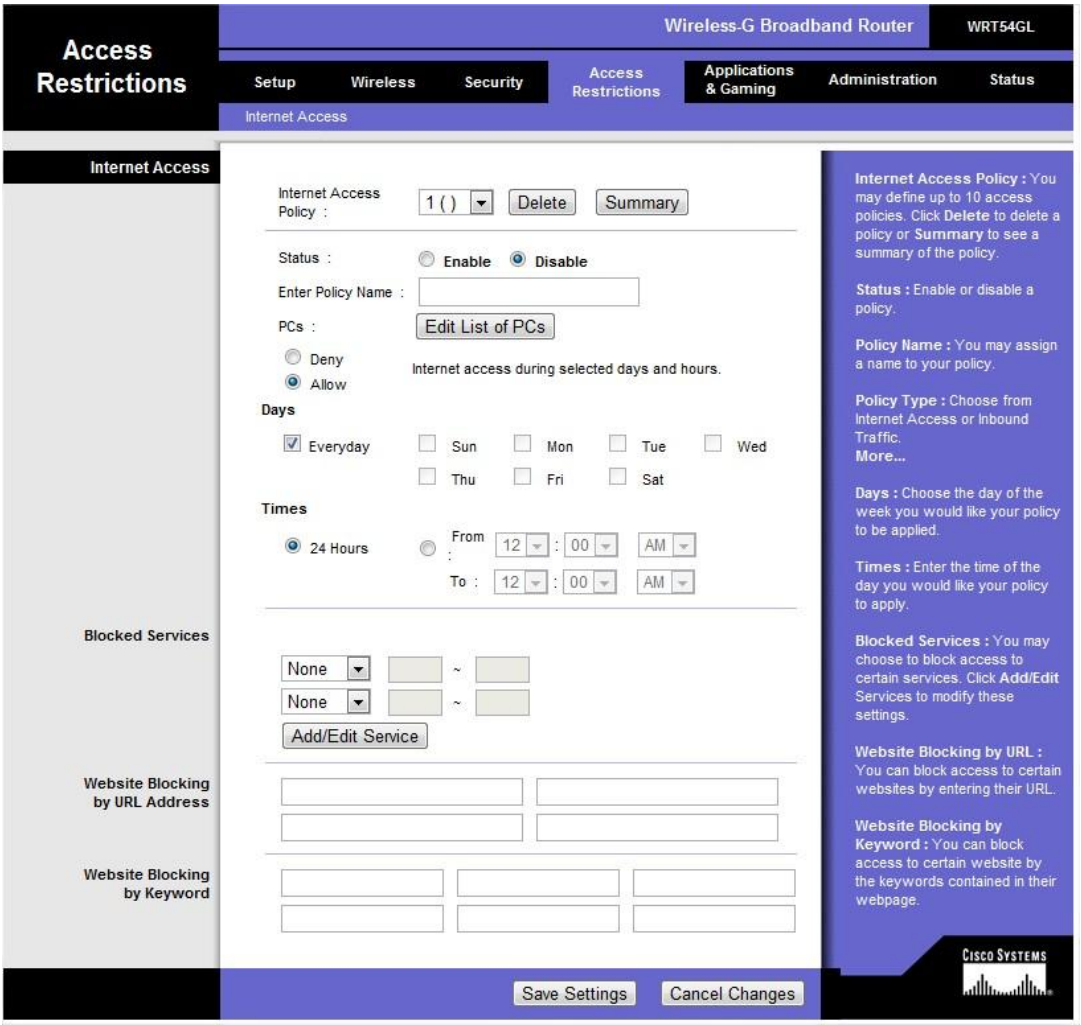
A negyedik opció egy speciális portot figyel a 113-as porton üzemelő IDENT (Ident Protocol), amely egy speciális authentikációs szolgáltatáshoz szükséges, amelyen keresztül hozzáférhetünk a felhasználóinkhoz, így biztonsági rést is jelenthet egy belső hálózat szempontjából.

A következő (VPN) panelen tudjuk szabályozni, hogy az útválasztónk mely protokollokat engedje át virtuális magánhálózat kiépítése céljából. Itt 3 protokoll közül tudunk választani IPSec, PPTP, és L2TP. Az, hogy melyikre van szükségünk az attól is függ, hogy a belső hálózatunkat, vagy egy külső VPN hálózatot mely protokoll segítségével szeretnénk elérni. A protokollok működésükben merően eltérnek, ezért szükséges ismerni a technikai hátteret.


Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Firewall
VPN
IPSec Passthrough :
Enable
Disable
PPTP Passthrough :
Enable
Disable
L2TP Passthrough :
Enable
Disable
Save Settings
Cancel Changes

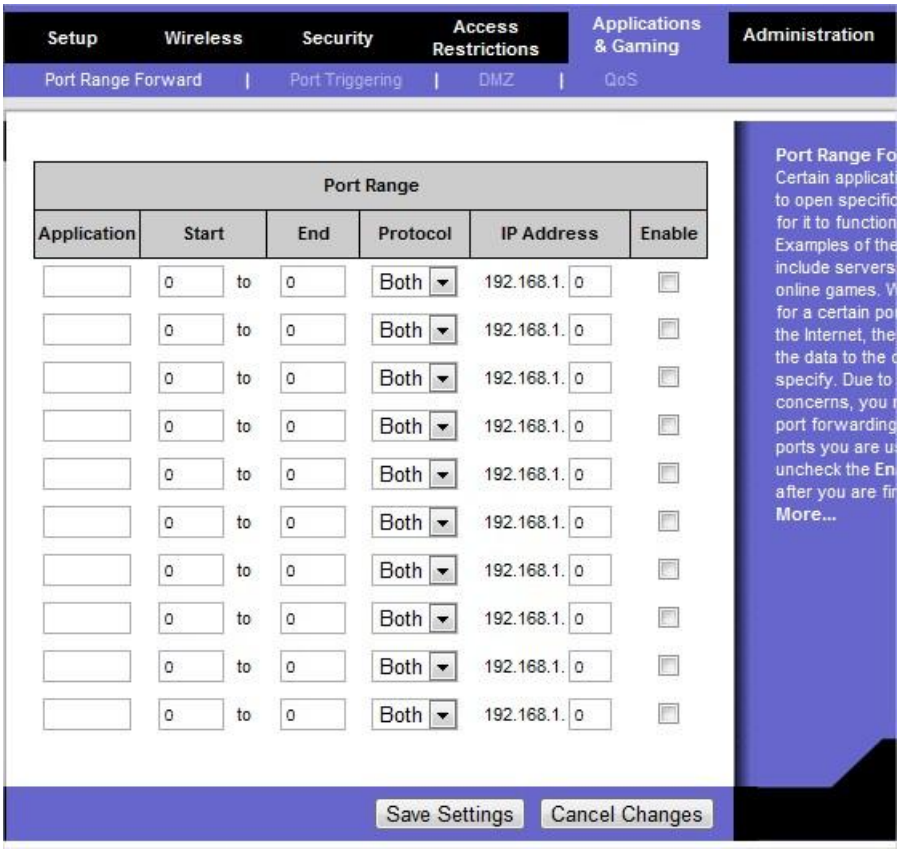
8. Következő panelünk az „Access Restrictions”, amely a hálózati, illetve Internet elérésünk szabályozásában lehet segítségünkre. Ezen a panelen több házirendet (Policy) tudunk kialakítani, amelyet testreszabhatunk gépenként, időszakonként (napok, napon belüli időszak).

   A korlátozásoknál lehetőségünk van szolgáltatások tiltani protokoll szinten, vagy új szolgáltatást felvéve tiltani port szinten, továbbá weboldalakat blokkolhatunk közvetlenül URL által, vagy keresőszavakat megadva.

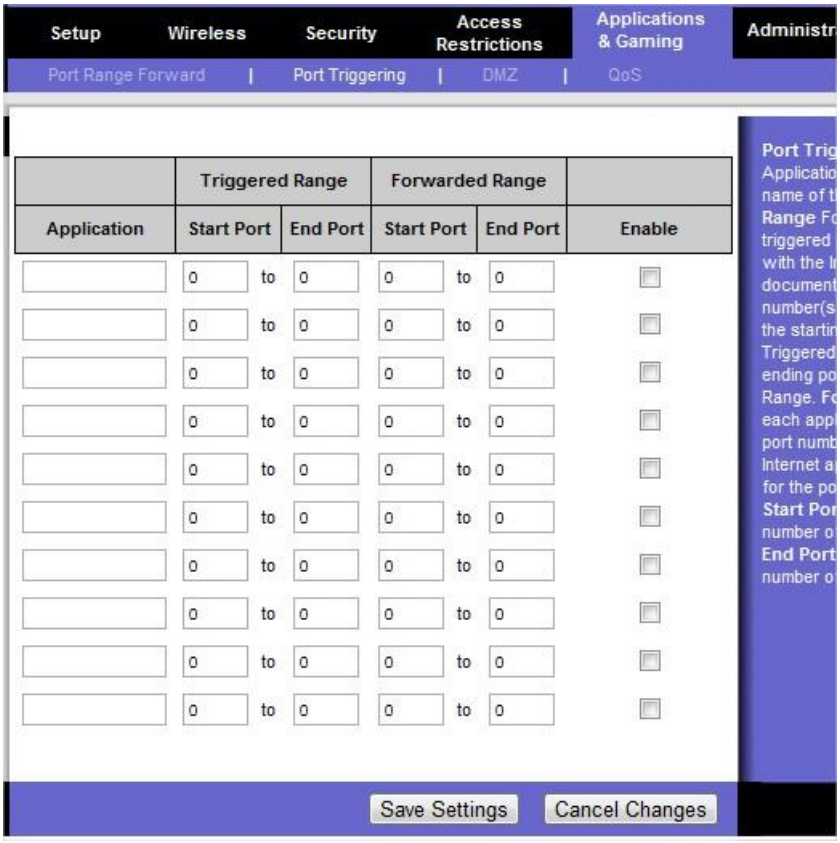


9. Az „Applications & Gaming” menüpontban tudjuk szabályozni a különböző alkalmazások (programok, játékok) használatához szükséges hálózati beállításokat. Itt tudjuk, beállítani, hogy a külső és a belső hálózat között a kommunikáció hogyan menjen vége alkalmazás, port, protokoll szinten.
   Első körben a **Port Range Forward** (Porttovábbítás) használatával a bejövő adatforgalmat a hálózat egy meghatározott ügyfeléhez továbbíthatja. A portok olyan csatlakozások, amelyeket a számítógép a különféle hálózati adatforgalmak szervezésére használ. Egy port támogathat egyidejűleg kimenő és bejövő hálózati adatforgalmat, illetve egyirányú hálózati adatforgalmat.

   Ha megnyit egy portot, egy meghatározott szolgáltatás lesz hozzárendelve, és az a szolgáltatás a hálózat felé csak azon a porton keresztül kommunikál. Néhány alkalmazásnak szüksége lehet nyitott szervizportokra, mint pl. internetes játékok, videokonferencia, internetes telefon vagy hasonló alkalmazások.E funkció kihasználásának egyik példája, ha webkiszolgálót üzemeltet valamelyik hálózati kliensen. A porttovábbítás engedélyezésével a webhely adatforgalma áthalad az útválasztón, és közvetlenül a megfelelő hálózati klienshez jut ahelyett, hogy az útválasztón áthaladva elérné az egész hálózatot.
   Például, az útválasztó alapértelmezett porttovábbítási szabállyal rendelkezik egy web szerverhez a hálózaton, ahol a portokat a web forgalomhoz (80) a webkiszolgáló IP-címéhez kell irányítani (alapértelmezett IP-cím: 192.168.1.120). A szabály engedélyezéséhez válasza az **Enable** bejelölő négyzetet a szabályhoz.

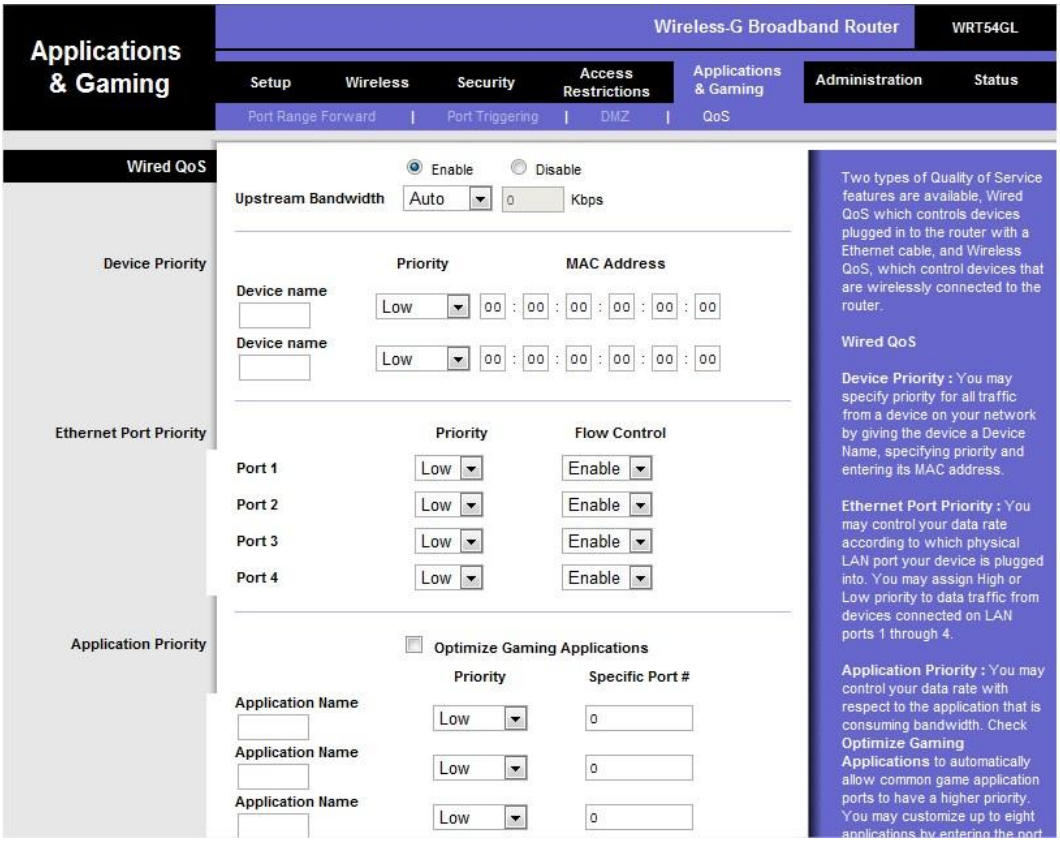


A második opció, mint **Port Triggering** (Portfigyelés) segítségével elérhető az, hogyha néhány alkalmazás úgy csatlakozik az internethez, hogy egy vagy több kimenő portot használ elvárva, hogy a távoli hoszt visszacsatol egy, vagy több bejövő porton. Alapértelmezetten az útválasztó lezár minden bejövő kapcsolatot. A portfigyeléssel beállíthatja az útválasztó tűzfalát úgy, hogy a válaszok elérjék ezeket az ügyféleszközöket.

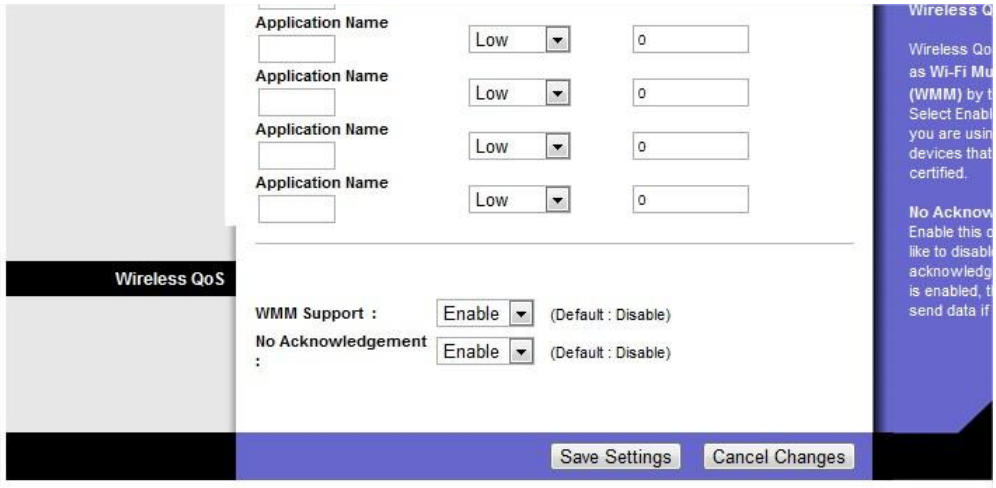


Harmadik almenüpontukban a DMZ zónára vonatkozó beállításokat tehetjük meg. A DMZ (Demilitarizált övezet) egy olyan számítógép, amelyhez minden külső internetforgalom befut, mint például egy webkiszolgáló. Így a számítógép számára lehetővé válik a korlátozás nélküli kétirányú kommunikáció. Ezt a funkciót óvatosan kell használni, mert megkerüli a számítógép biztonságát jelentő tűzfalat.

Jelen főmenüpontunk utolsó almenüjében a **QoS** (Quality of Service), mint minőségi szolgáltatás technológiáját kihasználva tudunk különböző konfigurációs beállításokat elvégezni. Ezen opció segítségével a különböző szolgáltatások minőségén tudunk javítani akár vezetékes akár vezetéknélküli kapcsolatban állunk az útválasztónkkal. Megadhatjuk az előtérbe helyezett sávszélességet, prioritási szempontból a különböző eszközöket (WiFi), rangsorolhatjuk a router vezetékes portjait, továbbá alkalmazásokat rangsorolhatunk.



Az utolsó 2 pontban a WMM (Wifi Multi Media) támogatását tudjuk szabályozni, ahol a WMM tanúsított eszközök élveznek elsőbbséget. Az utolsó opcióval pedig az újraküldést tudjuk tiltani adatküldés során, ha valamilyen hibe lépett fel.

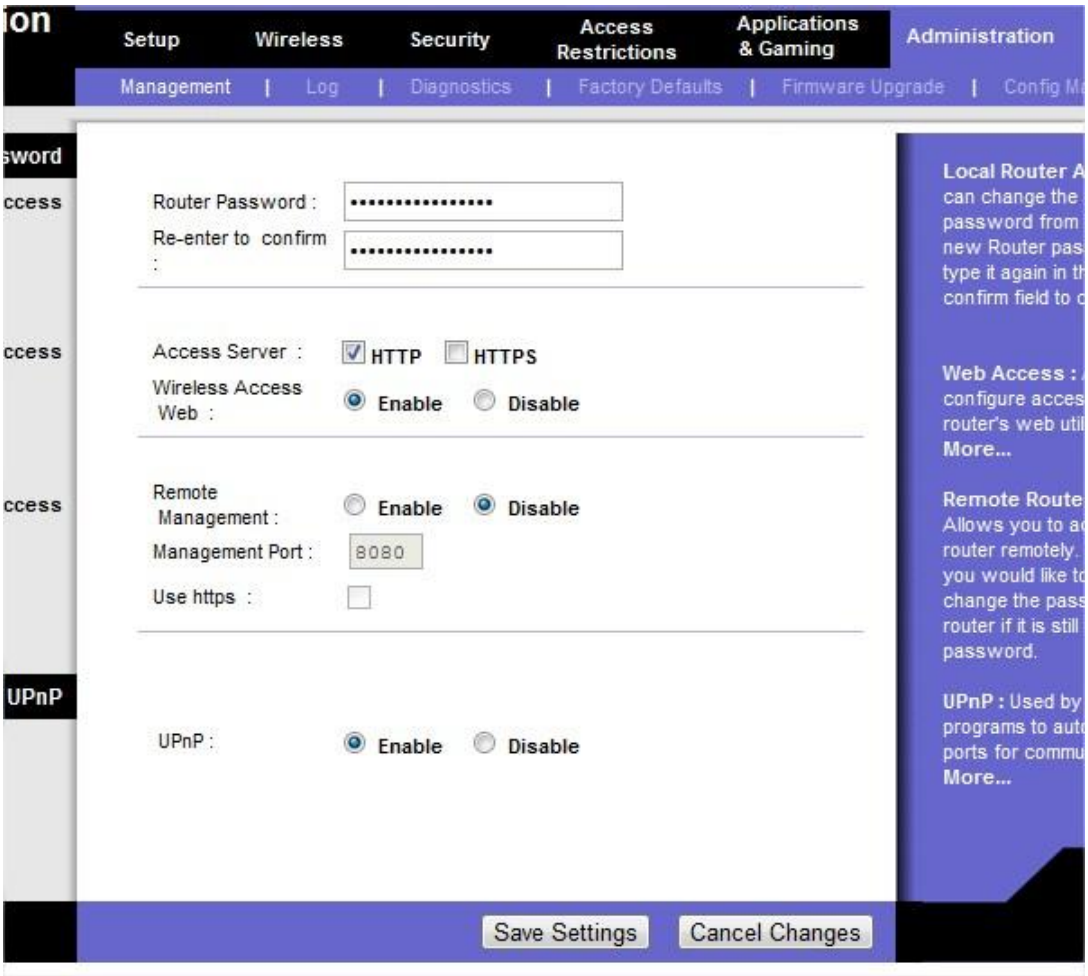


10. Az utolsó előtti „Administration” menüpontunk az útválasztó tényleges adminisztrációját, illetve a hozzá tartozó hozzáféréseket, beállításokat, frissítéseket tartalmazza.

    Az első almenüben a „Management” esetében tudjuk meghatározni a router konfigurációs felületéhez tartozó jelszót tudjuk beállítani, továbbá tudjuk szabályozni, hogy az adminisztrációs felületet web felületen keresztül el tudjuk-e érni, és ehhez melyik protokolt vagy protokollokat használjuk (http, https), elérhető-e a felület vezetéknélküli kapcsolaton keresztül.

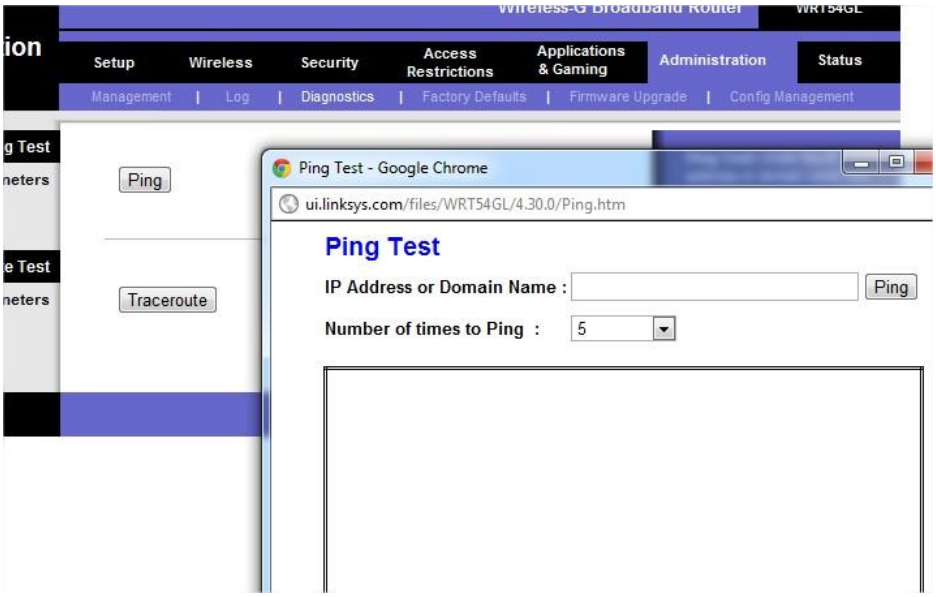
    Lehetőségünk van távoli menedzsment bekapcsolásra, ekkor meg kell adnunk, hogy a távvezérléshez melyik portot használjuk.

    Utolsó opcióként pedig az **UPnP** (Universal Plug and Play) funkciót tudjuk engedélyezni, amelyre akkor van szükség, ha bizonyos programoknak szükségük van speciális portokra a működésükhöz, de mi nem szeretnénk ez folyamatosan menedzselni (lásd korábban a „Port Range Forward”), így a programok automatikusan engedélyt kapnak port nyitásra és zárásra.



Második almenüben egyszerűen a naplózást (Log) tudjuk bekapcsolni, illetve kikapcsolni, és itt van lehetőségünk a bejövő és kimenő naplókat tanulmányozni.

Harmadik almenüpontunk a „Diagnostics”, ahol hálózati diagnosztikát tudunk elvégezni, ez a „Ping” és a „Tracerouter” parancsban merül ki, amelyek segítségével tesztelni tudunk távoli, vagy belső IP címeket, domain neveket, ezáltal látjuk, hogy a kapcsolat él-e, esetleg az útvonal esetében valahol valamilyen elakadásra számíthatunk.



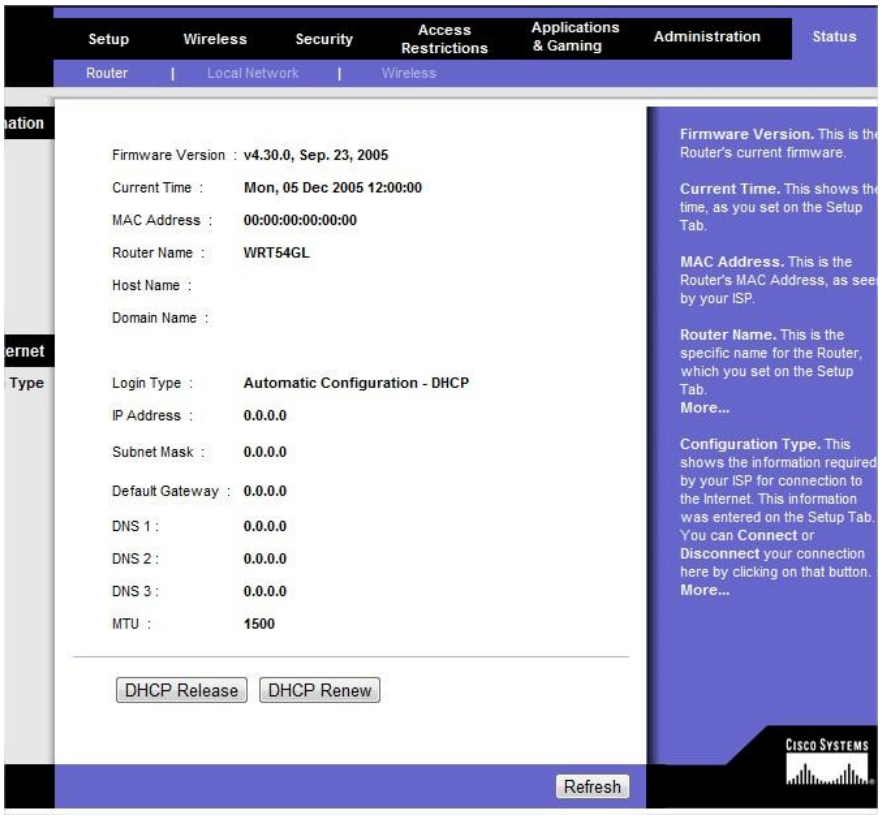
Negyedik almenünkben egyszerűen a gyári beállításokra térhetünk vissza, és nem szükséges hardveres resetet csinálnunk.

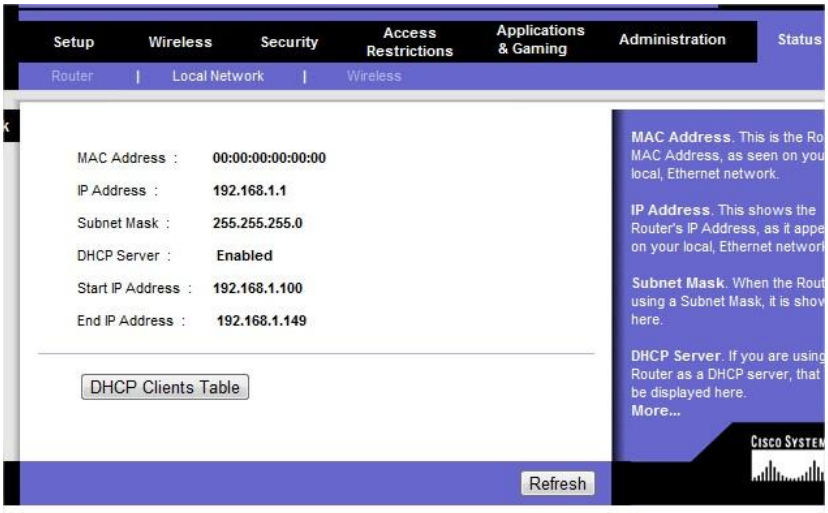
Az ötödik almenü pontunkban tudjuk a meglévő firmware-t frissíteni. Itt gyakorlatilag a gyártó oldaláról letöljük az újonnan kijövő szoftvert, és ezt ebben a menüpontban betöltjük, amire vigyáznunk kell, hogy a frissítés alatt folyamatos árram forrás legyen, és lehetőleg a routerünk kábeles kapcsolatban legyen a frissítést végző számítógéppel.

Az utolsó menüpontban pedig a meglévő konfigurációkat tudjuk letölteni, amit egy esetleges resetelés, vagy frissítés után nyugodtan visszatölthetünk, és nem szükséges újonnan elvégeznünk a konfigurációs beállításokat.

11. Status

Az utolsó főmenüpontban „Status” egyszerűen a beállításokról szerezhetünk információt, mind az útválasztó, mint a helyi hálózat (Local Network) és a vezetéknélküli hálózattal kapcsolatosan.





Ezzel a rövid leírással szerettem volna bemutatni az egyik közkedvelt router (útválasztó) menüpontjait, és egy lehetséges konfigurációt.

Azonban fontos megjegyezni, hogy a menüpontok, és az általuk vezérelt konfigurációs paraméterek routerenként eltérőek lehetnek, és ezért figyelmesen olvassuk el és tanulmányozzuk a saját roterünk beállítását.