1. Bevezetés

A számítástechnika napjaink egyik leginkább fejlődő iparága. A rendkívüli ütemű technikai fejlődésnek köszönhetően napjainkra már csaknem mindenki számára elérhető közelségbe kerültek a különféle számítógépek. Az otthoni felhasználásra szánt konfigurációk teljesítménye messze meghaladja az elmúlt évtizedek, évek elképzeléseit – lassan már az átlag felhasználó igényeit is. Az elektronikai berendezések ára – beleértve a számítógépeket is – jelentősen kedvezőbb lett a gyártási technológiák fejlődésének köszönhetően. Mára már a modern elektronikai berendezéseket is gyakran kisebb teljesítményű számítógépek vezérlik. A számítógépek felhasználhatóságuk sokszínűsége miatt is egyre jobban terjednek. A felhasználók más és más szempontok szerint választják ki a számukra megfelelő konfigurációt. A különféle igényeknek megfelelően előfordul, hogy egyetlen számítógép nem elegendő, így egyre gyakoribb az, hogy egy háztartáson belül több számítógép is van. Több számítógép, több felhasználó esetén előbb-utóbb felmerül az igény a különböző adatok, erőforrások megosztására. A kényelmi szempontokat is figyelembe véve a legegyszerűbb megoldás a számítógépek közötti kommunikáció megteremtése.

A számítógépek közötti kommunikáció megvalósításának feltételeit különféle szabványokban rögzítik (IEEE 802 szabvány család). A hálózatba szervezéskor a hálózati topológiák előnyeit, hátrányait szem előtt tartva az igényeknek megfelelően számos megoldás létezik. Kezdetekben a számítógépek közötti fizikai kapcsolat létrehozására a legkézenfekvőbb megoldás a direkt kapcsolat létrehozása kábelekkel megvalósítva. A vezetékes (helyi) hálózatok körében az Ethernet (802.3) és Token Ring (802.5) terjedt el leginkább. Később a tudomány és a technika fejlődésével elérhető közelségbe került a számítógépek hálózatokba szervezése vezetékek nélkül. A vezeték nélküli hálózatokat a 802.11x szabvány család foglalja magába. A 802.11a, 802.11b és a 802.11g változatok terjedtek el leginkább, melyek a frekvenciatartományukban, modulációban és ezek következtében a sávszélességben térnek el egymástól. Napjainkban a 802.11 szabvánnyal megvalósított vezeték nélküli hálózatok sávszélessége meghaladhatja a 100Mb/s -ot.

Manapság a kisebb-nagyobb otthoni-, irodai-, egyetemi- és egyéb magánhálózatokon túlmenően egyre jellemzőbb, hogy az önálló, helyi hálózathoz nem csatlakoztatott számítógépek is csatlakoztatva vannak egy globális hálózathoz, az Internethez. Ez komoly kockázati lehetőségek tárházát tárja fel előttünk. Amíg a számítógépek nem voltak hálózatokba szervezve, a bizalmasan kezelt, digitális formában tárolt adatokhoz csak kevesen és nehezen juthattak hozzá, ehhez fizikailag is a gép mellett kellett tartózkodniuk. A számítógép hálózatra való csatlakoztatását követően lehetőség nyílt a más számítógépeken tárolt (bizalmas) adatok hozzáférésére – a hálózat kiterjedésétől függően akár több 100km távolságról is. Az adatok távoli elérésének lehetősége jogosan váltja ki azt a nyilvánvaló kérdést, miszerint: „Biztosan csak a jogosult személyek férnek hozzá az adatokhoz?”.

Mai rohanó világunkban már egyre kevesebb szituációban követelik meg a személyes kapcsolatfelvételt, ügyintézést, minden elintézhető egy hivatalos levéllel, kérvénnyel, egyszerű telefonhívással vagy akár az interneten keresztül is. A számítógépes hálózatok tehát nem csak az otthonunkban található, „jól elzárt”, „lekódolt” számítógépen tárolt (bizalmas) adatainkra jelentenek veszélyt, hanem ezen adatait meggondolatlanul közlő felhasználó személyére is. Interneten keresztül történő ügyintézésekor például vásárláskor, pénzügyi tranzakciók bonyolítása esetén a megfelelő intézkedéseket (titkosítás, stb.) a pénzintézetek biztosítják ugyan, de a felhasználó gondatlansága, naivitása, ismerethiánya ellen lehetetlen 100%-osan védekezni.

Elsősorban tehát a hálózathoz való illetéktelen csatlakozás lehetőségét kell minimalizálni. Ehhez biztosítani kell, hogy a felhasználó számítógépét ne tudják mások jogosulatlanul használni, valamint a hálózat kábeleihez, aktív eszközeihez se férjenek hozzá illetéktelen személyek. A vezetékes hálózatokhoz való (illetéktelen) csatlakozás bár adott esetben szabad szemmel is látható, nehezen megelőzhető. A vezetékek „megcsapolása” nem lehetetlen, bár az optikai szálak esetében ez lényegesen komplikáltabb, mint UTP, vagy koaxiális kábelek esetén. A vezetékes hálózatokkal szemben a vezeték nélküli hálózatokhoz való illetéktelen csatlakozásnak, csatlakozási kísérletnek „nincsenek” látható nyomai. A vezeték nélküli hálózatok esetén a hálózat fizikai elérése mindössze a rádiójel erősségétől függ, ha van a csatlakozáshoz elegendő jelerősség, akkor már csupán a hitelesítési, titkosítási protokollok állnak az illetéktelen felhasználó útjában.

Egyelőre még csak a hálózatokhoz való fizikai csatlakozásról esett szó, de ezt követően természetesen a hálózatot el is kell érni a megfelelő jelszavakkal, azonosítással, hitelesítő igazolással. Az illetéktelen adathozzáféréseket megelőzendő sokfajta szoftveres-, hardveres védelmi mechanizmus és eszköz létezik. Ezeknek a lehetőségeknek a zöme viszont a hálózatra már csatlakoztatott számítógépek, valamint azok adatainak védelmét próbálják biztosítani, és nem pedig a hálózathoz való illetéktelen csatlakozást.

Vezetékes hálózat esetén, ha a hálózathoz fizikailag csatlakozik a számítógép, akkor általában már nincs további authentikáció, a hálózat teljes mértékben elérhető. A vezeték nélküli hálózatok biztonságára a hálózati közeg jellege miatt kell komolyabb figyelmet szentelni. Mivel a vezeték nélküli hálózathoz való csatlakozás „feltűnésmentes”, ezért általában a csatlakozáskor azonosítania kell magát a hálózathoz kapcsolódni szándékozó számítógépnek. Az azonosításnak több módja is lehet, ez a vezeték nélküli hálózat biztonsági szintjétől függ. Az authentikáció módja gyakran további adattitkosító eljárásokra is utal.

A továbbiakban a vezeték nélküli hálózatok tulajdonságait, változatit, eléréséhez, biztonságos használatához szükséges authentikációs és titkosítási technikákat ismertetem. A technikai részleteket csak a téma megértéséhez feltétlen szükséges mélységig érintem.

2. OSI – tól a 802.11x – ig…

Open Systems Interconnection Reference Model, magyarul a *Nyílt rendszerek Összekapcsolása referencia modell.* Az OSI modell egy rétegekbe szervezett rendszer absztrakt leírása, amely a számítógépek kommunikációjához szükséges hálózati protokollokat határozza meg.

Az OSI modellje a különböző protokollok által nyújtott funkciókat egymásra épülő rétegekbe sorolja. Minden réteg csak és kizárólag az alsóbb rétegek által nyújtott funkciókra támaszkodhat, és az általa megvalósított funkciókat pedig csak felette lévő réteg számára nyújthatja. A hét réteg hierarchikus rendszere meghatározza a két számítógép közötti kommunikáció feltételeit. Az *International Organization for Standardization* (ISO – Nemzetközi Szabványügyi Szövetség) a modellt az ISO 7498-1 szabványában írta le, és ’70-es évek végéig javasolta, mint hálózati szabványt.

Az OSI modell széleskörben elterjedt megvalósítása a TCP/IP, mely az Internet működését napjainkig biztosító protokollstruktúra. A TCP/IP modellt alapvetően négy réteg alkotta, melyet később ötre bővítettek (Hibrid modell).

- *Alkalmazási réteg (Application Layer)*
- *Szállítási réteg (Transport Layer)*
- *Hálózat (Internet) réteg (Network Layer)*
- *Adatkapcsolati réteg (Data Link Layer)*
- *Fizikai réteg (Physical Layer)*

Az OSI modellhez viszonyítva az 5-6. réteg (a viszony- és megjelenítési réteg) hiányzik.

A napjainkban már történelminek számító, különböző (általában egymással inkompatibilis) számítógépes hálózatokból az erőteljes szabványosításoknak köszönhetően kifejlődött az Ethernet. Az ISO foglalkozik a szabványosításokkal, vagyis, hogy a különféle technológiák széleskörben használhatóak, lehetőség szerint kompatibilisek legyenek. A számítógépes hálózatok szabványait a *Villamos és Elektronikus Mérnöki Intézet (Institute of Electrical and Electronics Engineers – IEEE)* dolgozta ki.

Az Ethernetet 1983-ban szabványosították (IEEE 802.3). A további Ethernet szabványok a Token Bus (802.4) és a Token Ring (802.5) nem kompatibilisek a 802.3–al, és mára már csak kevés helyen használják (csaknem teljesen halott szabványok). A szabvány a technikával együtt fejlődött, így nagyobb sávszélességet elérve, az eddigiekkel kompatibilis IEEE 802.3u Fast Ethernet és az IEEE 802.3z Gigabit Ethernet szabványok is megjelentek.

Az első vezeték nélküli hálózat a Hawaii Egyetem által 4 szigeten létrehozott ALOHAnet volt, melyben 7 állomás alkotta a kétirányú csillagtopológiájú hálózatot. Az eredeti IEEE 802.11 –et 1997-ben szabványosították.

Az IEEE 802.11 –es szabvány alapvetően két eszközt definiál. Az egyik a *vezeték nélküli állomás (wireless station)*, a másik elem a *hozzáférési pont (Access Point - AP)*, amely a vezeték nélküli állomásokkal kommunikál. Ennek megfelelően a szabvány szerint kétféle topológia létezik:

- ad-hoc
- infrastrukturális.

Az *ad-hoc (Peer to Peer – P2P)* topológia esetén a vezeték nélküli állomások közvetlen kommunikálnak egymással. Az ad-hoc üzemmódú állomások folyamatosan keresik az ad-hoc üzemmódra képes eszközöket. Ebben a topológiában nincs forgalomirányítás, így a kommunikáló állomások számának növekedésével az ütközések száma is jelentősebb. A kommunikációban résztvevő állomások számára való érzékenysége miatt az ad-hoc mód csak otthoni, illetve kevés vezeték nélküli állomással rendelkező, kisebb vállalati hálózatok kialakítására alkalmas.

Az *infrastrukturális* mód esetén a vezeték nélküli állomások hozzáférési ponton keresztül kommunikálnak egymással. Természetesen egy Access Point egyidejűleg több hozzá csatlakoztatott állomással is kommunikál egyidejűleg. A hozzáférési pontokat lehet csatlakoztatni a már meglévő (vezetékes) hálózathoz, így a vezeték nélküli állomások nem csupán egymással, hanem a már meglévő, hálózatba csatlakoztatott állomásokkal is képesek lesznek kapcsolatot létesíteni.

A *Wi-Fi (Wireless Fidelity)* védjeggyel ellátott Ethernet-kompatibilis, rádiófrekvenciás, vezeték nélküli helyi hálózatok előírásait és ajánlásait magába foglaló szabványgyűjtemény a 802.11. Az Ethernet vezeték nélküli verziójának is tekinthető. A vezeték nélküli hálózatok (WLAN) csupán az OSI modell alsó két rétegében térnek el a vezetékes (helyi) hálózatoktól (LAN). A 802.11 a fizikai és adatkapcsolati rétegeket definiálja, tehát a magasabb szinteken lévő protokollok (TCP/IP, stb.) működésében nincs különbség.

Az Ethernet szabványban a csatornát a csomópontok állandóan figyelik. Az ütközések detektálását a *CSMA/CD* (*Carrier Sense Multiple Access with Collision Detection*) protokoll segítségével valósítják meg. A CSMA/CD a Gigabit Ethernet esetén már csak félduplex működési módban szükséges, duplex mód esetén felesleges.

A 802.11x szabvány család mindegyik változata már a *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidence*) protokollra épül, az a, b, g változatok csupán a fizikai réteg kivitelében (modulációs módban, adatátviteli sebességben) különböznek. A CSMA/CA már jobban alkalmazkodik a vezeték nélküli közeghez, hiszen nem csak detektálja az ütközéseket, hanem meg is előzi azokat (az adatátvitel kárára). A hiba detektálása, elkerülésére- és kijavítására tett kísérlet a csomagok számát, a hasznos adat mennyiségét befolyásolja, korlátozza. A közeg adottságaitól függően is változó a maximális adatátviteli sebesség, ami általában a névleges érték maximum 50-60%-a.

A 802.11 szabvány család alszabványai egymással nem feltétlenül kompatibilisek, viszont a gyártók által forgalmazott eszközök mára már nem csupán egyetlen szabványt támogatnak. Ennek megfelelően léteznek olyan eszközök, melyek mind a három széleskörben elterjedt alszabványt (a, b, g) támogatják.

A *Wi-Fi* embléma nem a szabvány neve, hanem egy termékre kapható tanúsítvány. Ezt a Wi-Fi Alliance nonprofit szervezet adja 1999-től azoknak a termékeknek, amelyek valóban képesek gyártó függetlenül együttműködni egymással. A szövetségnek már néhány száz tagja van és ezernél is több termék kapta már meg ezt a minősítést.

2.1 Az IEEE 802.11x általánosan használt alszabványai és tulajdonságai

Az IEEE 802.11x szabványcsalád			
Alszabvány neve	*Frekvenciasáv*	*Max. adatátviteli sebesség*	*Modulációs technikák*
802.11	2,4GHz	1-2 Mbps	DBPSK, DQPSK
802.11a	5,7GHz	54 Mbps	ODFM
802.11b	2,4GHz	11 Mbps	DSSS, CCK
802.11g	2,4GHz	54 Mbps	DSSS, CCK, ODFM, DSSS-ODFM
802.11i	-	-	Biztonságtechnikai alszabvány
802.11n	2,4 GHz	540 Mbps	Még nem elfogadott

A 802.11x szabványcsalád fő tulajdonoságai

Az eredeti 802.11 szabvány 1-2 Mbps adatátviteli sebesség elérésére képes, és *FHSS (Frequency Hopping Spread Spectrum)* frekvenciaugratásos szórt spektrumú átviteli technikát alkalmaz. Az adó frekvenciáról frekvenciára ugrál egy másodperc alatt akár több százszor is. 79 db 1 MHz széles csatornát használ és álvéletlenszám generátor alapján ugrál. Ha az elején szinkronizálnak, vagyis ugyanazt a kezdőértéket (*seed*) használják, akkor ugyanazokat a frekvenciákat fogják végigjárni. Ezt a technológiát alkalmazza a mobiltelefonok körében igencsak elterjedt adatátviteli technológia a *Bluetooth* is. (Ezért kell a készülékeket „párosítani” a kapcsolat létrehozásakor.) A frekvenciaugrások miatt az átvitel biztonságos, a spektrumszórás következtében kevésbé érzékeny az interferenciára, az átvitel zavartűrése jobb lesz. Hátránya az alacsony sávszélessége.

A 802.11x eszközök az *ISM (Industrial, Scientific, Medical)* szabadon használható frekvenciasávban működnek. Az ISM sávban sok más eszköz működik, a garázskapunyitóktól kezdve, a vezeték nélküli- telefonokon, fejhallgatókon keresztül csaknem minden, ami a háztartásokban is használatos vezeték nélküli technológia. Szintén ezen a frekvencián üzemelnek a mikrohullámú sütők is. A frekvenciasáv viszonylagos zsúfoltsága miatt szükség van különböző, az átvitel megbízhatóságát elősegítő technikák alkalmazására. A 802.11 alszabványai ezen technológiákban és az alkalmazott ISM sáv frekvenciájában különböznek.

IEEE 802.11a

1999. őszén, a 802.11b-vel, egyidőben került szabványosításra. Működési tartománya 5GHz, ennek következtében nem kompatibilis a többi (2,4GHz–es) alszabvánnyal. Az 5GHz–es frekvenciasáv és az *OFDM (Orthogonal Frequency-Division Multiplexing)* moduláció alkalmazásának köszönhetően érték el a 802.11b-hez képest magasabb 54 Mbps maximális adatátviteli sebességet. 52 különböző frekvenciát használ 48-at az adatok továbbítására 4-et a szinkronizációra. A kódolási rendszer 18 Mbps–ig fázisbillentyűzésen, felette a QAM-en (Quadrature Amplitude modulation) alapul. Az 5GHz–es frekvenciasávot kevesebb eszköz használja, mint a 2,4GHz–et, így az interferencia lehetősége is jelentősen alacsonyabb. Amennyiben a vezeték nélküli hálózat működését lehetővé tevő közeg, a körülmények nem ideálisak, a rendszer 54 Mbps helyett kisebb (48, 36, 24, 18, 12, vagy 6 Mbps) átviteli sebességen működik.

IEEE 802.11b

1999. őszén szabványosították. Működési tartománya a 802.11a–tól eltérően, a 2,4GHz–es ISM frekvenciasáv. A 11 Mbps adatátviteli sebesség mellett az 5,5 Mbps, 2 Mbps és 1 Mbps sebesség is alkalmazható, ha az átviteli közeg állapota nem ideális. *DSSS (Direct Sequence Spread Spectrum*), azaz közvetlen sorrendű szórt spektrumú átvitelt alkalmaz. A frekvenciasávot 5 MHz vagy 25MHz–es csatornákra bontják. Az átvitt jelet egy bináris álvéletlen sztringgel (szórókód) modulálják. A bitek átvitelére Barker sorozatot alkalmaz. A CDMA egyik változatát, a *CCK (Complementary Code Keying)* modulációt használja.

IEEE 802.11g

A 802.11g szabvány a 2003-as évben került bevezetésre. A 2,4 GHz-es sávban biztosít maximálisan 54 Mbps adatsebességet, valamint visszafelé kompatibilis a 802.11b szabványú eszközökkel. 802.11b–vel való kompatibilis működés esetén 11 Mbps maximális adatátviteli sebességen, DSSS-t használva működik. Ettől eltérően („normális" működés esetén) *OFDM* modulációs technikát alkalmaz. A kompatibilitás a 802.11b szabványt támogató eszközök nagy száma miatt szükséges, így a már kiépített hozzáférési pontokhoz az új, *802.11g* szabványt támogató eszközök is képesek csatlakozni, ekkor viszont az átviteli sebességük maximuma értelemszerűen a szűkebb keresztmetszetű (*802.11b* szabványú) hozzáférési pont maximális sebessége lesz. A *802.11g* szabványt támogató hozzáférési pontok képesek visszafelé kompatibilisan működni, így ezekhez is csatlakozhatnak a már meglévő (*802.11b* szabványú) adaptert használó kliensek is. Természetesen a működési kompatibilitásnak „hátránya" is van, mégpedig, hogy a régi eszközök nem lesznek képesek nagyobb sebességre, még ha az eszközök saját belső szoftverét (*firmware*) le is cserélnék. Előnye viszont, hogy a korszerűsítés, a nagyobb bitsebesség elérését biztosító eszközökre való átállás zökkenőmentesen, fokozatosan elvégezhető.

A *802.11b* és *802.11g* közötti kompatibilitást tehát a szabványok biztosítják. Ennél lényegesen nagyobb problémát jelent a *802.11a* és a *802.11b* közötti átállás. A vezeték nélküli alszabványok közötti kompatibilitás hiányát a gyártók próbálják pótolni, azáltal, hogy a napjainkban forgalomban lévő eszközök gyakran mindhárom szabványt egyidejűleg támogatják.

2.2 További IEEE 802.11x alszabványok

802.11e

Egy olyan új, elosztott közeghozzáférési eljáráson alapul, mely képes kezelni különböző forgalmi osztályokat. Két metódust definiál, ezek az *EDCF (Enhanced Distribution Coordination Function)* és a *HCF (Hybrid Coordination Function)*. A vezetéknélküli szolgáltatás minőségére vonatkozó alszabvány. (A *QoS–t , CoS–t* biztosítja).

802.11f

A hozzáférési pontok (Acces Point) közötti protokoll *IAPP (Inter Access Point Protocol)* ajánlásait tartalmazza. Az IAPP lehetővé teszi, hogy különböző gyártók eszközei (AP) együttműködjenek.

802.11h

Az 802.11a kikerülésére tervezett alszabvány. A MAC réteget egészíti ki, hogy az európai előírásoknak (pl.: sugárzási teljesítmény vezérlés – *Transmission Power Controll, TPC*) megfeleljenek. Az 5 GHz frekvencián lehetőséget biztosít olyan eszközök használatára, amelyek észlelik a többi, ugyanezen a frekvencián üzemelő berendezést, például radart, és képesek a kisugárzási teljesítmény csökkentésére, valamint az üzemi frekvencia elhangolására (dinamikus frekvenciaválasztás – *Dynamic Frequency Selection, DFS*).

802.11i

2004 nyarán fogadták el, ami nem külön kommunikációs vagy fizikai réteget határoz meg, hanem biztonsági előírásokat tartalmaz. Célja, hogy bevezetésével eltűnjenek a korábbi biztonsági hiányosságok. Adattitkosításra az *AES–t (Advanced Encryprtion Standard)* használja. Biztonsági szempontból előírja továbbá a *WPA (Wi-Fi Protected Access)* protokoll használatát.

802.11n

A *MIMO (Multiple Input / Multiple Output)* technológián alapul és 540 Mbps–os maximális adatátviteli sebességre képes. Két vagy több, egymást nem zavaró rádiócsatornát használ egyidejűleg a maximális sávszélesség eléréséhez. A 2,4GHz-es ISM sáv a működési tartománya.

802.11s

Egy olyan hálózat alapjait készíti elő, melynek tagjai egyfajta hozzáférési pontként is működhetnek, így képesek lehetnének automatikusan route-olni az adatcsomagokat, ezáltal jelentősen kiterjesztenék egy vezeték nélküli hálózat lefedettségi területét.

802.11w

Jelentősen megnövelné módosításaival a vezeték nélküli hálózatok biztonságát. A MAC rétegen elvégzett módosításokkal, titkosítással a jelenlegi 802.11i szabványnál is erőteljesebb védelmet biztosítanának.

2.3 Közeghozzáférés (MAC) és ütközéskezelés

A 802.11 szabvány szerint kétféle működési mód létezik:

- DCF (Distributed Coordination Function) Elosztott koordinációs funkció
- PCF (Point Coordination Function) Pont koordinációs funkció

Az alapvető 802.11 szabvány MAC protokollja a DCF. Elosztott rendszerben működik, nincs központi vezérlés (ebben az Ethernetre hasonlít). CSMA/CA protokollt használ. A vezeték nélküli állomások versengnek a csatornáért. Fizikai és virtuális csatornaérzékelést is alkalmaznak. A PCF rendszerben van egy bázis állomás, ami mindent vezérel. A PCF csak opcionális, szabvány szerint nem kötelező.

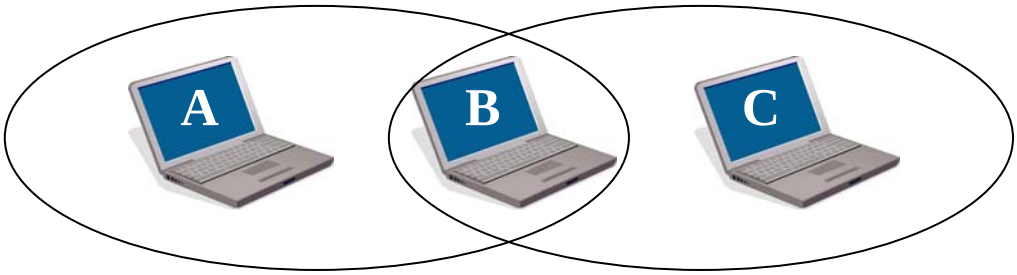
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence)

Ha a vezeték nélküli állomás adni kíván, akkor előbb belehallgat a csatornába, hogy folyik-e épp kommunikáció. Miután meggyőződött róla, hogy nincs másik adatátvitel folyamatban, megkezdi az adást. Csomagütközés ezesetben is lehet (pl.: rejtett állomás problémája). Az ütközés elkerülő mechanizmus úgy működik, hogy ha a csatorna szabadnak bizonyul, még akkor is vár az adó egy kis ideig. A várakozási idő egy minimális időtartamból és egy véletlen visszatartási időből *RBT (Random Backoff Time)* tevődik össze. A minimális időtartam az az idő, amíg a csatornának szabadnak kell lennie, ez a DIFS *(DCF Interframe Space)*. Ha ezalatt az időtartam alatt még mindig szabad a csatorna, akkor megkezdheti az adást az állomás. Az adó ekkor küld egy *RTS (Request To Send)* keretet, mellyel lefoglalja a csatornát, valamint a lefoglalás időtartamát (teljes átvitel- és nyugtázás időtartama) is átküldi. A vevő a *CTS (Clear To Send)* keret visszaküldésével nyugtázza az igényt.

Minden sikeresen vett keret esetén a vevő egy SIFS (Short Inter Frame Space) idő után küld egy ACK (Acknowledge) keretet, nyugtázva ezzel a hibátlan vételt (pozitív nyugtázás). Ha az ACK nem érkezik meg, az adó újraküldi a keretet. Ha a backoff periódusban ismét foglalttá válna a csatorna, akkor a backoff érték nem nullázódik, hanem a következő adási lehetőségnél folytatja a visszaszámlálást.

Szintén az ütközések elkerülése miatt a hosszú keretek fragmentálva, egyedi nyugtázással továbbítódnak. Ez azért is előnyös, mert ha valamelyik keret nem érkezik meg, akkor csak azt kell újra küldeni. Hátránya viszont, hogy a keretek szerkezete miatt sok kontroll byte kerül továbbításra, ami az adatátvitel hatékonyságot rontja.

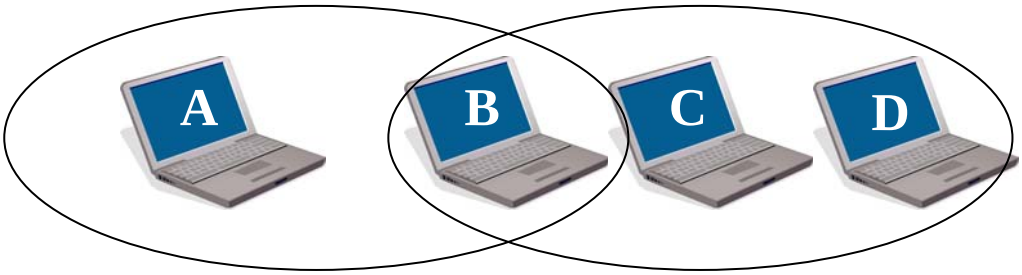
Rejtett állomás problémája (Hidden terminal)



A problémát az jelenti, hogy egy adott pillanatban az „A” és a „C” állomás egyszerre érzékeli szabadnak a csatornát, így mindketten elkezdenek forgalmazni, így a „B” állomás az interferencia miatt nem tudja venni az üzeneteket.

A rejtett állomás probléma hatásainak csökkentésére az IEEE 802.11-ben definiálták az RTS/CTS mechanizmust.

Felfedett Állomás problémája (Exposed terminal)



A probléma akkor merül fel, ha a „B” állomás akar forgalmazni az „A” számára, míg a „C” a „D” számára. Amikor a „B” elküldi az adatcsomagot, a „C” foglaltnak érzékeli a csatornát, így szükségtelenül visszafogja a „D”-nek szánt adását. Itt tehát nem az interferencia jelenti a problémát, hanem a nem elég hatékony csatorna-kihasználás.

Ebben az esetben is megoldásra vezet az RTS/CTS üzenetek alkalmazása. Mivel a „C” mobil állomás hallja a „B” által kiadott RTS üzenetet, tudja, hogy a következő csomag nem neki fog szólni, így folytathatja az adását a „D” állomásnak, amikor szabadnak érzékeli a csatornát.

3. A WLAN biztonsága

Alapvető követelmény hálózatba szervezett számítógépek esetén annak a biztosítása, hogy a csomópontok csak a nekik (is) címzett csomagokat dolgozhassák fel. Vezeték nélküli hálózatok esetén a hálózat elérése csupán a jelerősségtől, majd az ezt követő esetleges hitelesítéstől (authentikációtól) függ. A vezeték nélküli hálózat hatósugara a jelerősség erősítésével (külső antennákkal) növelhető. A vezeték nélküli hálózat adatforgalmát biztonsági szempontból a következő képpen lehet csoportosítani:

- titkosítatlan
- titkosított

A csoportosítás egyrészt utal az authentikáció szükségességére, másrészt a vezeték nélküli hálózatokon terjedő csomagok közvetítésének módjára. A vezeték nélküli hálózatok biztonsági szintjének megfelelően többféle authentikáció létezik.

A titkosítatlan hálózatok egyik speciális változatának tekinthető a HOT SPOT, amin keresztül egyre több publikus helyen (repülőtereken, éttermekben, kávézókban, stb.) férhetünk hozzá meghatározott összeg ellenében az Internethez. Ez a fajta kapcsolat (a díjfizetés miatt) időben erősen korlátozott, valamint biztonsági szempontból is hagy némi kívánni valót maga után. A titkosítatlan hálózatokat bárki szinte korlátozás nélkül elérheti, így a felkészületlen felhasználó könnyen áldozatává válhat valamiféle nem kívánatos adatmegosztásnak.

A titkosítatlan vezeték nélküli hálózatok általában a hitelesítést sem követelik meg, illetve *nyíltrendszer hitelesítést* (*Open System Authentication*) alkalmaznak, ami nem kifejezetten hitelesítés, csupán MAC alapján azonosít. Az AP minden csatlakozási kérést elfogad, így a hálózathoz bárki tud csatlakozni, ha hatótávolságon belül tartózkodik. Ezt követően a hálózat teljes mértékben elérhető számára, a csomagok titkosítatlanul terjednek, azokat a hálózathoz csatlakozva bárki láthatja.

A nyíltrendszer hitelesítés mellé a *MAC szűrést* is szokták alkalmazni, ami azt jelenti, hogy a hozzáférési pontok csak a korábban manuálisan megadott MAC című adapterrel rendelkező számítógépek számára engedélyezik a csatlakozást a hálózathoz. Ez azonban még mindig nem elegendő hitelesítés, ugyanis a MAC cím is manipulálható, valamint az adatok titkosított továbbítása továbbra sem biztosított. Nagyobb hálózatok esetén a MAC szűrés nem célszerű a nehézkes manuális karbantartás miatt.

A hitelesítés történhet egy titkos kulccsal (jelszóval) is. Az osztott kulcsú hitelesítés (*Pre Shared Key authentication*) használatakor a hozzáférési pont ellenőrzi, hogy a csatlakozni szándékozó kliens rendelkezik-e a megfelelő titkos kulccsal. A kulcsok kiosztását a szabványok nem szabályozzák, ezért általában a könnyebb konfigurálhatóság érdekében közös kulcsot alkalmaznak. Osztott kulcsú hitelesítést alkalmaz a WEP is.

A tikosított hálózatokhoz való csatlakozás mindig authentikációhoz van kötve. A hitelesítést követően a kommunikáció során a csomagok különböző kriptográfiai algoritmus segítségével titkosítva továbbítódnak. A titkosítási protokoll és az authentikáció szorosan összefügg. Az eredeti 802.11 szabványban meghatározott biztonsági előírások több oldalról is sebezhetőnek bizonyultak, így a biztonság fokozása érdekében a *802.11i* szabvány már megbízhatóbb technikákat követel meg a vezeték nélküli hálózatoktól. Ezeket alkalmazza a WPA.

A vezeték nélküli hálózatok biztonsági kérdéseivel a felhasználók nagy többsége a figyelmeztetések ellenére még a mai napig mindig nem foglalkozik. Gyakran hiányos számítástechnikai ismereteik következtében nem gondoskodnak az általuk kialakított vezeték nélküli hálózatok védelméről. A titkosítatlan, authentikációt nem igénylő hálózatok nem biztonságosak, azt bárki igénybe veheti. A rosszul, vagy egyáltalán nem biztosított hálózatok „üzemeltetői” nem csupán ingyenes (Internet) szolgáltatást biztosítanak, hanem saját számítógépük megosztott erőforrásait is tálcán kínálják fel a hálózat hatótávolságán belüli vezeték nélküli eszközöknek.

A védtelen vezeték nélküli hálózatok növekvő számának következtében egyre elterjedtebb jelenség az ún. WarDriving, vagyis amikor egy-egy települést nyílt, gyengén védett vezeték nélküli hálózatok szempontjából feltérképeznek. A feltérképezést követően sajnos, ezen sebezhető hálózatokról begyűjtött információkat az Interneten a nagyközönség számára is elérhetővé teszik. Ehhez mindössze egy vezeték nélküli adapterrel szerelt mobil eszköz (notebook, PDA, stb.), egy nagyobb hatótávolságú antenna és néhány program szükséges. „Térképészünk" elszántságától függően még egy GPS navigációs rendszer is szükséges lehet, hogy koordináta-pontosan határozza meg a sebezhető hálózatokat. Ezek mindegyike könnyedén beszerezhető az Internet segítségével is.

A vezeték nélküli hálózathoz való hozzáférést célszerű tehát szabályozni. Erre a napjainkban forgalomban lévő eszközök általában többféle lehetőséget is biztosítanak. Az AP eléréséhez szükséges adatok az *SSID (Service Set Identifier)* és egy jelszó párosa, valamint adott esetben (távoli konfigurálás esetén) szükség lehet még az AP MAC és IP címeire. A gyártók az eszközökben az SSID és jelszó párost egy alapértelmezett értékre állítják be, amit a felhasználók nagy többsége nem változtat meg, így a hálózathoz minden különösebb erőfeszítés nélkül hozzáférhet egy kevésbé szakavatott illetéktelen felhasználó is.

Az AP elérését kell tehát elsőnek biztosítani, hogy az illetéktelen felhasználók ne tudjanak csatlakozni hozzá. Ehhez célszerű az SSID-t és a jelszót megváltoztatni, illetve az SSID Broadcast–ot kikapcsolni. (A felhasználók jelszóhasználati szokásainak „elemzésétől" most eltekintve, feltételezzük, hogy előbb–utóbb megtanulják gondosan megválasztani és használni jelszavaikat.) A hozzáférési pontok többségét távolról is lehet konfigurálni, ami további figyelmet érdemel biztonsági szempontból. Biztosítani kell itt is, hogy csak az illetékes felhasználók tudják távolról konfigurálni a hozzáférési pontot.

A hozzáférési pont biztosítása fontos, hisz a vezeték nélküli hálózathoz való hozzáférést ez kontrollálja. Hiábavaló akármilyen authentikáció és titkosítás, ha a hozzáférési pont nincs biztosítva. Ha valaki illetéktelenül hozzáfér az AP–hez, akkor tudja azt úgy konfigurálni, hogy a továbbiakban már „jogosultan", akár észrevétlenül használja a hálózatot.

A hálózat védelmét fixen kiosztott IP címekkel is biztosítani lehet, ez viszont a rugalmasság kárára történik. Ezzel a vezeték nélküli hálózat egyik előnyét veszítené el, hiszen a vezeték nélküli hálózatok esetén gyakran más és más mobil eszközök csatlakoznak a hozzáférési ponthoz, amiket fix IP esetén manuálisan kellene kezelni, engedélyezni. A *DHCP* (*Dynamic Host Configuration Protocol*) engedélyezésével, automatikusan osztott IP címek esetén viszont a hálózat védelme teljes mértékben a hitelesítésre hárul. A vezeték nélküli hálózatok hozzáférési pontjai végzik a csatlakozni szándékozó állomások hitelesítését.

A vezeték nélküli hálózatok esetén több authentikációt és adattitkosítást megvalósító technika is létezik. Ezek többnyire a hitelesítésen, a hálózati forgalom titkosításán túlmenően az adatintegritás megőrzését is megvalósítják egyúttal. Ezen lehetőségek a következők:

- WEP
- WPA
- WPA2

3.1 WEP

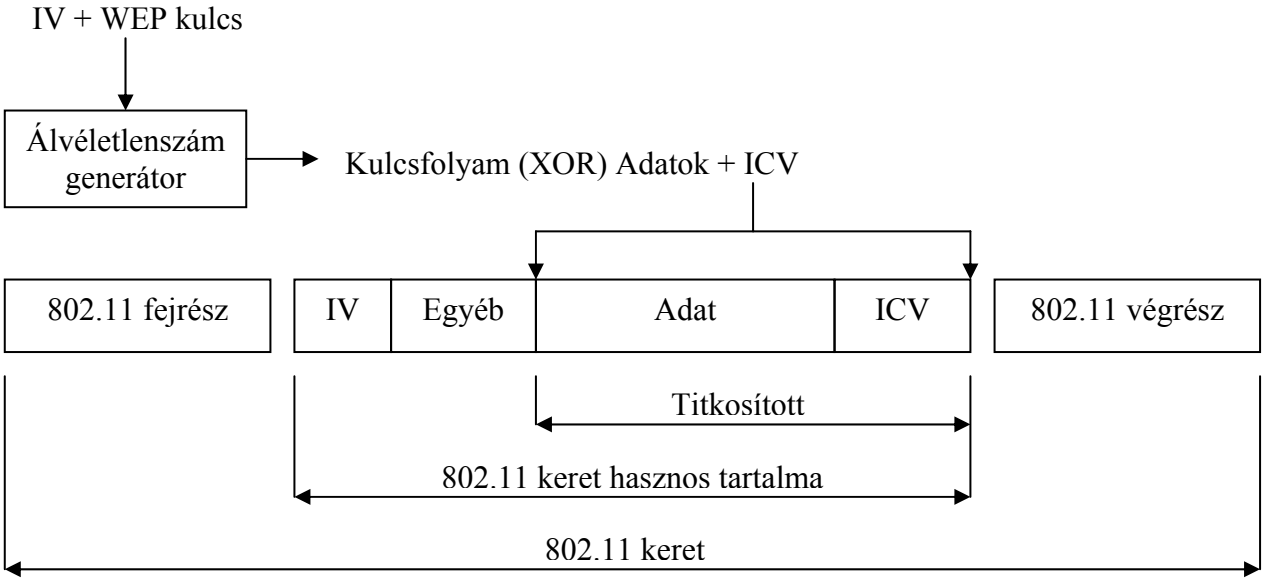
A *WEP (Wired Equivalent Privacy)*, magyarul a Vezetékessel Egyenértékű Titkosítás a kezdeti WiFi szabványok biztonsági technológiája. A WEP-et eredetileg a vezeték nélküli kapcsolatok titkosítására találták ki, a helyi hálózatokkal megegyező biztonsági szintet vártak tőle. A vezeték nélküli állomások authentikációjára és az általuk forgalmazott csomagok titkosítására szolgál. Az Ethernet esetén a csomagok titkosítatlanul közlekednek, így azokat a hálózathoz csatlakozott számítógépek mindegyike láthatja. Ez is jelent ugyan biztonsági kockázatot, de ehhez legalább a hálózat közvetlen közelében kell lenni. A WEP adatintegritás ellenőrzést is biztosít, a nyílt szövegből számol egy ellenőrző összeget, majd ezt a nyílt szöveggel együtt titkosítja és továbbítja. A WEP alapötlete jó volt, később látni fogjuk azonban, hogy több helyen is sebezhetőnek bizonyult.

WEP esetén biztonsági szempontból az első és legfontosabb a megfelelő authentikáció. Ezt a hálózat résztvevői között előre kiosztott, közös titkos kulcs biztosítja. A közös kulcs használata további biztonsági kérdéseket vet fel, valamint a kulcsok kiosztásának módjára sincs előírás a WEP–ben. Szimmetrikus 64 illetve 128 bites, változó hosszúságú kulcsot használ. A gyártók próbálkoztak 256 bites változattal is, de mivel ez nem volt szabvány a kompatibilitás nem volt biztosított. A 64 bitből 40 bit a titkosító kulcs, ezért gyakran csak 40-bites kulcsként emlegetik (a 128 bites változatnál 104 bites a kulcs). A titkos kulcs használatával próbálják a vezeték nélküli kliensek magukat hitelesíteni a hozzáférési pontoknál, ennek hiányában nem tudnak csatlakozni a hálózathoz. Hitelesítéskor a kliens egy *Request* üzenetet küld, amire a hozzáférési pont egy *Challenge* üzenetet visszaküld, majd ezt az üzenetet a titkos kulccsal titkosítva a kliens *Response* üzenetben küldi vissza. Az AP a titkos kulcs alapján dekódol, és ha az így kapott üzenet egyezik az eredetivel, akkor engedélyezi a csatlakozást.

A sikeres authentikációt követően, a WEP az adatok „biztonságos” továbbítását hivatott ellátni. Nem csupán az adatok titkosítását, hanem a csomagok sértetlen megérkezését is „garantálja”. A 802.11 keretek fejrészében található egy mező, ami jelzi, hogy a csomagok WEP-el titkosítva vannak-e. Az RSA által kifejlesztett RC4 folyamkód titkosítást használ – aminek mára már ismertek a hiányosságai.

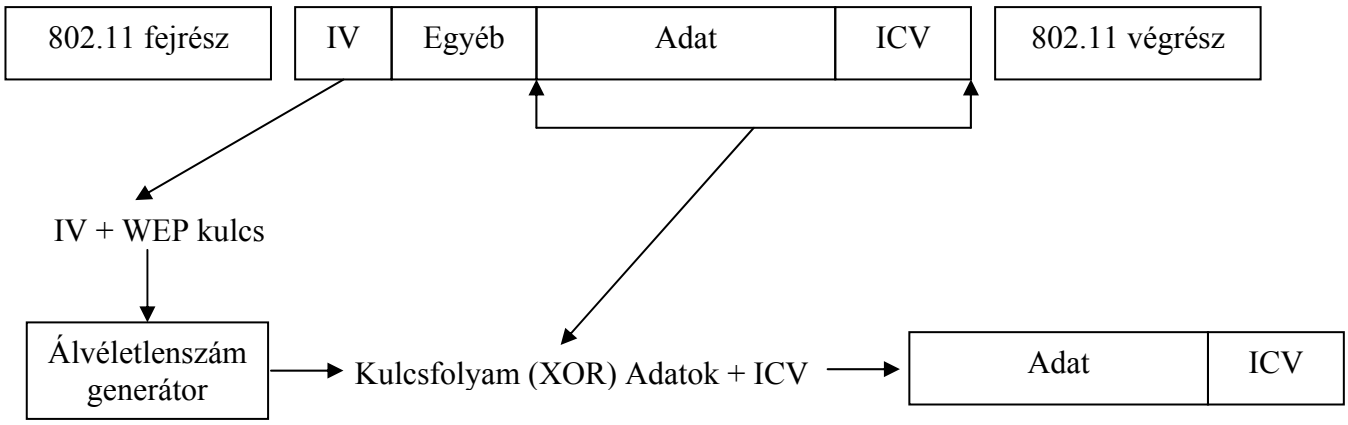
A titkosítás

1. A nyílt szöveghez egy 32 bites ellenőrző részt (*ICV- Integrity Check Value*) kalkulál, ezzel ellenőrizhető a csomag integritása.
2. Az ellenőrző részt a szöveghez fűzi ([adat + ICV]).
3. A kódoló inicializálásához egy 24 bites *IV (Initialization Vector)* kezdővektort hozzácsatol a WEP titkosító kulcshoz.
4. Az IV-ből és a WEP titkosító kulcsból egy álvéletlenszám generátor létrehoz egy olyan bitsorozatot (*kulcsfolyam*), ami méretre megegyezik az [adat + ICV] folyam méretével.
5. A kulcsfolyamot bitenkénti *KIZÁRÓ VAGY (XOR)* művelettel hozzákeveri az [adat + ICV] bitsorozathoz, így áll elő a titkosított folyam.
6. A titkosított bitsorozatot átvitelekor a MAC keret tartalmazza az IV-t is.



A visszafejtés

1. Az érkezett csomag dekódolása az IV leválasztásával kezdődik.
2. Az IV-t hozzáfűzi a (közös) WEP titkosító kulcshoz.
3. Az IV és a WEP segítségével előállítja a kulcsfolyamot. Az álvéletlenszám generátornak köszönhetően ez a kulcsfolyam azonos lesz a küldő kulcsfolyamával.
4. A kulcsfolyam és a titkosított szöveg logikai összeadásával dekódol.
5. Az ellenőrző összeg újraszámolódik, majd összehasonlításra kerül a fogadott, előzőleg dekódolt ellenőrző összeggel. Ha egyeznek, akkor a csomag módosítás nélkül, sértetlenül megérkezett. Amennyiben nem minősíthető érvényesnek a csomag, eldobja a rendszer.



A WEP sebezhetősége

A WEP bevezetését követő években egyre több hiányosság derült ki, melyeket publikálva rövid idő alatt megbízhatatlanná vált biztonsági szempontból. Minden WEP-el biztosított hálózat „feltörhető”, ezért napjainkban már senki sem ajánlja a használatát. A 64 bites WEP kulcsszó visszafejtése a mai számítógépek segítségével alig néhány perc, pár ezer adatcsomag vizsgálata elegendő hozzá. Mára már különösebb szakértelmet sem igényel, hiszen számos (Internetről letölthető) szoftver van, ami teljesen automatikusan működik és alkalmas a WEP kulcsok megfejtésére (AirSnort, WEPCrack).

A WEP több oldalról is támadható. A legalapvetőbb probléma az osztott kulcsok alkalmazásából adódik, illetve, hogy az eredeti szabvány a kulcsok kezelésére vonatkozó előírásokat nem tartalmaz. A kulcsok kiosztásának módjára és érvényességi idejükre vonatkozóan sincs ajánlás. A kulcskezelés egyik legnagyobb hátránya, hogy a könnyebb karbantartás érdekében a kliensek ugyanazzal a közös titkos kulccsal hitelesítik magukat a hozzáférési pontnál, és ugyanezzel a kulccsal titkosítják a hálózat forgalmát. Mivel a kulcs kiosztásának menete nem szabályzott, ezért a lehetőség, hogy a kulcs illetéktelen kezekbe kerül viszonylag nagy. (Itt még csak a közös kulcs gondatlan használatára gondolok és nem pedig a működési elv hiányosságaiból adódó egyszerű visszafejtésére.) A kulcs érvényességének időtartama a másik fontos kérdés. Ha ritkán cserélik a kulcsot, azzal szintén növelik az esélyt, hogy illetéktelen felhasználók is megszerezhessék. Nagyobb kiterjedésű hálózatok esetén a kulcsok kiosztása is problémás lehet, így azok gyakori cseréjére valamiféle automatizált eljárást kellene alkalmazni.

A WEP titkos kulcs hátránya továbbá, hogy ez egy karaktersorozat. Gyakran az sem követelmény, hogy a kulcsot csak HEXA karakterek alkossák, így az ASCII karakterek kínálta lehetőséggel élve sokan egyszerű, beszédes, gyenge WEP kulcsokat alkalmaznak. (Vannak akik a HEXA karakterek felhasználásával is szavakat próbálnak titkos kulcsként beállítani, pl.: C0DE). A 128 bites WEP változatnál is csak 104 bit a kulcs, ami 26 db hexadecimális karaktert jelent. Egyes gyártók 256 bites eszközöket is forgalmaznak, aminél már 58 HEXA karakter a titkos kulcs.

A WEP legnagyobb hiányossága azonban a vezeték nélküli hálózaton titkosítatlanul is küldözgetett IV kezdővektor. Az átlagos IV méretéből (24 bit) adódóan meg van az esély arra, hogy bár üzenetenként más és más IV-t kap egy keret, de előbb – utóbb ismétlődni fog. Magasabb adatátviteli sebesség esetén kevesebb idő eltelte után fog ismét használatba kerülni ugyanaz a kezdővektor, vagyis gyorsabban visszafejthető a kulcs. A problémát az jelenti, hogy a kezdővektor titkosítatlanul is átkerül a vevő oldalra, így a kulcsfolyamból (IV + WEP kulcs) az adatforgalom monitorozásával (*sniffering*) különösebb erőfeszítések nélkül visszafejthető a titkos kulcs. A titkosítási eljárás működési elvének köszönhetően a kulcs méretének növelésével nem feltétlenül lesz nagyobb biztonságban a hálózatunk.

A WEP sebezhető pontjai közé sorolható az adatintegritást biztosító funkció is. Az alkalmazott módszerről ugyanis belátták, hogy az adatok módosítása mellett az ellenőrző összeg is manipulálható oly módon, hogy a vevő oldalon sértetlen, módosítatlan üzenetnek tűnjön.

A vezeték nélküli hálózatokat alkotó eszközök mindegyike támogatja a WEP-et, viszont a régebbiek csak ezt támogatják. Amennyiben a hálózati eszköz frissítése, cseréje valamiért nem megoldható, és ennek következtében mindenképpen WEP-et kell használni, akkor érdemes a lehető legmagasabb biztonsági szintet kihozni belőle. 128 bites WEP kulcsokat alkalmazva, azok gyakori (akár óránkénti) cseréjével a hálózat biztonsága kis mértékben fokozható ugyan, de soha nem lesz feltörhetetlen.

A WEP gyengeségeit próbálták különböző fejlesztésekkel kijavítani, de mivel az alapvető hiányosságok megmaradtak, így csak kis mértékben tudták növelni a biztonságot. Ráadásul a különböző gyártók fejlesztései nem voltak kompatibilisek, ezért nem tudtak a tovább fejlesztett változatokat támogató eszközök elterjedni.

A WEP talán leggyengébb pontja az IV vektor. A fejlesztések során a kezdővektor mérete és annak ismétlődése miatti gyengeséget próbálták kiküszöbölni, de ezzel többnyire csak időt nyertek. A WEP-nek két tovább fejlesztett változata van a *WEP2* és a *WEP+*.

WEP 2

A WEP továbbfejlesztése, a vezeték nélküli eszközök csak egy része támogatja. Az IV vektor méretét növelték meg benne (128 bit) és hatékonyabb 128 bites titkosítást alkalmaz. Az IV ismétlődést azonban nem tudták kiküszöbölni, így ez is feltörhető, csupán kissé lelassítja az illetéktelen csatlakozást.

WEP Plus (*WEP+*)

Az IV vektor gyengeségeinek elkerülésére tett kísérletek következtében jött létre a WEP+ változat, ami viszont csak akkor hatásos, ha a vezeték nélküli kommunikációban résztvevő mindkét fél ezt alkalmazza. Ez nem jelentett volna különösebb problémát egy új hálózat létesítésekor. A meglévő hálózatok viszont nem feltétlen tudtak volna együttműködni, vagy csak a standard WEP protokoll alkalmazását tették volna lehetővé.

A használatban levő csak WEP képes vezeték nélküli eszközök száma még mindig jelentős, ezek saját belső szoftverének (*firmware*), illesztőprogramjának frissítése, hogy az újabb protokollokat is támogassa, általában lehetséges.

A WEP protokoll napjainkban már nem nyújt elegendő védelmet, ezért egyértelmű igény merült fel egy újabb, megbízhatóbb protokoll kifejlesztése iránt. Egy olyan protokoll, ami biztonságosabb authentikációt, hatékonyabb kriptográfiai technikákat alkalmaz, ami leválthatja a WEP-et.

3.2 WPA

A WEP-et támogató eszközökkel működő vezeték nélküli hálózatok lehetőségei korlátozottak. Nem várható el, hogy az éppen modernizált hálózatokat, hálózati eszközöket a WEP biztonsági hiányosságai miatt ki kelljen cserélni, ezért olyan protokollra volt szükség, amit a meglevő eszközök képesek adaptálni, és biztonságosabb, mint a WEP. A WEP különböző javított, tovább fejlesztett változatai mellett új protokoll kifejlesztésén is dolgoztak a gyártók. 2003-ra elkészült egy olyan protokoll, ami a WEP leváltására alkalmas. A *WPA* (*Wi-Fi Protected Access*), magyarul Védett Wi-Fi Elérés a 802.11i biztonsági szabvány része, már a szabvány elfogadása előtt ajánlották alkalmazását, de csak átmeneti megoldásnak szánták. A WPA tervezésekor a teljes kompatibilitás megvalósítása volt a cél, azaz, hogy a WEP-el lefele a tervezett WPA2-vel felfele legyen kompatibilis a protokoll.

A vezeték nélküli hozzáférési pontok firmware-ük frissítését követően adaptálni tudják a WPA technológiát. A WEP-ről WPA-ra való átállás megkönnyítése végett a gyártók az AP-k firmware-ét úgy módosították, hogy azok képesek legyenek vegyes működésre is, így az átállás fokozatosan is kivitelezhető volt. Vegyes működés alkalmazásakor a hozzáférési pont egyidejűleg képes kezelni a WEP és a WPA klienseket. A vegyes környezet egyetlen hátránya, hogy a WPA ügyfelek számára sem lesz megvalósítható a dinamikus kulcskezelés, viszont minden más további biztonsági megoldást alkalmazni tudnak.

A WPA (csakúgy, mint a WEP) a vezeték nélküli hálózatok teljes biztonságát hivatott ellátni, az authentikációt, a titkosított adatátvitelt és az átvitt adatok integritásának megőrzését. A vezetékes hálózatoknál is alkalmazott 802.1x hitelesítést, tovább fejlesztett titkosítási és adatintegritás ellenőrző algoritmusokat használ. A WEP 40 bites statikus kulcsa helyett 128 bites dinamikus kulcskezelést alkalmaz. A WPA-nak a hálózat méretétől, a biztonsági szint mértékétől és a felhasználók típusától függően két változata van:

- Enterprise
- Personal

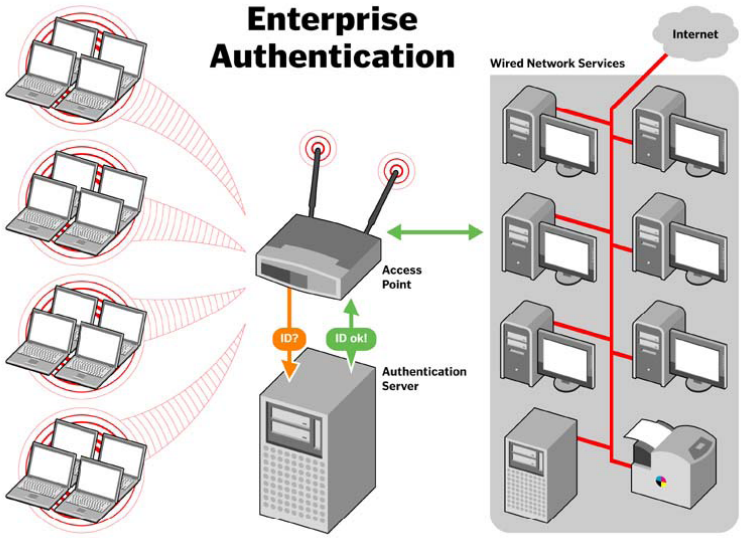
A WPA a nagyvállalatok számára az *Enterprise* változatot ajánlja, ami a *RADIUS* (*Remote Authentication Dial-in User Service*) és az *EAP* (*Extensible Authentication Protocol*) hitelesítéseket egyaránt képes alkalmazni. A RADIUS infrastruktúrával ellátott hálózatok esetén a hitelesítést egy központi hitelesítő kiszolgáló végzi.

Az EAP egy pont–pont protokoll (*PPP – Point to Point Protocol*) alapú hitelesítési mechanizmus. Jelenleg is számos változata van. A kapcsolat felépítésekor, a hitelesítési fázisban állapodnak meg a csatlakozó felek, hogy melyik EAP változatot használják.

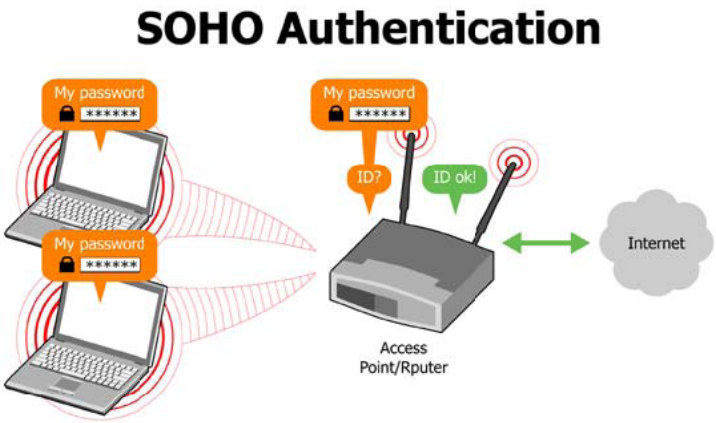
A legelterjedtebbek:

- EAP TLS (EAP Transport Layer Security)
- EAP TTLS / MSCHAPv2 (Tunneled TLS / Microsoft Challenge Authentication Handshake Protocol)
- PEAPv0 / EAP – MSCHAPv2 (Protected EAP)
- PEAPv1 / EAP – GTC
- LEAP (Lightweight EAP)
- EAP SIM

Az EAP-ot alkalmazó helyi hálózati protokollok az EAP üzeneteket beágyazzák saját kereteikbe, ez a 802.1x szabvány esetén az EAPoL (EAP over LAN).



A 802.1x hitelesítés alapján minden felhasználó saját kulcsot kap, bár osztott kulcsú üzemmódban is képes működni. Az osztott kulcsú üzemmódot az otthoni és kis vállalati hálózatok számára ajánlják (*SOHO - Small Office / Home Office*), akiknek nem lenne gazdaságos, és felesleges bonyodalmakkal járna egy RADIUS szerver üzemeltetése. A *WPA-PSK (Pre Shared Key)*, más néven a WPA *Personal* változata.



A kulcsok kiosztásáért és újrakódolásáért a *TKIP* (*Temporal Key Integrity Protocol*), vagyis Ideigleneskulcs Integritás Protokoll a felelős. A WPA kulcskezelése dinamikus, ennek megfelelően kulcs hierarchiát vezet be, és megkülönböztet két kulcsot. Az egyik kulcs a *címzett üzenet kulcs* (*session key*), és van egy globális, mindenki által használt kulcs *többes üzenet kulcs* (*global key*). Az egyszeres üzenetküldés titkos kulcsa keretenként változik, ezeket a változásokat a vezeték nélküli eszközök között szinkronizálni kell. A globális kulcs a hitelesítéshez szükséges, majd a sikeres authentikációt követően automatikusan új kulcsot generál a TKIP, amivel a kommunikáció megkezdődhet. A hitelesítéshez használt osztott kulcs megválasztásánál lehetőleg (mint ahogyan minden egyes jelszónál illene) kis– és nagy betűket, valamint számokat egyaránt tartalmazó, hosszú karaktersorozatot használjunk. A hálózaton folyó adatforgalom monitorozásával immáron nem lehet megfejteni a hitelesítéshez szükséges titkos kulcsot, mivel azt csak egyszer használják fel. A dinamikus (akár üzenetenkénti) kulcsváltással a támadónak nem lesz lehetősége az adatok lehallgatását követően a dekódolására, mert mire megfejti a titkos kulcsot, addigra már új kulccsal titkosít a TKIP.

Az adatfolyam titkosításra a WEP által is alkalmazott RC4 kódolást használja egy 128 bites kulccsal. Az inicializáló vektor (IV) mérete 48 bit. A kulcsok és az IV-k méretének növekedésével és egy biztonságosabb üzenet ellenőrzési rendszer hozzáadásával a WEP csaknem minden hiányossága ki van javítva.

Az adatintegritás ellenőrzésre a *Michael* módszert alkalmazza, ami 8 byte-os ellenőrző összeget kalkulál ez a *MIC* (*Message Integrity Check*).

A WPA a TKIP titkosítást írja elő, ezt a vezeték nélküli eszközök illesztőprogramjuk, vagy saját belső szoftverük frissítését követően képesek alkalmazni, viszont az *AES* (*Advanced Encryption Standard*) a fejlett titkosítási szabvány firmware frissítéssel sem biztos, hogy adaptálható, ezért az AES opcionális.

Az AES titkosításra képes eszközök egy számláló mechanizmust alkalmaznak (*CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), amely érzékeli a TKIP-törési kísérleteket, és ilyen esetben ideiglenesen blokkolja a kommunikációt a támadó gépével.

	WEP	**WPA**
Titkosító algoritmus	*RC4*	*RC4 / [AES]*
Titkos kulcs	*40 bit / 104 bit*	*128 bit*
Kezdővektor (IV)	*24 bit*	*48 bit*
Adatintegritás ellenőrző	*ICV (CRC)*	*MIC*
Kulcskezelés	*Statikus*	*Dinamikus (EAP)*

3.3 WPA2

A WPA tulajdonképpen még a 802.11i biztonsági szabvány véglegesítése előtt jött létre, utódja WPA2 néven már a 2004 őszén ratifikált 802.11i szabvány szerves részeként vált ismertté. A WPA2 már kötelezően tartalmazza az erősebb AES alapú CCMP titkosítási módszert is (gyakran ezt is csak AES-ként emlegetik), lecserélve a WPA első verziója által alkalmazott (gyengébb) RC4 titkosítási algoritmust, amit a WEP is használ.

Wi-Fi Protected Access 2 (Wi-Fi Védett hozzáférés 2-ik generáció). Ez a manapság egyre jobban terjedő titkosítási forma, biztonságos, de sajnos még kevés a támogatottsága, illetve kompatibilitási problémák is vannak. A legelterjedtebb operációs rendszerek 2005. májusa óta képesek az új, biztonságosabb protokoll használatára, 2006. tavaszától a gyártók minden eszköze támogatja, amik a WPA-val természetesen teljes mértékig kompatibilisek (lefele).

Az AES alapú CCMP a hitelesítés mellett az adatok titkosítását és az adatintegritás megőrzését is biztosítja. A WPA-hoz hasonlóan 128 bites dinamikus kulcsot alkalmaz az adatok titkosítására. Elődjéhez hasonlóan ennek is két változata van a *Personal* és az *Enterprise*.

A *WPA2 Personal* változatot a kisebb terjedelmű hálózatot üzemeltető kis vállalatoknak és otthoni felhasználásra szánják. A vezeték nélküli hozzáférési pontban be kell állítani az authentikációhoz szükséges „jelszót”, egy 8-63 byte hosszú karaktersorozat (*passphrase*). Az osztott kulcs (PSK), operációs rendszer szinten tárolódik, tehát csak egyszer kell beállítani a kliensek esetén is. Osztott kulcs esetén a vezeték nélküli hálózat biztonsága nagy mértékben függ a választott kulcs hosszától és bonyolultságától.

Csakúgy, mint a WPA-nál a (közös) titkos kulcsot csak az authentikációkor egyszer alkalmazzák, ezt követően új, automatikusan generált titkos kulcsokkal történik a kommunikáció titkosítása, így a támadónak nincs elég ideje az aktuálisan használatban levő kulcsok megfejtésére.

A *WPA2 Enterprise* változat a nagyvállalatok számára készült, AES titkosítást alkalmaz az authentikációt pedig egy hitelesítő kiszolgáló szerver látja el. A WPA és WPA2 által támogatott EAP típusok (EAP-TLS, EAP-TTLS/Mschapv2, Peapv0/Eap-mschapv2, Peapv1/EAP-GTC, EAP-SIM, EAP-LEAP) megegyeznek, így a kompatibilitás EAP hitelesítés esetén is biztosított. Természetesen az egyéb, céges rendszerek számára készített speciális 802.1x kliens és szerver Wi-Fi eszközök ezektől eltérő EAP típusokat is támogathatnak, azonban kompatibilitásukat ekkor már a szabvány nem garantálhatja.

A vezeték nélküli hálózatok elleni ismert támadási módszerek nagy többsége ellen már a WPA is kellő védelmet nyújt, viszont a WPA2 minden tekintetben komolyabb védelmet biztosít, elsősorban az AES alapú kriptográfiai algoritmusnak köszönhetően, így használata mindenképpen javasolt. WPA-ról WPA2-re való átállás esetén a gyártók biztosítják a hozzáférési pontok számára a vegyes módú működést, azaz egyidőben képesek mind a WPA-t, mindpedig a WPA2-t alkalmazó kliensek kiszolgálására. A vezeték nélküli eszközök cseréjét azonban ezúttal már nem feltétlenül lehet „megúszni”, hiszen azok egy egyszerű firmware frissítéssel sem biztos, hogy képesek az AES adaptálására.

	WPA	**WPA2**
Titkosító algoritmus	*RC4 / [AES]*	*AES*
Titkos kulcs	*128 bit*	*128 bit*
Kezdővektor (IV)	*48 bit*	*48 bit*
Adatintegritás ellenőrző	*MIC*	*CCMP*
Kulcskezelés	*Dinamikus (EAP)*	*Dinamikus (EAP)*

4. Összegzés

Az elmúlt években a vezeték nélküli hálózatok és a vezeték nélküli hálózati adapterrel ellátott számítógépek száma rohamosan nőtt. A vezeték nélküli technológia alkalmazása a felhasználók szemszögéből egy részről praktikus és kényelmes, másrészről viszont alkalmazása sok esetben elkerülhetetlen, a vezetékes hálózat kiépítése nem lehetséges. A gyártók az egyre magasabb igényeknek megfelelően nagyobb és nagyobb adatátviteli sebességre képes technológiákat fejlesztenek ki, és valósítják meg eszközeikben, amiknek a mai világ biztonsági normáinak is eleget kell tenniük. A nagyobb hálózatok esetén megengedhetetlen, hogy a vezeték nélküli számítógépes hálózatuk bármilyen szempontból is sebezhető legyen. (Gondoljunk itt az államtitkok, vagy a nagyvállalatok esetén az üzleti titkok megszerzésére, stb.)

Nem lehet eleget hangsúlyozni, hogy a veszély a kis vállalatokat és az otthoni hálózatokat is fenyegeti. A kisebb vezeték nélküli hálózatok védelmének kérdését is komolyan kell venni. A WarDriving kifejezés a védtelen, vagy könnyen sebezhető vezeték nélküli hálózatok lokalizálását, a hálózat illetéktelen felhasználását jelenti. Terjedése bizonyítja, hogy a felhasználók a folyamatos figyelmeztetések ellenére sem foglalkoznak az üzemeltetett vezeték nélküli hálózatok védelmének megfelelő biztosításával.

Az illetéktelen hálózat használat kifejezés alatt az otthoni felhasználók általában az általuk előfizetett és mások által (is) használt Internet elérésre gondolnak, gyakran ezért sem fordítanak különösebb figyelmet hálózatuk védelmére. Ennél azért jóval többről van szó. Senki sem örülne neki, ha a titkosítatlan adatforgalomnak köszönhetően a nevében e-mail-eket küldözgetne valaki, vagy akár személyazonosságával komolyabban visszaélne. Ha az illetéktelen felhasználó esetleges szabálysértéseket, bűncselekményeket követ el védtelen hálózat használatával, az üzemeltetőnek igencsak sok kellemetlenséget tud okozni, mert a megfelelő szervek képesek (és joguk van) a hálózat azonosítására és a hálózati forgalom monitorozására.

A vezeték nélküli hálózatok megfelelő védelmének biztosítása tehát minden tekintetben saját érdekünk.

A vezeték nélküli hálózat tervezésekor meg kell ismernünk a vásárolandó eszközök tulajdonságait. Nem csupán az adatátviteli sebességet kell szem előtt tartani, hanem azt is, hogy az eszközök mely biztonsági protokollokat támogatják. A napjainkban forgalomban levő eszközök mindegyike támogatja a WEP, a WPA és nagy többségük a WPA2 protokollokat is. Nem elég csupán a magasabb biztonsági szintet megvalósítani képes eszközöket megvásárolni, ezeket megfelelően konfigurálni is kell. A gyártók által forgalmazott eszközök ugyanis alapértelmezés szerint nyílt hálózati beállításokkal kerülnek a boltokba.

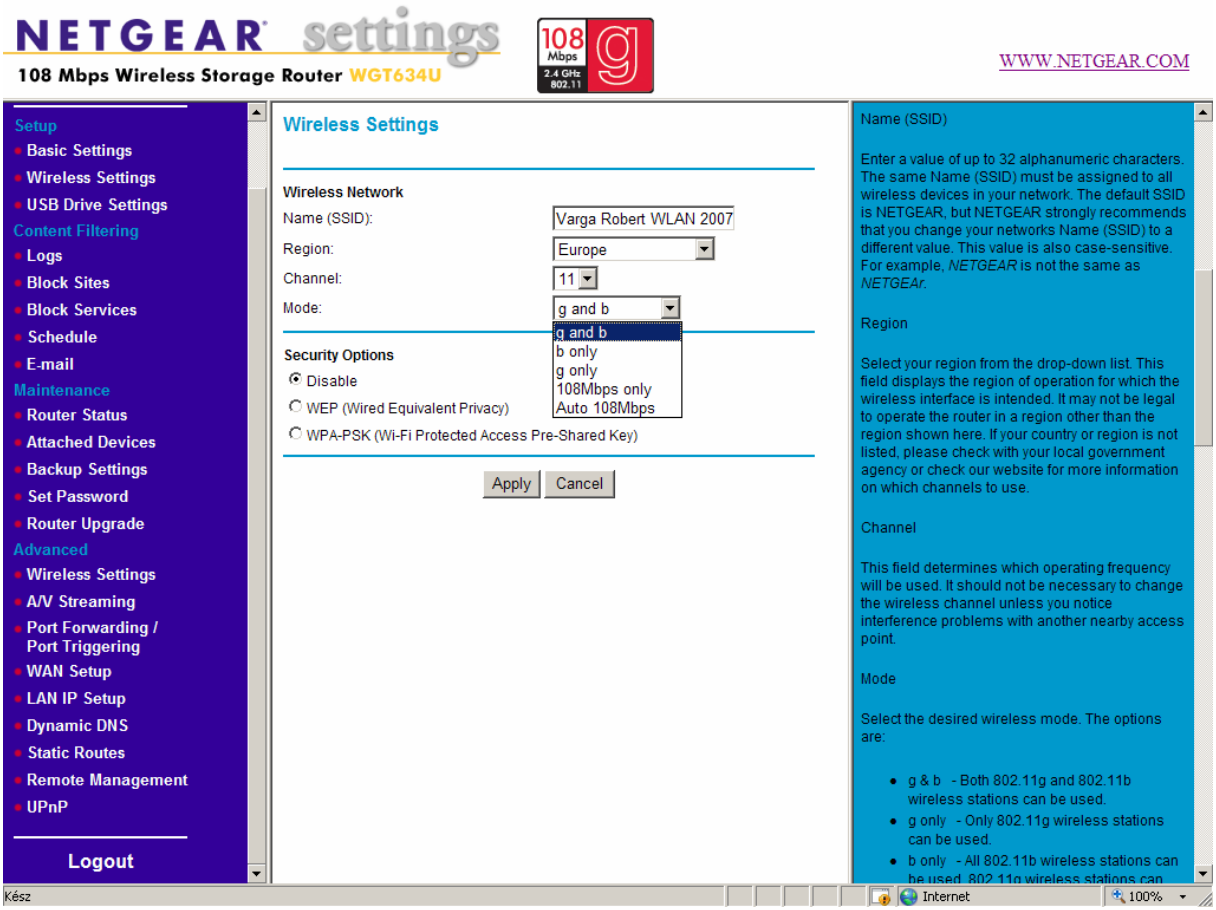
A vezeték nélküli hálózat támadásokkal szembeni első védelmi vonala a hozzáférési pont. Az AP megfelelő konfigurálására tehát időt kell szentelni. A 802.11x alszabványai által támogatott biztonsági protokollok közül a WEP-et biztonsági hiányosságai miatt nem célszerű választani. (Itt meg kell jegyezzem, hogy egy gyenge védelemmel és titkosítással ellátott hálózat is több védelmet nyújt, mint a teljesen nyílt, titkosítatlan hálózatok.) Otthoni vezeték nélküli hálózatok kialakításakor, lehetőség szerint minimum a WPA-PSK beállítása erősen javasolt.

A vezeték nélküli hozzáférési pont (esetünkben egy router) további javasolt, alapvető beállítási lehetőségeit a dolgozat végén, a *Függelék* részben néhány egyszerű lépésben bemutatom.

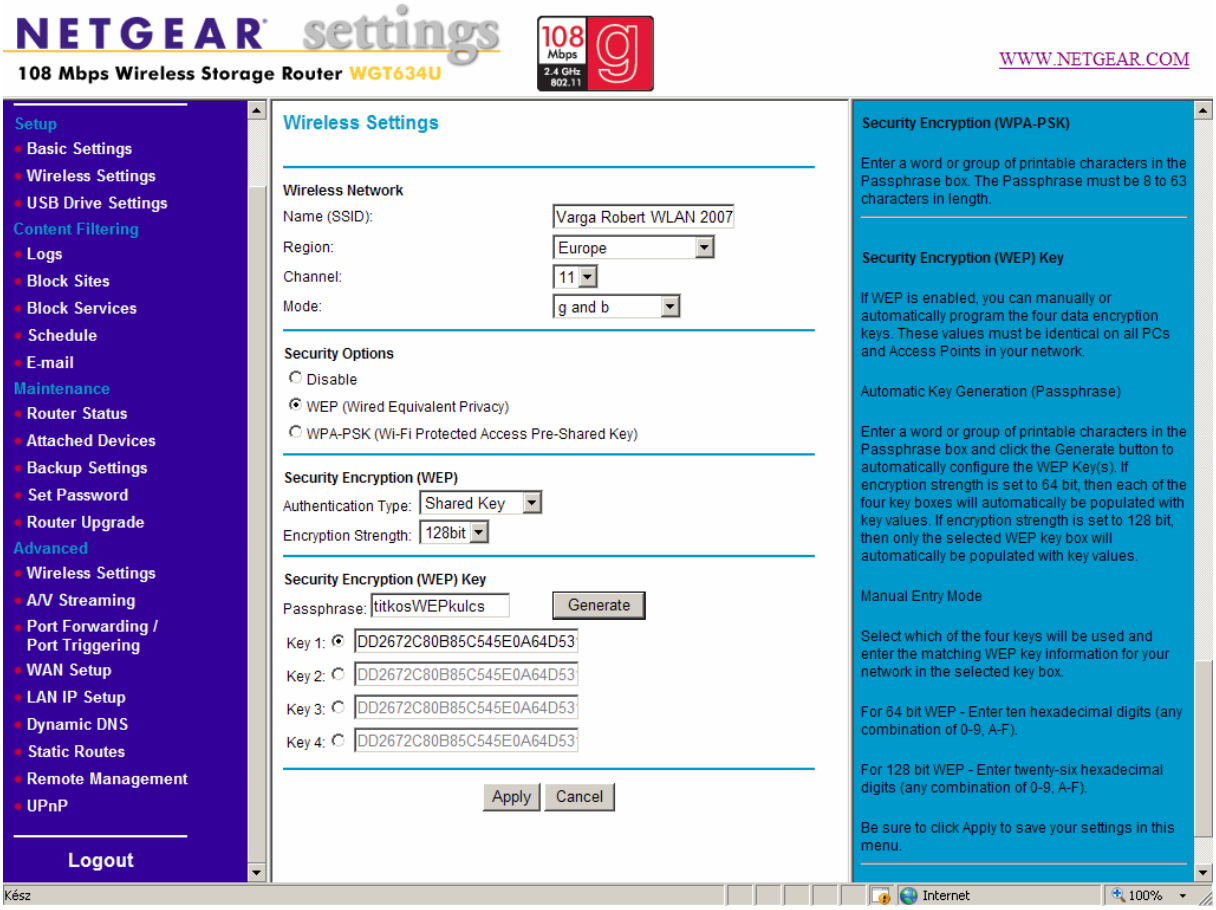
A dolgozatban ismertettem a vezeték nélküli eszközök által alkalmazott 802.11x szabvány családot és a vezeték nélküli technológia által alkalmazott biztonsági protokollok működését, esetleges hiányosságait. Ezek ismeretében általánosságban kijelenthetjük tehát, hogy a vezeték nélküli hálózatok biztonsága a megfelelő óvintézkedések megtétele mellett kielégítő. Feltörhetetlen hálózat nem létezik és soha nem is lesz, hiszen a számítástechnika biztonságának világában a leggyengébb tényező mindig az ember.

Függelék

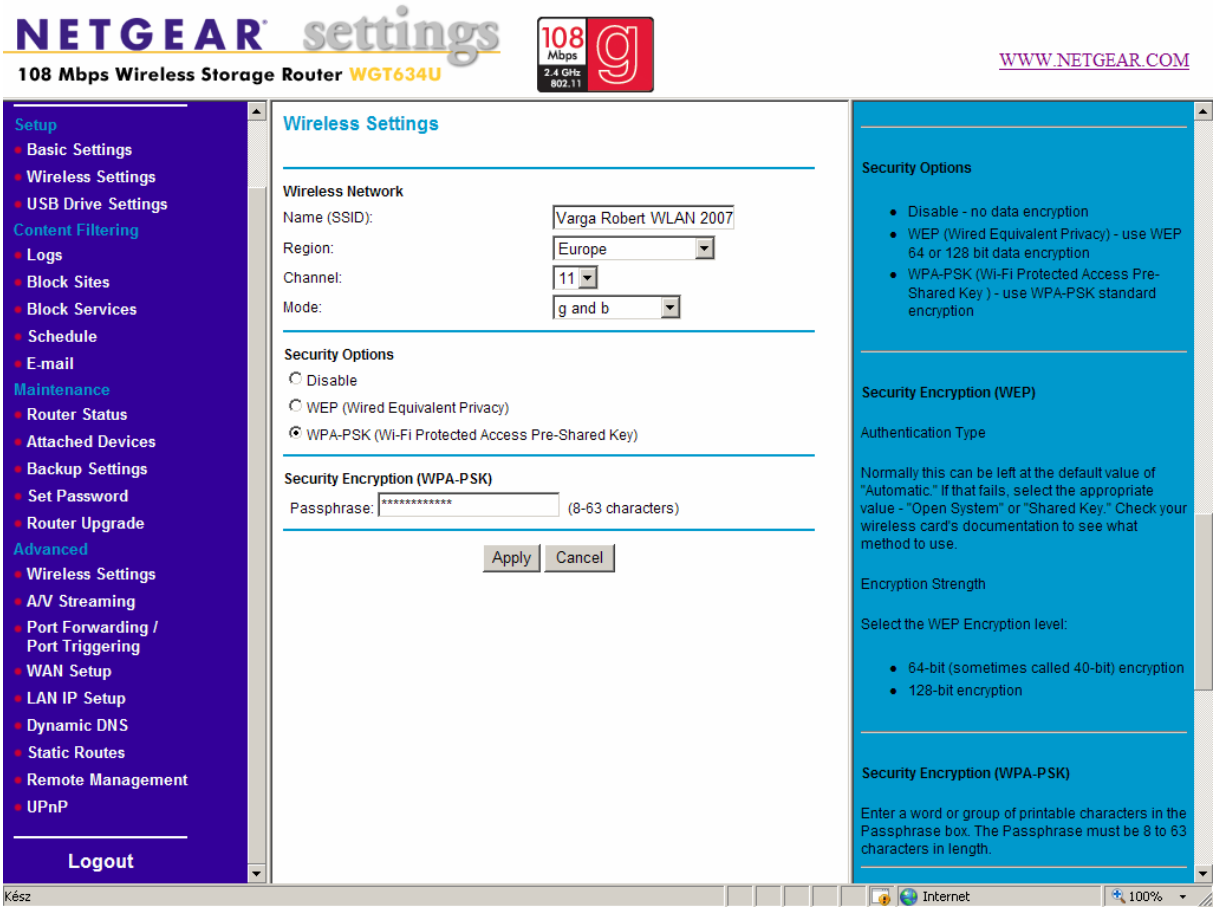
A következőkben egy beépített hozzáférési ponttal (Access Point) rendelkező vezeték nélküli router alapvető biztonsági beállításait mutatom be. Az első lépésben változtassuk meg a vezeték nélküli hálózat „nevét” (SSID), valamint a router eléréséhez szükséges jelszót. Állítsuk be továbbá, hogy a router melyik 802.11 szabvány szerint működjön. Azt a működési módot állítsuk be, amivel a számítógépünkben lévő vezeték nélküli adapter működni képes. Amennyiben 802.11b szabványt támogató és 802.11g szabványt támogató adapterekkel szerelt számítógépeket szeretnénk egyidejűleg hálózatunkhoz csatlakoztatni, úgy lehetőségünk van közös mód kiválasztására is (a 802.11b és 802.11g alszabványok között biztosított kompatibilitás miatt).



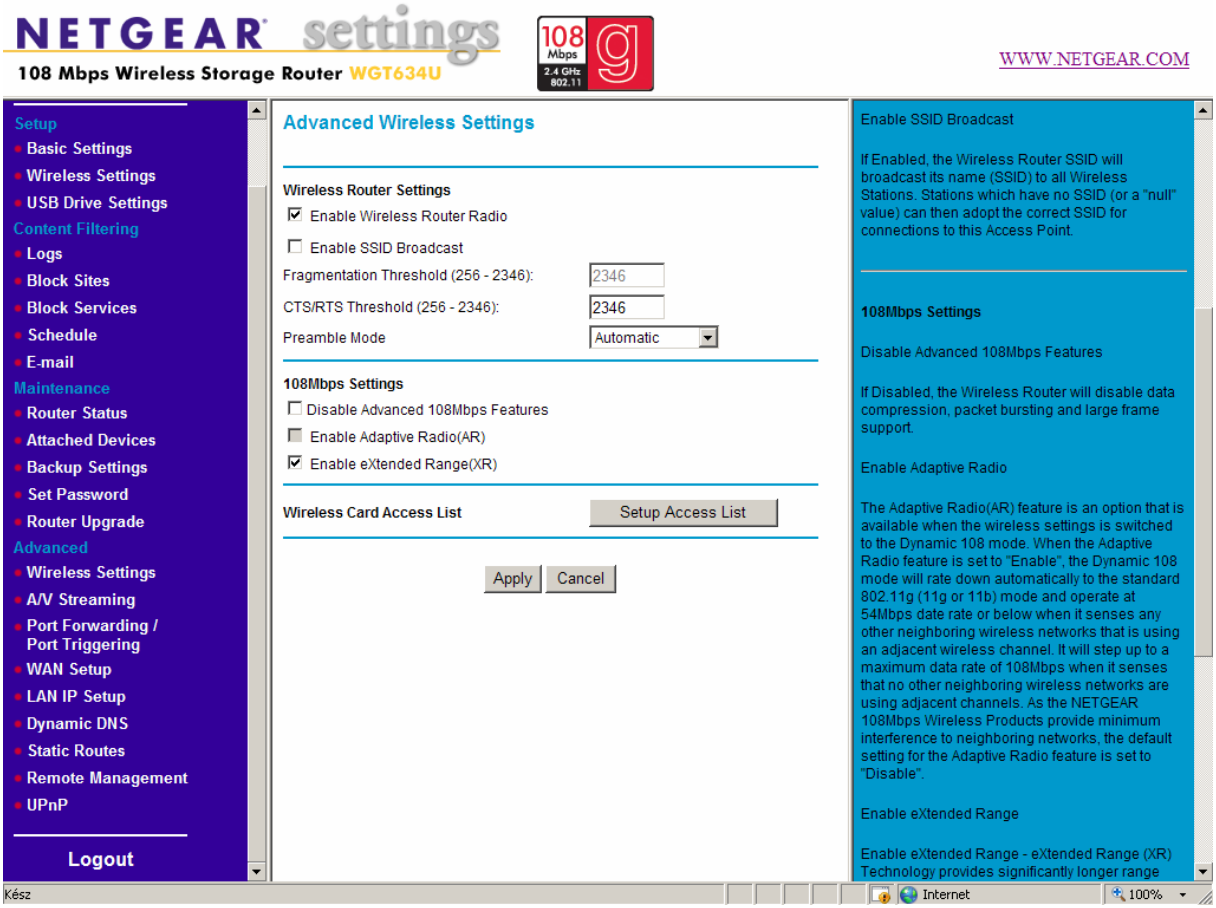
Ezt követően állítsuk be az alkalmazni kívánt titkosítási protokollt. WEP kiválasztása esetén lehetőségünk van választani nyílt rendszerű, vagy osztott kulcsú működési módok, valamint 64 bites, vagy 128 bites titkos kulcs közül.



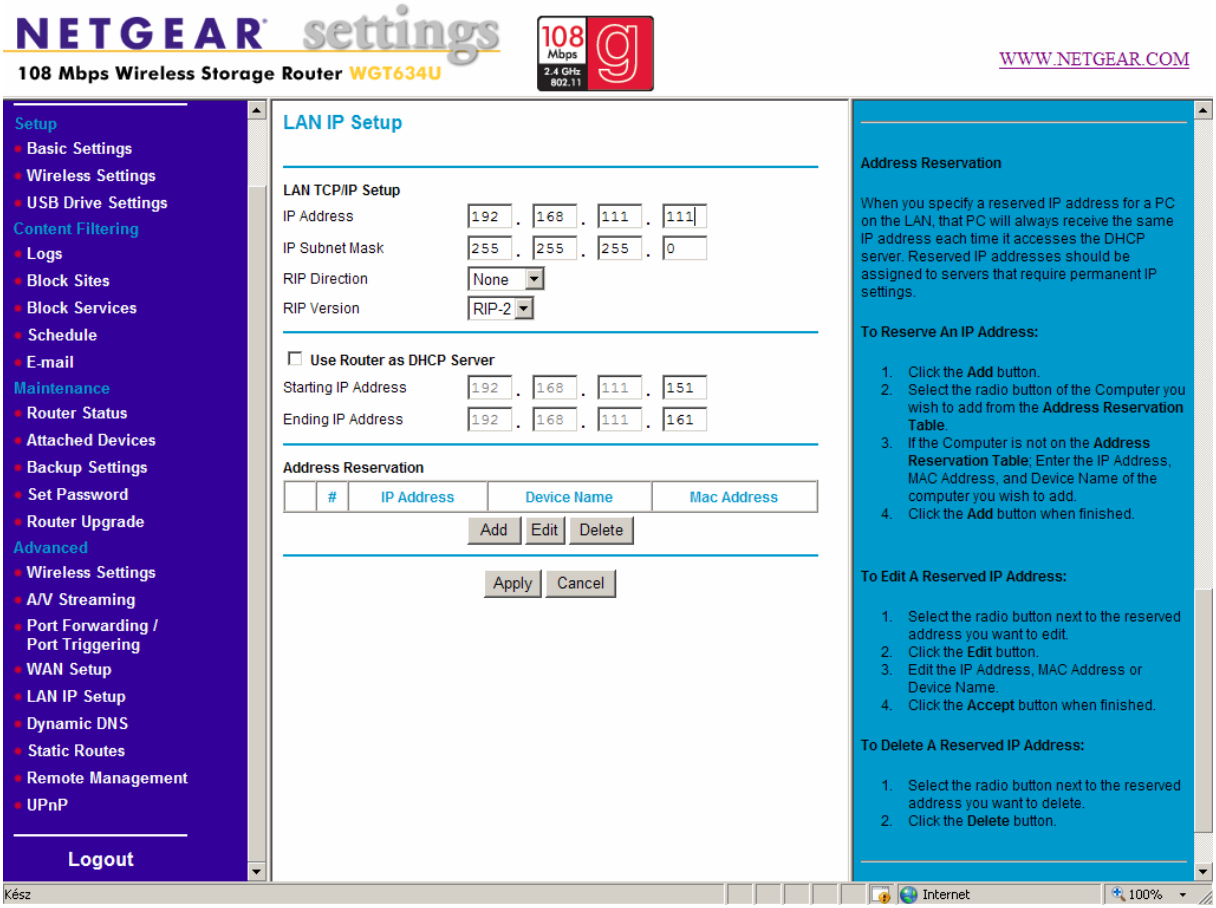
Természetesen a vezeték nélküli hálózati eszközeinknek megfelelően a lehető legbiztonságosabb protokollt érdemes választani, jelen esetben ez a WPA-PSK. A WPA SOHO hálózatok számára ajánlott Personal változatánál, azaz osztott kulcsú működés esetén lehetőleg minél hosszabb és bonyolultabb karaktersorozatot állítsunk be.



Mindezek után természetesen lehetőségünk van a router-ünk további finomhangolására többek között az SSID Broadcast letiltására, valamint a MAC szűrés beállítására. Mindezeken túlmenően is számos további beállítási lehetőség van, ami a hálózatok biztonságát hivatott szolgáltatni, viszont ezek már a vezetékes kliensekre is vonatkoznak.



A vezeték nélküli hálózat nevének és a router adminisztrátor jelszavának megváltoztatása mellett célszerű az alapértelmezettként beállított alhálózat beállításokat is módosítani. A DHCP szerver engedélyezését szintén meg kell fontolni, ugyanis letiltásával a biztonság szintje tovább fokozható.



IRODALOM JEGYZÉK

Jon Adney, William A. Arbaugh:

Real 802.11 Security: Wi-Fi Protected Access and 802.11i (Addison Wesley)

Andrew S. Tanenbaum:

Számítógépes hálózatok (Panem)

Chris Hurley, Michael Puchol, Russ Rogers, Frank Thornton:

WarDriving: Drive, Detect, Defend: A Guide to Wireless Security (Syngress)

Rob Flickenger:

Building Wireless Comunnity Networks (O' Reilly)

Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet, Jefrey Posluns, David M. Zendzian:

Hack Proofing Your Wireless Network (Syngress)

Joseph Davies:

Biztonságos vezeték nélküli hálózatok MS Windows alatt,
az IEEE 802.11 szabvány szerint (SZAK)

További források (Internet)

http://en.wikipedia.org/wiki/

http://hu.wikipedia.org/wiki/

http://www.microsoft.com/wifi

http://wi-fi.org

http://www.pdamania.hu/content/4543/

http://standards.ieee.org/getieee802/802.11.html

http://wirelessdefence.org

http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

http://www.huwico.hu