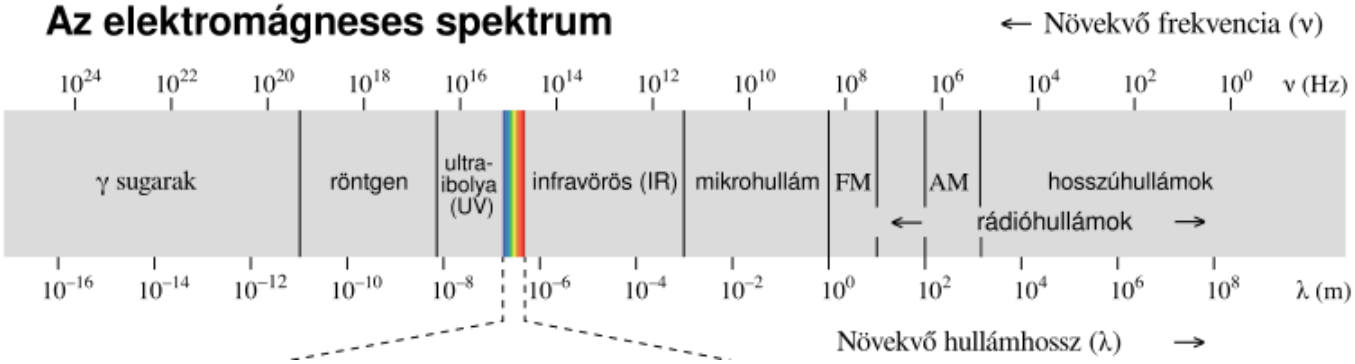
9. fejezet – A vezeték nélküli adatátvitel és WLAN

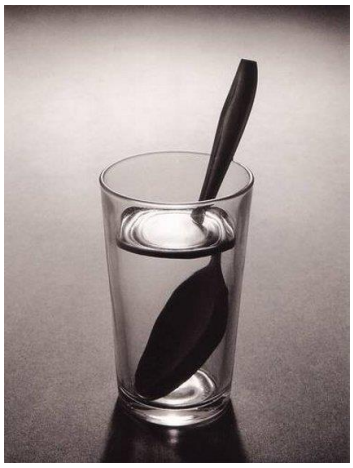
A vezeték nélküli adatátvitel

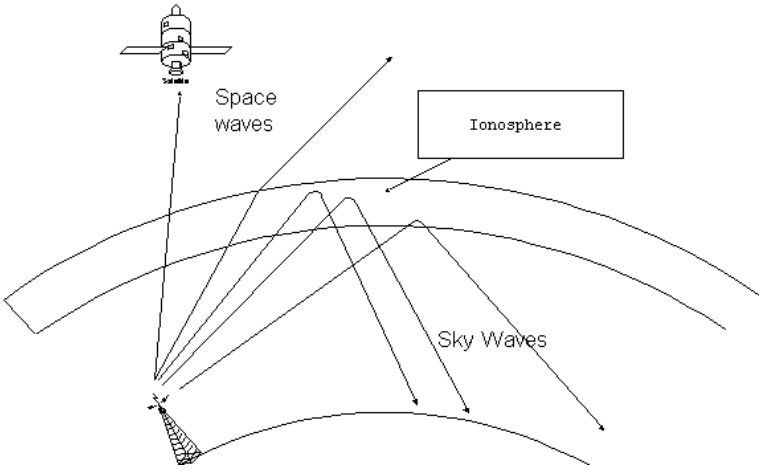
Az elektromágneses hullámok könnyen eljuthatnak olyan helyekre is, ahová elektromos illetve optikai kábelt sem lehet gazdaságosan elvezetni, vagy abszolút nem is érdemes elvezetni. Ez adódhat a terület megközelíthetetlenségéből (pl. sok kis sziget esetében), vagy pusztán a távolságból (pl. kontinensek esetében).
Az elektromágneses hullámok esetében nem szabad megfeledkezni arról, hogy terjedéssel kapcsolatos tulajdonságaik a frekvencia növekedésével megváltoznak.



Amíg a legalacsonyabb frekvenciájú rádióhullámok képesek a Föld görbületét követni, a magasabb frekvenciájú hullámok már egyre inkább csak egyenes vonalban terjednek és jól fókuszálhatók. Ezért például a mikrohullámok már jól irányíthatóak. Egy másik fontos különbség az, hogy az alacsonyabb frekvenciájú rádióhullámok könnyebben haladnak át szilárd tárgyakon, mint a magasabb frekvenciájú rádióhullámok. Egy középhullámú rádiót minden további nélkül vehetünk egy betonépületben is, de műholdas TV vétel csak kültéri parabola antennával valósítható meg – ráadásul a műhold pozícióját is pontosan ismernünk kell a terjedés egyenes vonala miatt.
A rövidhullámok már főleg egyenes vonalban terjednek, de a Földet kb. 100km és 500km közötti zónában körülvevő ionoszféráról (amit töltött részecskék alkotnak) visszaverődnek, így akár a Föld egy távoli pontjára is eljuthatnak. A célzás és a találat ezzel a „mandíner-technikával” nem egyszerű, tekintettel arra, hogy az ionoszféra nem egy statikus öv, hanem folyamatosan hullámzik.

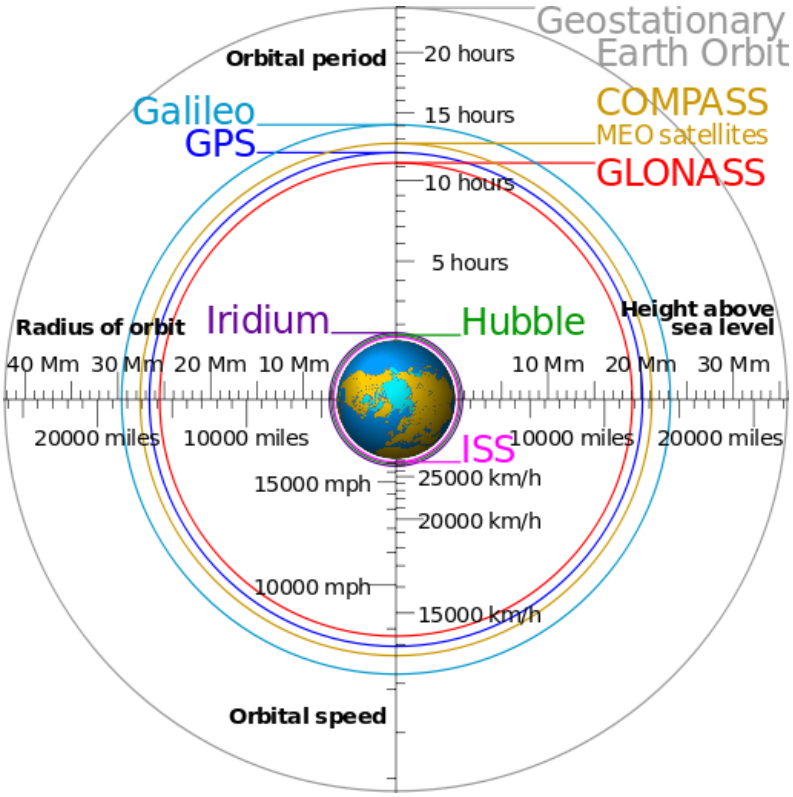
A magasabb frekvenciák, például a mikrohullámok már átjutnak az ionoszférán, de haladásuk egy kis törést szenved. Ezt a megtörést legegyszerűbben úgy tudjuk elképzelni, mint ahogy a kanál képe is megtörik egy átlátszó üvegpohár vízben.

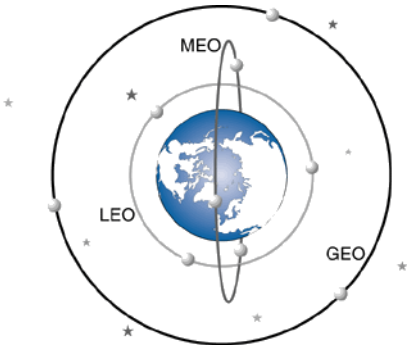


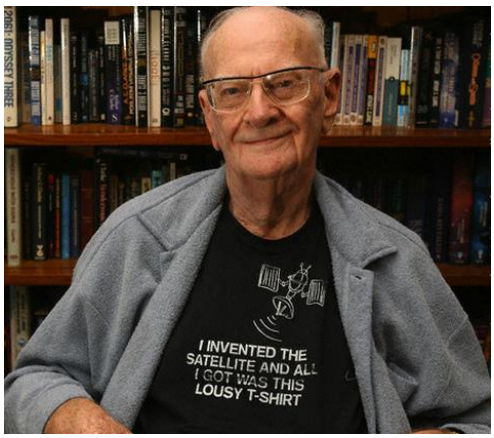


Az infravörös és a látható fény – még abban az estben is, ha koherens, azaz Lézer – ki van téve a légkör torzító hatásainak. Elég csak a délibáb jelenségére gondolni, máris felismerhetjük ezen rendszerek korlátait. Az pedig nyilvánvaló, hogy szilárd tárgyakon a fény nem hatol át, egyszóval ennek a technológiának is megvannak a maga korlátai.

A kommunikációs műholdakat a tengerszint feletti pályamagasságuk alapján szokás 3 csoportba sorolni: LEO (~500-1.500km), MEO (~5.000-22.000km), GEO (Low, Medium, Geostacionary Earth Orbit – Alacsony/Közepes/Geostacionárius Föld feletti Pálya).







A navigációs műholdak (GPS, GLONASS, GALILEO, COMPASS) a MEO pálya magasabb régióiban keringenek.
A pálya minél közelebb van annál kisebb a jel futási ideje (késleltetése), azaz amíg a Földről elér a műholdig és vissza. A légkör fékező hatása a közeli pályákon a legnagyobb, de még a legtávolabbi pályákon sem elhanyagolható!

A műholdas kommunikáció szempontjából a legfontosabbak az úgynevezett geostacionárius műholdak. Ezek a műholdak – Arthur C. Clarke 1945-ben leírt ötlete alapján valósultak meg, amit az ipar lehetővé tette a gyártást és a pályára állítást. Az első geostacionárius műhold az 1964-ban pályára állított Syncom-3 volt. (Az 1962-ben pályára állított első távközlési műhold, a Telstar LEO pályán volt; a Syncom-1 és Syncom-2 pedig geoszinkron pályán mozgott, azaz csak mozgó parabola antennával volt követhető.)
[geostacionárius pálya: A műhold mindig a Föld ugyanazon pontja felett van, azaz együtt, szinkronban mozog a Föld forgásával. Így a műhold a Földről mozdulatlannak látszik, tehát egy fix állású parabolaantennával folyamatosan lehet a műholddal kommunikálni. Az inklináció (pályasík) és az excentricitás (pályalapultság) is nulla fok, azaz a műhold az egyenlítő felett körpályán van. Keringési távolság kb. 35.800km a tenger szintje felett.]

Pont a terjedési tulajdonságok okozták a 750km-es, LEO pályájú Iridium műholdas mobiltelefon rendszer bukását, ugyanis az óceán közepén kiválóan működik a rendszer, de ha már egy-két vagy több betonfödém van köztünk és a műhold között (pl. egy sokemeletes házban) akkor a rendszer már használhatatlanná válik. Az Iridium elnevezés a tervezett 77db műholdra vezethető vissza (az iridium a 77. elem – a végső megvalósítás során azonban elegendő volt 66 műholdat pályára állítani), melyek mindegyike képes a 4 közvetlen szomszédjával kommunikálni.

A műholdas távközlést legjobban meghatározó tényező az, hogy vétel, mint kommunikációs irány egyszerűen megvalósítható, de az adás már bonyolultabb feladat. A vételhez általában egy 60-80cm-es parabola antenna elegendő, de az adáshoz, azaz a felsugárzáshoz ennél lényegesen nagyobb antennákra illetve nagy adóteljesítményre van szükség.
A gyakorlatban a távközlési műholdak nagy többsége gyakorlatilag adatszórást végez, főleg a Földről felsugárzott TV és Rádió műsorokat sugározzák vissza meghatározott területekre. Jelentős a műholdak szerepe a telefonhálózatok összekapcsolásában is – de ez esetben a műholdakkal történő kommunikáció egy földi központi állomáson történik, ahonnan a végfelhasználókhoz a jel már hagyományos telefonvonalon jut el. A közvetlen műholdas telefon polgári használatban nem jelenik meg a mindennapokban.

Klasszikus számítógépes hálózat komponensként, például az internetes forgalom továbbításában részt vesznek műholdak, de polgári alkalmazásokban jellemzően főleg vételi irányban. A kommunikáció lehet kétirányú közvetlen a műholddal is megfelelő antenna és adóteljesítmény esetén, de a jellemző inkább az, hogy a felhasználó egy hagyományos (pl. telefon vagy ADSL) vonalat használ a feltöltéshez.

A vezeték nélküli hálózatok (WLAN – Wireless Local Area Network)

A vezeték nélküli hálózatokkal az IEEE 802.11 szabvány foglalkozik.
A szabványos vezeték nélküli hálózatok létrehozásának első lépése annak a frekvencia sávnak a megtalálása volt, ahol a szintén szabványos adóteljesítménnyel dolgozó kliensek sem egymást sem más elektronikus berendezéseket sem zavartak (túlságosan). Ezeket a frekvenciasávokat az ITU-R (International Telecommunication Union / Nemzetközi Távközlési Unió) az ISM sávban (Industrial, Scientific and Medical / Ipari, Tudományos és Orvosi Rádiósávok) sávban jelölte ki. Ez a sáv persze kellően telített cordless telefonokkal, garázskapu nyitókkal, mikrohullámú sütőkkel, stb., azaz a teljesítménykorlátozás kiemelt fontosságú kérdés.
Egy vezeték nélküli hálózat felépítését tekintve lehet „ad hoc” ahol a kliensek közvetlenül kommunikálnak egymással, vagy állhat bázisállomásokból (Access Point) melyek a kliensek közötti (illetve a kliensek és az internet közötti) kapcsolatot biztosítják.
Érdemes megjegyezni, hogy a vezeték nélküli hálózatokra vonatkozó IEEE 802.11 szabvány és az Ethernet-re (vezetékes LAN-okra) vonatkozó IEEE 802.3 szabvány is a „duplex” alapon adja meg a sávszélességet, miközben egy LAN eszköz jellemzően képes a Full-Duplex átvitelre, addig egy WLAN eszköz pedig csak Half-Duplex átvitelre képes.

Amikor egy vezeték nélküli hálózathoz kívánunk csatlakozni, akkor (általában) ismernünk kell az úgynevezett SSID-t (Service Set Identifier / Szolgáltatásbeállítási Azonosító). Maga az azonosító egy maximum 32 karakter hosszú szabadon választott név. Az esetek jelentős részében ezt egyszerűen ki tudjuk választani a hatókörön belül elérhető hálózatok listájából. Egyes biztonsági megfontolások lehetővé teszik az SSID elrejtését, így csak az SSID pontos ismeretében kapcsolódhatunk a hálózathoz. Ahhoz, hogy a kiválasztott hálózaton adatcserét is folytathassunk általában az SSID ismerete nem elégséges feltétel. Ismernünk kell a titkosítás módját és jelszavát, hacsak nem publikus, azaz jelszó nélküli hálózathoz csatlakoztunk. Ez utóbbi esetben valószínűleg az eszközünk kap is IP címet az Access Point-tól, hacsak nem kerül a MAC azonosítója alapján tiltólistára (ezeknek a részleteiről a félév során a későbbiekben részletesen lesz szó), míg az előbbi esetben az is elképzelhető, hogy nem történik automatikus IP cím kiosztás, hanem egy IP tartományból

magunknak kell egy szabad címet a gépünkre beállítani. Az SSID és a titkosítási jelszó ismerete, valamint az, hogy az eszközünk MAC azonosítója nem esik korlátozás alá tehát nem feltétlenül elégséges a kapcsolódáshoz, hiszen ezzel csak az eszközünket azonosítottuk, magát a felhasználót nem. A felhasználó azonosítása otthoni hálózatok esetében jellemzően soha nem szükséges, míg vállalati hálózatok esetében jellemzően mindig megkövetelt.

Technológiák és szabványok

IEEE szabvány	Megjelenés ideje	Működési frekvencia (GHz)	Sebesség (jellemző) (Mbit/s)	Sebesség (maximális) (Mbit/s)	Hatótávolság beltéren (méter)	Hatótávolság kültéren (méter)	Moduláció
Eredeti 802.11	1997	2,4	0,9	2	~20	~100	Frekvencia-ugrás
802.11a	1999	5	23	54	~35	~120	OFDM
802.11b	1999	2,4	4,3	11	~38	~140	DSSS
802.11g	2003	2,4	19	54 (108 SuperG)	~38	~140	OFMD
802.11n	2009	2,4 / 5	74	300, 450, 600	~70	~250	MIMO, OFMD
802.11ac	2012	5	200	6.930	~50	~250	multi user MIMO, 256-QAM
802.11ax (WiFi 6)	2019	2,4 / 5	1.500	13.000	~70	~240	OFDM 1024-QAM

OFDM – Orthogonal Frequency-division Multiplexing (Ortogonális Frekvenciaosztásos multiplexelés) Az átviteli elv lényege, a nagy sebességű jelfolyam több kisebb sebességű jelfolyamra bontása. A szomszédos sávok az átfedések ellenére sem zavarják egymást.

DSSS – Direct Sequence Spread Spectrum (Direkt-szekvenciális Szórt Spektrumú Moduláció) Az átviteli elv lényege, hogy több (11 darab) szekvenciális egymást részben átfedő (83MHz-es) csatornát használ a (2.4GHz-es) spektrumban. A tartományon belül 3 darab (22MHz-es) csatorna van úgy kialakítva, hogy ezek nem egymásra lapoltak, azaz részben sem fedik át egymást. Ez a technológia teszi lehetővé a frekvenciaugrásos technológiánál nagyobb átviteli sebességet.

MIMO – Multiple in Multiple out

A MIMO ismertetése előtt foglalkozzunk egy pillanatra a 802.11b és a 802.11g szabványok által ígért átviteli sebességek és a gyakorlati tapasztalatok összevetésével. A tapasztalat azt mutatja, hogy a 802.11b esetében az elméleti 11Mbps (ami bitenként átszámítva több

mint 1MB/s) sebességnek jellemzően a fele teljesül, több eszköz egyidejű csatlakozása esetén pedig még ennyi sem. A 802.11g esetében sem sokkal jobb a helyzet, az elméleti 54Mbps (ami bitenként átszámítva több mint 6MB/s) a gyakorlatban még egy eszközzel is elérhetetlen. A közeg jellegéből fakadó problémák, melyeket majd a hiba detektálás illetve hibajavítás témakörben fogunk tárgyalni nyilván nem hidalhatók át, de valamit mégiscsak lépni kellett a technológia fejlesztésének útján, hogy az elméleti és a gyakorlati sebességek lényegesen közelebb kerüljenek egymáshoz.
A MIMO szabvány a nagyobb hatótávolságot és sávszélességet, valamint az elméleti és a gyakorlati adatátviteli sebességek közelítését, az adatátviteli csatornák párhuzamos használatával éri el. Használatához azonban már nem két, hanem legalább három antennára van szükség. A MIMO-val minimalizálódik a visszaverődésből eredő jelgyengülés, a jelirány változása, illetve az emiatt bekövetkező jelkésedelem. Ugyan, a MIMO nem kizárólag a 802.11n eszközök kiváltsága (bár tény, hogy a szabvány leginkább erre támaszkodik), hiszen a technológiával több-kevesebb sikerrel ugyan, de már a 802.11g szabványnál is kísérleteztek.
A szokásos egyetlen jel duplázása vagy erősítése helyett több, különálló jelet alkalmaznak, azaz egyszerre több hálózati kapcsolat épül ki az adó és a vevő között. Mivel teljesen elkülönülő jelekről van szó, kevésbé zavarják egymást, és jelentősen megnövekszik a hasznos sávszélesség.
A Multi User MIMO tulajdonképpen az SDMA technológia olyan kiterjesztése, ahol ugyanabban a frekvenciasávban kommunikálhat egyszerre több adó és vevő is.

####-QAM – Quadrature Amplitude Modulation (Kvadratúra Amplitúdómoduláció)
A kvadratúra amplitúdómoduláció egy olyan modulációs eljárás, ahol az információt részben a vivőhullám amplitúdójának változtatásával, részben annak fázisváltoztatásával (kvadratúra) kódoljuk. Az eljárás a komplex számokra épül, oly módon, hogy a két jellemző egy komplex értékkel jellemzett amplitúdómodulációt határoz meg. (A fázismoduláció tekinthető a QAM egy speciális esetének, ahol az amplitúdó állandó, és csak a fázis változik. Ugyanez kiterjeszthető a frekvenciamodulációs eljárásra, ahol a fázis állandó.) Leggyakrabban nagy sávszélességű digitális jelek analóg csatornán történő továbbításakor használatos. A digitális alkalmazások esetén mind az amplitúdó, mind a fázis kvantált, és így ábrázolható egy X-Y koordináta rendszerben, ami egy pontokból álló mintázatot, egy úgynevezett „QAM képet” eredményez. Az egyszerre átvitt bitek mennyisége növelhető a nagyobb átviteli sebesség érdekében, vagy csökkenthető a megbízhatóbb átvitelért cserébe. A 256-QAM 8 bitet, az 1024-QAM 10 bitet kódol egyetlen jelváltozással.

WEP – Wired Equivalent Privacy (Kábellel Egyenértékű Titkosság)
A WEP volt az első vezeték nélküli titkosítási szabvány. Létezik 64, 128, 256 és 512 bites változata is. Legelterjedtebb a 64 és a 128 bites WEP.
Sajnos az a tapasztalat, hogy még jól beállított eszközök használata mellett is a titkosításhoz használt kulcs az interneten elérhető módszerekkel és eszközökkel visszanyerhető, azaz feltörhető. A WEP titkosítás ugyan védelmet nyújthat az alkalmi próbálkozók ellen, de egy kicsit hamis biztonságérzetet ad. Publikus adatok szerint egy 64bites kulcsot 25.000, míg egy 128bites kulcsot 100.000 csomaggal már nagy valószínűséggel fel lehet törni. A helyzet mégsem annyira drámai, hiszen az Access Point üzemeltetője, ha kellő gondossággal jár el, akkor az Access Point kezelőfelületén azonosítani tudja az összes kapcsolódó felhasználót, be tudja azonosítani a „kéretlen látogatókat", és például a MAC (a kapcsolódó vezeték nélküli eszköz fizikai címe) cím alapján végleg kitilthatja ezeket az eszközöket a hálózatból. A „kéretlen látogatók" két szempontból jelenthetnek problémát, egyrészt megcsapolhatják a sávszélességet, másrészt, ha törvénysértő adatokat forgalmaznak (pl. pedofília, gyermekpornó, stb.) akkor az illetékes hatóságokat az interneten hagyott nyomok sajnos nem hozzájuk, hanem az Access Point üzemeltetőjéhez fogják eljuttatni – ami általában roppant kellemetlen az üzemeltetők számára.

WPA – Wi-Fi Protected Access (Wi-Fi Védett Hozzáférés)
A WPA egy 2003 óta létező titkosítási szabvány. A WPA a TKIP-et (Temporal Key Integrity Protocol / Időszakos Kulcs Sérthetetlenségi Protokoll) egy RC4 alapú titkosító algoritmust használja az adatok titkosítására. A TKIP fő előnye, hogy a beállított idő, vagy forgalmazott adatmennyiség után új kulcsot generál, akár adatcsomagonként is generálódhat új kulcs.

WPA2 – Wi-Fi Protected Access 2 (Wi-Fi Védett Hozzáférés 2. generációja)
A WPA2 titkosítási szabvány 2006-ban jelent meg, és szinte azonnal ki is szorította az első generációs WPA-t, hiszen annak a továbbfejlesztett változata. A TKIP mellett az AES (Advanced Encryption Standard / Fejlett titkosítási Szabvány) titkosítást is támogatja.
Meg kell jegyezni, hogy igazi biztonságot a WPA illetve a WPA2 is csak akkor nyújt, ha kellően hosszú és összetett jelszót használunk – amitől pedig a titkosításra illetve annak feloldására használt aritmetikai igény megnő.

Könnyű azt mondani, hogy ha az eszközünk támogatja a WPA-t, vagy a WPA2-t akkor inkább használjuk azokat, mert a WEP nyilvánvalóan ezeknél gyengébb biztonságot nyújt. Azt sem szabad azonban elfelejteni, hogy az egyes titkosítási eljárások mekkora aritmetikai igényt támasztanak a kapcsolódó eszközök felé. Egy több éves pl. Celeronos

eszköztől, vagy régebbi mobiltelefontól az erősebb titkosítások annyi erőforrást vonhatnak el, amitől az eszköz már-már kezelhetetlenül lelassulhat. Ilyenkor marad a kompromisszum, és a WEP használata. Ha a WPA-t vagy a WPA2-t nem támogatja, vagy képtelen érdemben kiszolgálni az eszközünk (adó és/vagy vevő oldalon), akkor lehetőleg gyakran és rendszeresen cseréljünk WEP kulcsot.

A WPA és a WPA2 továbbá képes hitelesítési szolgáltatást nyújtó szerverrel (pl. RADIUS – Remote Authentication Dial-In User Service / Távoli Hitelesítés Behívásos Felhasználói Szolgáltatásokhoz) is együttműködni EAP (Extensible Authentication Protocol / Kiterjeszthető Hitelesítési Protokoll) hitelesítési eljárással, vagy akár PSK (Pre Shared Key / Osztott Kulcs) üzemmódban is. Az osztott kulcs módot azon otthoni és kisirodai felhasználóknak fejlesztették ki, akik nem tudnak megengedni (pl. az ára és a bonyolultsága miatt) egy dedikált 802.1X kiszolgálót. A 802.1X szabvány hitelesítési keretrendszert biztosít különböző hitelesítési és kulcskezelési protokollokhoz. A RADIUS a felhasználók távoli behívásos bejelentkezését kezelő engedélyezési, hitelesítési és használatkövető ügyfél kiszolgáló protokoll, amely akkor lép működésbe, amikor egy ügyfél bejelentkezik a hálózati hozzáférést kezelő kiszolgálóra, vagy kijelentkezik onnan. A maximális azaz 256 bites WPA-PSK védelemhez olyan kulcs kell, ami 54 véletlenszerű alfanumerikus karaktert, vagy 39 véletlenszerű ASCII karaktert tartalmaz.

Érdekes tapasztalat, hogy egyes Access Point (illetve WLAN Router) gyártók eszközeinek beállításakor 802.11n üzemmód beállítása esetén is választható a WEP titkosítás, miközben a 802.11n szabvány leírásában a WEP már nem szerepel. Ez a gyakorlatban annyit jelenti, hogy 802.11n mellett WEP titkosítást beállítva az adott eszköz vagy 802.11b/g módban fog működni, vagy egyáltalán nem fog működni.

Érdemes megemlíteni még egy – jellemzően lakossági szegmensbe szánt – funkciót, ez pedig az egyes Access Point-okon (illetve WLAN Router-eken) található QSS (Quick Security Settings / Gyors Biztonsági Beállítás) vagy WPS (Wi-Fi Protected Setup / Wi-Fi Védett Beállítás) feliratú gomb szolgáltatása. Mindkettő lehetőség egy kényelmi funkció az eszközeink gyors csatlakoztatására. A gomb megnyomása után a kapcsolódást kérő eszközön megjelenő párbeszédablakba be kell írni azt általában 8 számjegyből álló a PIN kódot, ami az Access Point adattábláján szerepel, vagy amit az Access Point esetileg generált. Ilyen módon „megúszhatjuk” egy bonyolult hosszú jelszó begépelését illetve elgépelését.