Király László

Alkalmazott hálózati ismeretek – Vezeték nélküli kapcsolatok az informatikában

NSZFI
NEMZETI SZAKKÉPZÉSI ÉS FELNŐTTKÉPZÉSI INTÉZET

A követelménymodul megnevezése:

Számítógép javítása, karbantartása

A követelménymodul száma: 1174-06 A tartalomelem azonosító száma és célcsoportja: SzT-026-30

Új Magyarország Fejlesztési Terv

ALKALMAZOTT HÁLÓZATI ISMERETEK-VEZETÉKNÉLKÜLI KAPCSOLATOK AZ INFORMATIKÁBAN

ESETFELVETÉS - MUNKAHELYZET

Munkahelyén, egy komplex informatikai megoldásokat szállító vállalkozás alkalmazottjaként azt a feladatot kapja, hogy kapcsolódjon be a legújabb megrendelés, egy több telephellyel rendelkező cég informatikai hálózatának bővítésében.

A feladat komplex, hiszen a megrendelő telephelyein jelenleg is működnek már informatikai eszközök, ezeket fogják vezeték nélküli eszközökkel bővíteni és informatikai hálózatba integrálni, hogy a megrendelő cég a számítógépeivel az újonnan telepítendő mobil, wifi eszközök (PDA, notebook), a telephelyén belül és a telephelyek között is képesek legyenek adatátvitelre, kommunikációra.

Rendelkezésére áll cégének hálózati szakemberei által elkészített hálózati dokumentáció, valamint a tervezett bővítés után működtetendő hálózat terve.

Az ön feladata a hálózati tervdokumentáció alapján megismerni, a WLAN hálózat kialakításának terveit, valamint közreműködni az egyes wifi eszközök üzembehelyezésében, elvégezni a berendezések csatlakoztatását, ellenőrizni a csatlakoztatott egységek működését.

Jelen tananyag alapvető célja összefoglalni azokat a hálózati ismereteket, melyek a vezeték nélküli (WLAN) számítógép-hálózatokban használatos aktív elemek felhasználásához, rendszerbe állításához, az esetfelvetésben megfogalmazott munkahelyzet megoldása során nélkülözhetetlen.

SZAKMAI INFORMÁCIÓTARTALOM

1.BEVEZETÉS

1. **Vezeték nélküli hálózatok csoportosítása kiterjedésük alapján**

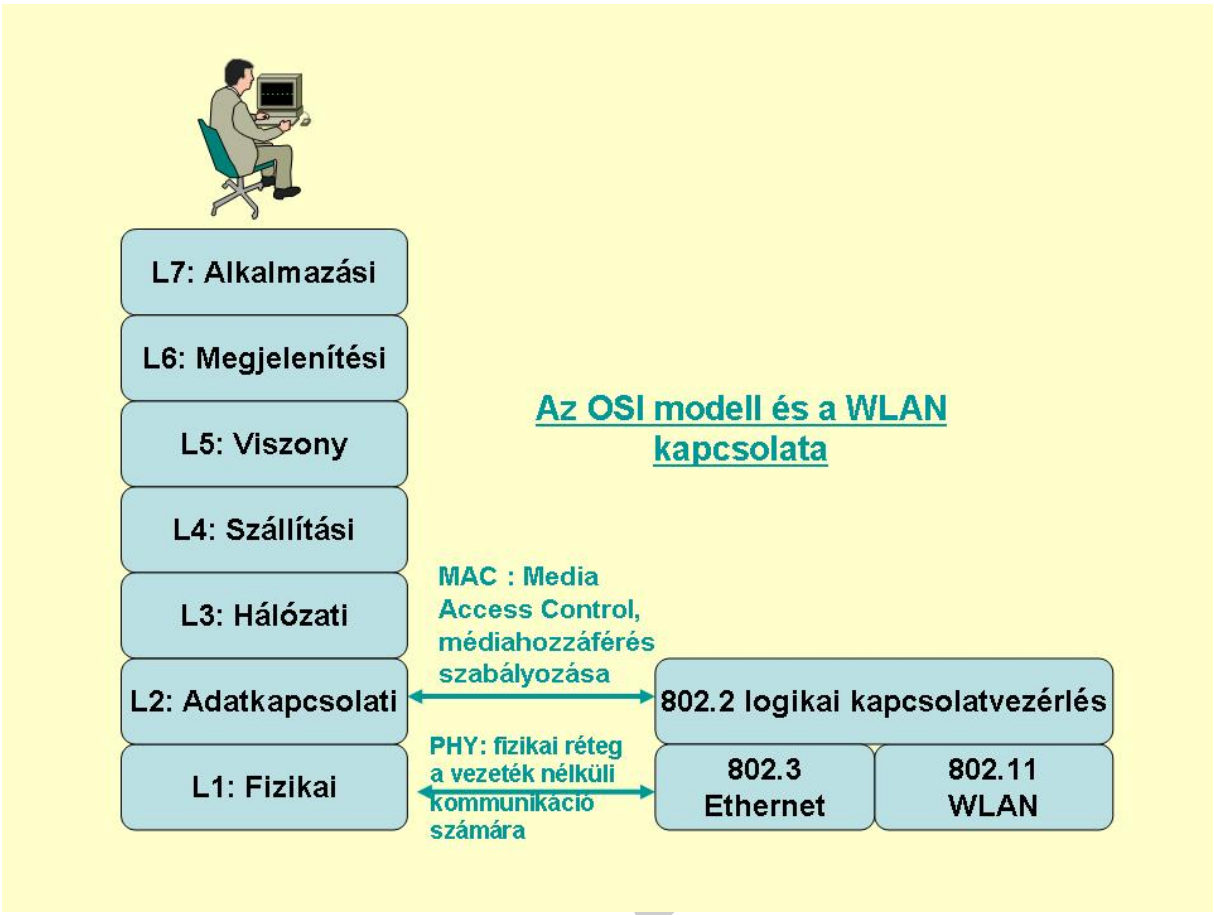
WPAN: a legkisebb méretű vezeték nélküli hálózattípus, melyet általában perifériális eszközök számítógéphez való csatlakoztatására használnak.(pl. egerek, billentyűzetek és PDA) . Az adatátvitel technológiája tipikusan Bluetooth.

WLAN : a vezetékes helyi hálózatok méretének a kiterjesztése céljából használják, vagy olyan helyen ahol a körülmények nem teszik lehetővé a vezetékes hálózat kiépítését (pl. műemlék épület). A WLAN rádiófrekvenciás technológiát használ. A vezetékes hálózathoz való csatlakozás a hozzáférési pontnak (Acces Point, AP) nevezett eszközön keresztül történik. A hozzáférési pont teszi lehetővé a vezeték nélküli állomások és az Ethernet kábeles hálózat állomásai között a kommunikációt..

WWAN : olyan vezeték nélküli hálózat, amely nagy kiterjedésű, földrajzilag nagyméretű területeken biztosítanak lefedettséget. Ilyenek például a mobiltelefonos hálózatok. Ilyen hálózatnak tekinthető például a Mobil kommunikáció globális rendszere (Global System for Mobile Communication, GSM).

2. Az OSI referenciamodell és a WIFI kommunikáció kapcsolata

A hálózati témakör 22. moduljában már ismertetésre került az OSI referenciamodell, mint a hálózatok modellezésére, működésük értelmezésére legáltalánosabban alkalmazott alapelv. Az OSI modell feleleventésére jelen esetfelvetésünk kapcsán azért van szükség, hogy eltudjuk helyezni az OSI rendszerben a WLAN hálózat alapvető jellemzőit. Az 1. ábrán látható, hogy a WLAN a vezetékes kapcsolatra épülő LAN-októl az alsó két rétegben tér el. Ez a tény alapvetően abból adódik, hogy az információátvitel közege nem valamilyen vezetéken keresztül vezetett, hanem a szabadtérben terjedő elektromágneses hullám viszi az információt.



1. ábra Az OSI modell és a WLAN kapcsolatáról

VEZETÉK NÉLKÜLI LAN SZABVÁNYOK

1. Az IEEE 802.11-es szabvány

A WLAN hálózati kommunikációt, a 802.11-es IEEE alapszabvány foglalja össze, amely eredetileg 2 vagy 1 Mb/s-os bitsebességet definiált és a 2,4-2,5 GHz-es frekvenciatartományt használta.

A 802.11-es IEEE alapszabványt a nagyobb bitsebesség elérése érdekében tovább bővítették. A legfontosabb kiegészítései:

802.11a

A 802.11a működési tartománya az 5 GHz környéki frekvenciasávokon található. (A pontos frekvencia a különböző országok hírközlési hatóságaitól függ). A szabványban definiált maximális adatátviteli sebesség 54 Mbps, amely ideális feltételek között érhető el. Az ideálisnál kedvezőtlenebb körülmények között a rendszer kisebb sebességekkel dolgozik. (48Mb/s, 36 Mb/s, 24 Mb/s, 18 Mb/s, 12 Mb/s, 4 Mb/s)

802.11b

A 802.11b a nagyobb bitsebességeket támogató fizikai réteget szabványosította. Működési tartománya egy 2.4 GHz környéki frekvenciasávon található.

802.11g

Nagy sávszélesség elérését teszi lehetővé (54Mbps elméletben, 20 - 30 Mbps a gyakorlatban) a 2.4 Ghz frekvencia tartományban. A hordozható újszámítógépek 95 %-a ma kompatibilis a 802.11b és g szabványokkal, amelyek 13 csatornát használnak. A támogatott adatátviteli sebességek 6,9,12,18,24,36,48,54 Mbps. Emellett képes együttműködni a 802.11b-vel, CCK modulációval 5,5 és 11 Mbps sebességgel, és a 802.11-el 1 Mbps és 2 Mbps sebességgel.

802.11i

Ez a szabvány egyszerre követeli meg az adatok titkosítását (kódolását) és a felhasználók azonosítását/autentikálását (802.1x szabvány), az adatok titkosítása a WPA 2 módszer szerint történhet. Ez a szabvány megfelel a vállalatok adatbiztonsági igényeinek.

802.11e

A szabvány a szolgáltatási minőséggel foglalkozik (Quality of Service-ről beszélünk Magyarországon, QoS). Célja, hogy fontossági (prioritási) sorrendbe szervezze a jelforgalmat (hang, majd video, majd adat). Elsősorban a Wi-Fi hálózatokon megvalósított IP alapú hangátvitelre (Voice over IP) vonatkozik.

802.11 f

Lehetővé teszi, hogy egyik hozzáférési pontról a másikra megszakítás nélkül lépjünk át. (roaming funkció)

802.11n

A várható elméleti maximális adatátviteli sebessége 540 Mbps, amely a 802.11g 10-szerese. A sebességnövekedést a MIMO (Multiple Input Multiple Output) rendszer bevezetésével érik el. A MIMO lényege, hogy egyszerre több adó- és vevőantennát használnak az eszközök az adattovábbításra.

2. A 802.11x fontosabb szabványainak összefoglalása

Szabvány	Működési tartomány	Szabványban rögzített elméleti max. átviteli sebesség Mb/s	Elméleti max. átviteli sebesség Mb/s	Tényleges max. átviteli sebesség Mb/s	Átlagos beltéri távolság
802.11	2,4GHz/5Ghz	1;2	2	1	50 m
802.11a	5 GHz	6;9;12;18;24;36;48;54	54	25	30 m
802.11b	2,4 GHz	5,5;11	11	6,5	50 m
802.11g	2,4 GHz	5;9;12;18;24;36;48;54	54	25	30 m
802.11n			540	200	50 m

3. A WIFI eszközök magyarországi használatának szabályai

Magyarországon a Nemzeti Hírközlési Hatóság (NHH) hatáskörébe tartozik a frekvenciagazdálkodás. Erre azért van szükség, mert a frekvencia (jelenleg) egy korlátos erőforrás. Az NHH két frekvencia sávot engedélyezett a WLAN eszközök számára: 2,4 GHz-es ISM sáv: Ez a sáv 2400 MHz-től 2483,5 MHz-ig terjed. Összesen 13, egymással átfedésben lévő WLAN csatornát definiáltak rajta. A csatornakiosztást a 3. táblázat tartalmazza. A maximálisan engedélyezett, nem engedélyköteles adóteljesítmény ebben a sávban 100 mW. Ezt a sávot számos eszköz használja még a WLAN mellett, ezért gyakran interferencia adódhat, amely rontja a WLAN teljesítményét. Ilyen eszköz például: Bluetooth, Cordless telefonok, Mikrohullámú sütő, stb.

Csatorna száma	Frekvencia MHz	Csatorna száma	Frekvencia MHz
1	2412	8.	2447
2	2417	9.	2452
3	2422	10.	2457
4	2427	11.	2462
5	2432	12.	2467
6	2437	13.	2472
7	2442	14.	2447

5 GHz környéki sávok: Ez a sáv 5725-5785 MHz-ig terjed. A sávban 1W-os maximális adóteljesítmény engedélyezett. A WLAN 802.11a szabványával kompatibilis eszközök működnek ebben a sávban.

RÁDIÓS ÁTVITEL JELLEMZŐI A VEZETÉK NÉLKÜLI HÁLÓZATOKBAN

A rádiós terjedést több tényező is befolyásolja. A falak alapanyaga (tégla, beton, vasbeton, stb.) és mennyezetek csökkentik a jel erősségét, visszaveri a jeleket, és a háttérzaj miatt nehéz a jelet visszaállítani az eredeti formájára (demodulálni). Egy tipikus környezetben, az akadályok és falakon való verődések miatt a különböző helyeken tapasztalható árnyékolási jelenség különböző minőségű jelet eredményez. A wifi csatorna minősége időben nagyon változékony, mivel a környezet nem állandó. A legtöbb gyártó definiálja azt átlagos maximális hatótávolságot, amelyre átlagos működési körülmények mellett a két wifi csomópontot (node-t) lehet helyezni.

1. Adóteljesítmény

Az adási teljesítményt, a kisugárzott jel Watt-okban (vagy miliWatt-okban) mért teljesítményével definiálják. A gyakorlatban a wifi eszközök által előállítható teljesítmény szabályozható, amivel beállítható az optimális vételi körülmények érdekében . Az adási teljesítmény szabályozhatósága elősegíti a más rendszerek által okozott interferencia hatásának csökkentését, de hatása van a frekvenciák újrafelhasználására mivel, ha több hálózatot kell egymáshoz közel üzemeltetni, azok zavarhatják egymást. A kisebb adási teljesítmény viszont csökkenti a besugárzott cella méretét.

2. Érzékenység

Az érzékenység annak a legkisebb jelnek az erősség, amely még a vevőben megbízhatóan érzékelhető, felfogható. Ez az adat alapvetően a vevő minőségével van összefüggésben. Minél kisebb jelet képes érzékelni a wifi eszköz, annál jobbnak kell lennie a vevő hardverének. Az érzékenységet dBm- ben szokás megadni. A tipikus érték – 80 dBm körüli, de minél kisebb ez az érték az érzékenység annál jobb (a -90 dBm érték jobb).

3. Csillapítás

Minél nagyobb a lehetséges csillapítás értéke, annál nagyobb lehet a távolság két eszköz között. 100 mW-os adási teljesítmény és -80 dBm érzékenység mellett, a maximális csillapítás értéke 100 dB. A csillapítás az adó és a vevő jelének logaritmikus viszonyát adja meg, azaz a jel csökkenésének mértékét. A levegőben a távolság négyzetével arányos a csillapítás.

4. Jel/zaj viszony (SNR)

A jel/zaj viszony megadja a vevőben vett jel és zaj teljesítményének a viszonyát. Ahhoz, hogy a vett jelet sikeresen lehessen dekódolni, a vevőben a jel/zaj viszonynak minimálisnak kell lennie. Ez az érték függ a választott modulációtól és a vevőegység minőségétől is.

5. Elhalkulás (fading)

A fading jelensége a rádiofrekvenciás jelátvitel gyakorlati alkalmazásának kezdeteitől fogva már ismert jelenség volt. A jelenség lényege ,hogy a wifi eszköz környezeti viszonyaitól és a terjedési körülményektől függően egy rövid idejű jelerősség csökkenés lép fel olyan környezetben, mint például egy irodaház, vagy lakóház. A jelenség magyarázata ,hogy a rádiójelek különböző úton érkeznek a vevőbe, amelyet a környezeti objektumokról való visszaverődés okoz. A fading átviteli hibákat okoz a jelben, amiket a rendszerben korrigálni kell, a hibák javítása plusz eljárásokat igényel. Minél nagyobb a hatótávolság, a fading jelenségek annál nagyobb valószínűséggel csökkentik a jelerősséget, és a kapcsolatvesztés is valószínűbb.

CSATLAKOZÁS A WIFI HÁLÓZATHOZ

1. Munkaállomás csatlakoztatása

A gyárilag már wifi hálózati kártyával ellátott munkaállomások rendelkeznek az adott hálózati kártya menedzselésére szolgáló szoftverrel, amely tartalmazza azokat a funkciókat, amelyek a wifi kapcsolat felépítéséhez szükséges beállítási lehetőségeket tartalmazzák.

2. ábra WLAN csatlakozás

Más a helyzet, ha a munkaállomás vezeték nélküli hálózati kártyával történő bővítése utólag történik. Ekkor a hálózati kártya hardveres illesztésén túl a hálózati kártya gyári szoftverének telepítését is el kell végezni.

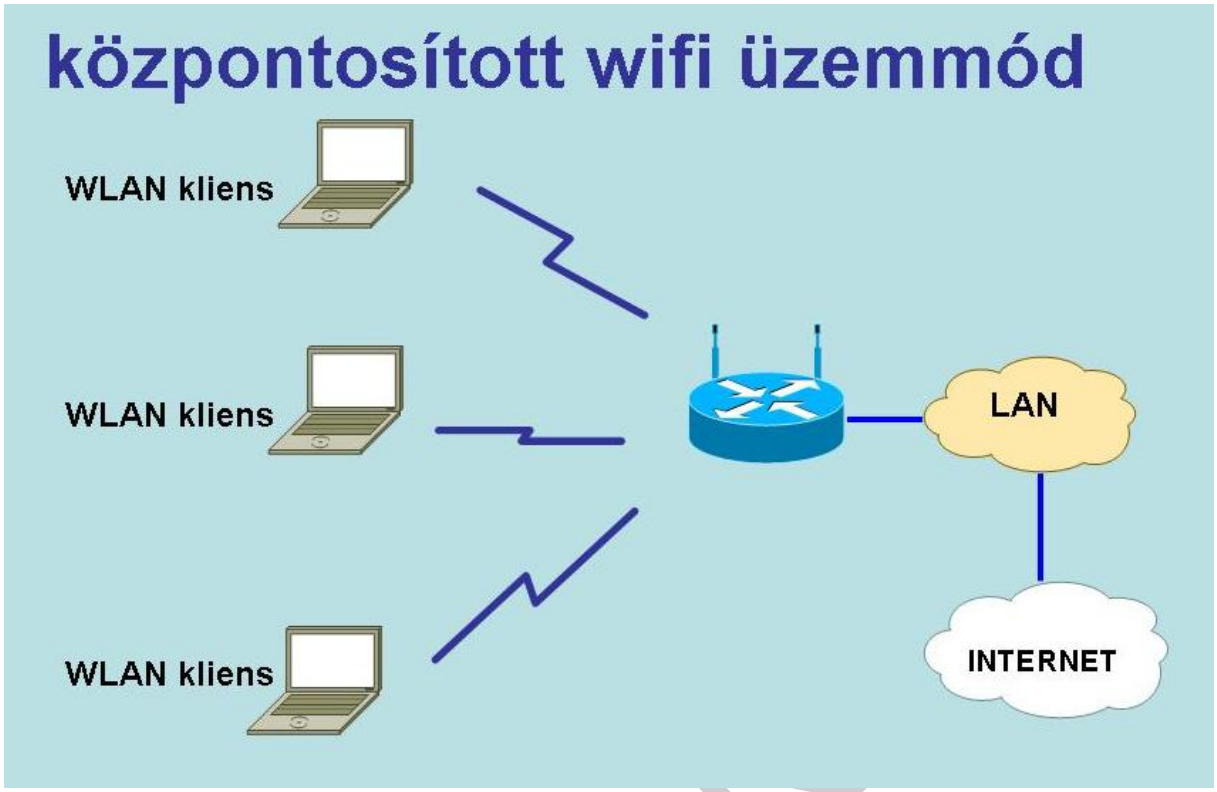
2. ad-hoc hozzáférési üzemmód - (IBSS - Independent Basic Service Set)

A vezeték nélküli állomások közvetlenül egymással kommunikálnak hozzáférési pontok nélkül. Az üzemmód használatával lehetővé válik a vezeték nélküli állomások számára, hogy hozzáférési pont hiányában is könnyen, hatékonyan és egyéb költségek nélkül létesítsenek egymással kapcsolatot. Ebben az esetben a felügyelő és vezérlő feladatot mindig valamelyik állomás látja el. Ha a kapcsolat felvételét kezdeményező eszközök a hatótávolság miatt nem látják egymást, akkor a köztük lévő állomások veszik át az átjáró (router) szerepét. Ha egy kapcsolat felépítésének kezdeményezése során az állomás közelében nincs hozzáférési pont, akkor létrehozhat egy saját IBSS-t, ezáltal hozzáférési pontként működhet.

3. ábra ad-hoc hozzáférési üzemmód

3. infrastrukturális mód vagy központosított mód (BSS – Basic Service Set)

Egy meglévő vezetékes LAN hálózathoz egy vagy több hozzáférési pont csatlakozik, és a vezeték nélküli állomások ezen keresztül kapcsolódnak a vezetékes LAN hálózathoz. Ebben az esetben a vezetékes LAN hálózat kibővül egy vezeték nélküli résszel. Ha egy állomás nem lát be akkora területet, mint amekkora két távoli vezeték nélküli állomás kommunikációjához szükséges, akkor a központosított módban működő hálózatok összefoghatóak egy nagyobb struktúrába, melyet bővített szolgálatnak (ESS – Extended Service Set) hívnak. Ebben az esetben a hálózat több hozzáférési ponton keresztül is elérhető.



4. ábra központosított wifi üzemmód

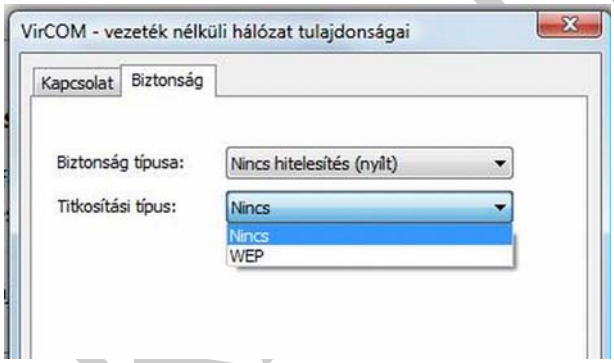
A VEZETÉK NÉLKÜLI HÁLÓZATOK BIZTONSÁGI KÉRDÉSEI

A WLAN (vagy más néven WiFi) által használt vezeték nélküli közeg miatt a biztonság garantálása sokkal fontosabb szerephez jut, mint a vezetékes hálózatok esetében. Ennek oka, hogy egy esetleges támadó egy nem megfelelően védett WLAN hálózathoz egyszerűen férhet hozzá (például egy WLAN-al ellátott épületen kívül is) és innen teljesen anonim módon indíthat támadást. A támadott fél ekkor úgy érzékeli, hogy a támadó az áldozat hálózatához tartozó személy (vagyis számítógép).

A biztonság szempontjából a protokollok két feladatot látnak el:

Hitelesítés (Authentication): A hitelesítő rendszer feladata eldönteni, hogy egy csatlakozni kívánó felhasználó valóban használhatja-e a hálózat erőforrásait. Vagyis például kapcsolódhat-e az adott hozzáférési ponthoz (AP – Access Point), és használhatja-e a vezeték nélküli hálózat erőforrásait, például az Internetet. Emellett létezik üzenethitelesítés is, amely már egy hitelesített viszonyban a titkosított üzeneteket védi a módosítással szemben (integritásvédelem).

Titkosítás (Encryption): A nyílt adatátviteli közeg feltétlenül felveti az illetéktelen hozzáférés kizárásnak kérdését. A lehallgatás lehetőségének kizárása, az adatok illetéktelenek hozzáférésétől való megvédése alapvető kívánalom. A nyílt adatátviteli közegen történő jelátvitel titkosítása alapvető feltétele a WLAN hálózat biztonságának. A vezeték nélküli jelátvitel titkosítási eljárásának a leírása a **WEP (Wired Equivalent Privacy)** a 802.11 szabványban jelent meg, célja – mint ahogy a neve is mutatja – a vezetékes szakasszal azonos biztonság nyújtása a vezeték nélküli szakaszon. Mint minden titkosítási eljárás ki van téve annak a szellemi kihívásnak, amely a kódfeltörők számára megfejtendő feladatot jelent. A protokollban található hiányosságokat meg is találták és 2002-ben sikeresen fel is törték.(Megfejtették a titkosított vezeték nélküli jelátvitellel közvetített információt.) Tehát a WEP nem tekinthető a vezetékes szakasszal azonos biztonságot nyújtó titkosítási eljárásnak. **Sőt egyáltalán nem biztonságos!** A WEP-el védett hálózatok manapság már csak 10 percig nyújtanak védelmet a lehallgatással, és az adatmódosításokkal szemben. A továbbiakban ismertetjük a WEP két hitelesítési eljárását, majd ezt követően bemutatjuk a WEP rejtjelezési módszerét és foglalkozunk a WEP keretek felépítésével is. Végezetül megvizsgáljuk, hogy a bemutatott módszerek miért nem biztonságosak, és tárgyaljuk a WEP hibáit is.



5. ábra WEP titkosítás

A WEP HITELESÍTÉSI ELJÁRÁSAI

1. NYÍLT HITELESÍTÉS

6. ábra nyílt hitelesítés

A nyílt hitelesítés esetén a kapcsolódni kívánó munkaállomás egy „Hitelesítés kérés” üzenetet küld a 802.11 keretben az AP-nak, amely mindenféle feltétel nélkül ezt elfogadja, és egy „Hitelesítés válasz”-ban jelzi a munkaállomás számára, hogy csatlakozhat a hálózathoz. **Az adatok végig titkosítatlanul haladnak.** Ezt az eljárást ezért is kicsit túlzás „hitelesítésnek” nevezni, ez inkább egyfajta igénybejelentés a kliens részéről.

2. OSZTOTT KULCSÚ HITELESÍTÉS (shared key authentication)

A hitelesítés folyamata:

1.seq.: a kliens a hozzáférési pont felé küldött üzenetében megadja, hogy egy osztott kulcsú hitelesítéssel szeretne kapcsolódni (auth=SK),

2.seq.: az AP erre válaszul egy olyan keretet küld, amelyben szerepel a hitelesítési eljárás típusa, továbbá egy véletlen számot (RAND) küld kihívásként a kliensnek.

3.seq.: a kliens erre válaszul a saját WEP kulcsával (KEY) betitkosítja a kapott véletlen számot (RAND), és ezt elküldi a szervernek.

4.seq.: A szerver ez után ellenőrzi, hogy a kliens valóban ismeri-e a hálózat WEP kulcsát. Ezt úgy teszi meg, hogy a titkosított véletlen számot kititkosítja a saját WEP kulcsával, és ha így az eredeti RAND értéket kapja meg, akkor igen nagy valószínűséggel (közel 100%) biztos lehet benne, hogy a kliens ismeri a kulcsot, és így jogosult a hálózathoz való kapcsolódásra. Az ellenőrzést követően – helyes RAND érték esetén – jelzi a kliens felé, hogy a hitelesítés sikerült, kapcsolódhat a hálózathoz (OK). Sikertelen hitelesítés esetében természetesen elutasítja a kapcsolódási igényt.

7. ábra kép osztott kulcsú hitelesítés

A WIFI HÁLÓZAT KIALAKÍTÁSÁNAK SZEMPONTJAI

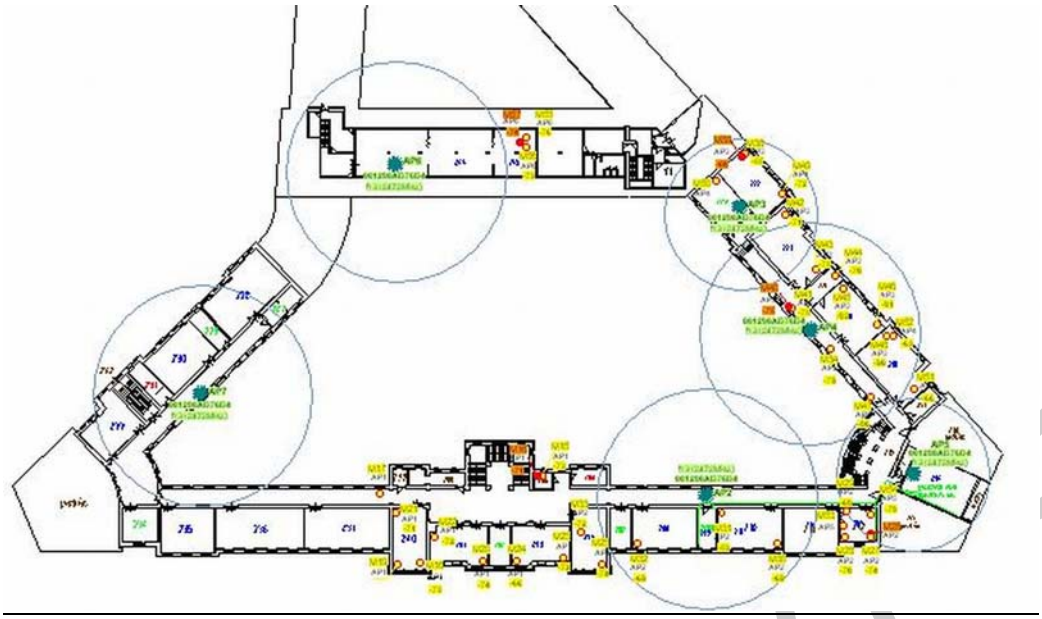
Egy új wifi hálózat létrehozása vagy egy meglévő bővítése előtt érdemes néhány fontos szakmai kérdést áttekinteni:

- mekkora sávszélességet igényelnek a hálózaton futtatott programok?
- hány felhasználó fogja használni a WLAN-t?
- mekkora lefedettségi területre van szükség?
- milyen a meglévő, bővítendő hálózati kiépítés?
- mekkora a rendelkezésre álló költségvetés?

Lefedettségi terület

A vezeték nélküli LAN hozzáférési hálózat feladata, hogy megfelelő lefedettség alkalmazásával a területén mobil, és/vagy fix kiépítésű WLAN kliensek részére a vezetékes LAN hálózathoz történő hozzáférést biztosítson.

A kialakítandó WLAN rendszertechnikai szempontból a WLAN hozzáférési csomópont által kiterjesztett pont - több pont (PMP) felépítésű lesz. A WLAN hálózat hatóköre, területi lefedettsége egyik kiinduló szempontként vetődhet fel. Ahogy a vezetékes hálózatnak az alkalmazott vezetékes technológiától függően van egy maximális hatóköre, úgy a vezeték nélküli hálózati technológiáknak, valamint a környezeti tényezőknek a függvénye a hálózat által elérhető terület.



8. ábra lefedettségi térkép

A 8.ábrán példát láthatunk arra, hogy a megvalósított WLAN hálózat egyes hozzáférési pontjai nem valósítják meg a teljes lefedettséget. Ez az eset nem feltétlenül hiba hiszen lehet, hogy a megrendelő eleve ilyen módon specifikálta a feladatot. Az biztos, hogy az ábrán látható épületrészletben nem valósítható meg a folyamatos wifi kapcsolat.

A WLAN kliens

A vezeték nélküli LAN hozzáférési végpont az AP-kon keresztül teljes joggal bíró kliense a vezetékes LAN hálózatnak. Ezért ugyanazon alkalmazások futtatására van lehetőség, mint a vezetékes LAN hálózatokon keresztül.

A vezetékes LAN hálózaton szereplő egyéb adatok biztonsága érdekében a gyakori megoldás az internet kapcsolat VLAN technológiával történő elkülönítése. A VLAN technológiával biztosítható, hogy a WLAN kliensek internet hozzáférése elkülönítve valósuljon meg. A vezeték nélküli végponti kliensek azonosítása MAC address alapú, melyet a WLAN hozzáférési csomópont konfigurációs beállítása biztosít.

WLAN hálózat felügyelete, menedzselése

A vezeték nélküli hozzáférési hálózat AP berendezései, mind lokálisan, mind távolról elérhetőek és konfigurálhatók. A WLAN kliensek beállításait lokálisan, működését távolról ellenőrizhetjük, miután kapcsolódott az AP-hoz.

Nagyszámú AP felépítettség esetén célszerű központosított szerver alapú hálózatfelügyeleti segédszoftvert alkalmazni, mely nem csak a hálózatban működő elemek ellenőrzését és beállítását képes elvégezni, hanem támogatást nyújt különféle RF monitorozásban és idegen WLAN elemek kiszűrésében is.

RÁDIÓS ÁTVITEL JELLEMZŐI A WLAN-OKBAN

A rádiós jelterjedést nagyon sok tényező befolyásolhatja. A falak és mennyezetek anyagi minőségüktől, kialakításuk módjától függően csökkenthetik a jel erősségét, visszaverik a jeleket, és a háttérzaj miatt nehéz a jelet a vevő egységben detektálni, illetve demodulálni. Az információ átviteli csatorna minősége időben nagyon változékony, mivel a környezet nem állandó. A legtöbb gyártó definiálja azt az átlagos maximális hatótávolságot, amely átlagos működési körülmények mellett értendő.

Adóteljesítmény

Az adóteljesítményt, a kisugárzott jel Watt-okban (vagy mW-okban) mért teljesítményével adják meg a gyártók, illetve a szabványok. A szabályozás természetesen korlátozhatja a készülékkel elérhető maximális teljesítmény értékét. Problémát jelenthet a nagy adási teljesítmény, amely elősegíti a más rendszerekkel történő interferenciára, tehát ha több hálózatot kell egymáshoz közel üzemeltetni, azok zavarhatják egymást. A kisebb adási teljesítmény viszont csökkenti a cella (vételi körzet) méretét, ezért az AP-k többségénél megválasztható az adóteljesítmény értéke.

Rádiófrekvenciás kiszóródás

Tipikus wifi probléma, hogy az épületek többségénél megjelenik a "rádiófrekvenciás kiszóródás" jelensége, ezáltal a WLAN hálózathoz történő elvi, jogtalan hozzáférés. Ennek a lehetőségét minimalizálhatjuk, ellensúlyozhatjuk, vagy az AP-k kimenő teljesítményének csökkentésével, vagy/és megfelelő WLAN security kialakításával.

Interferencia kialakulási lehetőségek

Zárt, beltéri térrészben a minél több sugárzó forrás alkalmazása, minél több interferenciás pont kialakulását eredményezheti. Ugyanakkor a meglévő fémes szerkezetek, újabb reflexiós pontot, újabb kiindulási határfelületet biztosítanak a rádiófrekvenciás jelnek. Ezért célszerűen törekedni kell az optimális bázisállomás, rádiófrekvenciás adó-vevő darab számának, valamint az alkalmazandó sugárzó forrásának helyes megválasztására.

Az AP-ok fizikai elhelyezésének rendezettsége lehetőséget ad egy helyesen megválasztott frekvencia újraalkalmazására, mely minimalizálja az interferenciás zavarok kialakulását. Az iskola területén belül biztosítható, hogy az AP-ok által lefedett térrészek kapcsolódási pontjainál nem alakulnak ki interferenciás területek, ahol akár 3 AP rádiófrekvenciás vivője is jelen lesz. Ezeken az interferenciás pontokon a WLAN kliens rádiófrekvenciás vevő egysége képtelen lesz határozott, kiértékelhető vezeték nélküli LAN kapcsolódásra.

Interferenciás zavarok

- Azonos csatornajelből származó zavarok

Több WLAN hozzáférési hálózat csomópont együttes működtetése esetén cella alapú hálózati rendszert szükséges kialakítani a zavarok kialakulásának csökkentése érdekében. Ezen szabály betartásával jártunk el az AP frekvenciavivőinek tervezésekor.

- Más alkalmazásból származó zavarok kialakulása

A szabadon használható, azonos WLAN frekvenciasávban működő berendezések együttesen zavarok okozhat a WLAN kapcsolatokra. Ezért törekedni kell ezen zavaró körülmények, működések kiküszöbölése vagy legalább a hatásuk csökkentésére a zavarok elkerülése érdekében. Feltételezzük, hogy csak WLAN hozzáférési hálózatot kívánunk üzemeltetni.

- Vezeték nélküli csatornák

Ha egy WLAN hálózaton belül több eszköz is kommunikál egymással, akkor a küldő és fogadó állomások közötti párbeszédet az egymás zavarásának kiküszöbölése érdekében el kell különíteni egymástól. Erre a feladatra a csatornák használatát alkalmazzák. A csatornák a rendelkezésre álló rádiófrekvenciás tartomány részekre bontásával jönnek létre. A csatornák által elkülönített párbeszédek eredményeképpen több hozzáférési pont képes egymáshoz közel üzemelni.

WLAN hálózatok biztonságának gyengeségei

- Szerver alapú azonosítás hiánya

Sok WLAN AP esetében körülményes a biztonsági beállításokat megváltoztatni és újra érvényesíteni.

- Gyenge azonosítási mód

A jogosult WLAN kliensek MAC cím alapú azonosítása meghamisítható, amennyiben egy idegen felhasználó azt megismeri. Többféle olyan wifi hálózati kapcsolat kiépítésére alkalmas szoftver létezik, amely a MAC cím utánzására (MAC klónozásán) építve kerüli ki az azonosítási védelmet.

- A jogosultság típusának megújítása

A rádiófrekvenciás jel titkosításához statikus kulcs van alkalmazva, melynek újból megváltoztatásához az összes hozzáférési csomópont konfigurációjának megváltoztatása szükséges. Ugyanígy a végponti WLAN kliensek esetében is szükséges frissíteni a hálózathoz történő hozzáférés kulcsát.

- WLAN hálózat felügyeleti nehézségek

Az AP-ok elhelyezésének magassága és megközelíthetősége a lokális konfigurálás lehetőségét nagymértékben megnehezíti. Az esetek többségében távolról célszerű ezen hálózatfelügyeleti tevékenységeket ellátni. Legkézenfekvőbb telnet, vagy http (https) alkalmazása egyéb hálózati felügyeleti szoftver alkalmazásának hiányában.

VEZETÉK NÉLKÜLI HÁLÓZATI ESZKÖZÖK TELEPÍTÉSE

A hálózati témakör 24. moduljában már ismertetésre került néhány wifi eszköz telepítési alaplépés, az alábbiakban konkrét vizsgáljuk meg azokat a lépéseket melyeket a wifi eszközök telepítési és üzemeltetési feladatkörébe tartoznak. Az eszközök gyártójától, típusától függően igen sokféle eltérés vagy változat jöhet szóba a telepítés vagy üzemeltetés feladatkörét tekintve, ezért néhány tipikus megoldást, villantunk fel.

Az informatika világában alapvető feladat az új eszközök használatba vétele előtt a készülékekhez biztosított gyári leírások áttanulmányozása, értelmezése vagy a készülék üzemeltetése során felmerülő kérdések megválaszolásához a szükséges műszaki leírások felkutatása.

1. Access point, Wifi router használata

A készülék üzembehelyezése

- Az eszközök elhelyezésénél gondosan, körültekintően kell eljárni figyelembe véve azokat a körülményeket melyek befolyásolhatják a készülékhez történő rádiófrekvenciás hozzáférés lehetőségét. Találja meg a megfelelő pontot ahova biztonságosan elhelyezhető a készülék. A legmegfelelőbb helye az AP(Elérési Pontnak) az a rádiós hálózat középpontja, olyan helyen, ahol minden vezeték nélküli eszköz a hatósugarába kerülhet.
- Állítsa be az antenna irányát. Igyekezzen olyan módon beállítani az antenna irányát, hogy a lehető legjobb vételi lehetőséget biztosítson a tervezett lefedettségi területen. Normális esetben minél magasabbra helyezi az antennát, annál jobb lesz a teljesítménye. Az antenna helyzete befolyásolja a vétel minőségét.
- Csatlakoztasson egy standard Ethernet kábelt az Elérési Ponthoz. A kábel másik végét egy switchhez vagy routerhez. Ily módon az Ön Elérési Pontja csatlakoztatva van a 10/100-as hálózathoz.
- Csatlakoztassa az áram-hálózati adaptert az Elérési Pont POWER csatlakozójához. Csak azt az adaptert használja amelyet az Elérési Ponttal együtt kapott csomagban.

Előlap információ forrásai:

Általában minden AP-n megtalálhatók olyan sorszámozott LED-ek melyek a hátlapon lévő, megfelelő portokról adnak visszajelzést. Kétféle funkciójuk van: ha a LED folyamatosan világít, a router az adott porton keresztül megfelelően csatlakozik egy eszközhöz. A villogó LED pedig azt jelzi, hogy az adott porton hálózati adatforgalom van.

- Power LED: akkor világít, ha a router áram alatt van. Ez a LED akkor villog, amikor minden bekapcsolás után a router egy önellenőrző eljárást futtat. Amikor ennek futása befejeződött, a LED folyamatosan kezd világítani.
- Wireless LED: akkor világít, amikor a router vezeték nélküli funkciója be van kapcsolva. Amikor a vezeték nélküli hálózaton adatforgalom van (a router adatokat küld vagy fogad) a LED villog.

- Internet LED: akkor világít, ha az Internet porton keresztül a kapcsolat felépült. A LED akkor villog, ha az Internet porton keresztül adatforgalom van.

9. ábra AP előlap

A WIFI beállítási feladatai:

IP cím: A hálózati tervdokumentáció alapján a hálózaton belül a készülék egyedi azonosítására szolgál.

Alhálózati Maszk : azonos kell legyen az Ethernet hálózat hasonló címével.

Átjáró: Ez a cím meg kell egyezzen azzal az átjáró címmel amely a helyi hálózat és az Internet között áll fenn.

Channel: Itt választhatja ki a megfelelő csatornát, amelyen a vezeték nélküli hálózati eszközei kommunikálni fognak. A hálózatban lévő azon eszközök, melyek között a kommunikációt biztosítani szeretnénk azonos csatornát kell, hogy használjanak !

A vezeték nélküli hálózat alapértelmezett nevének beállítása (SSID-jét) :A vezeték nélküli hálózatok a gyártó által beállított, alapértelmezett névvel (más néven SSID-vel) rendelkeznek. Ez maga a hálózat neve, ami maximum 32 karakter hosszú lehet. Pl. a Linksys termékek alapértelmezett SSID-je a linksys. Az első lépés mindenképen az, hogy változtassa meg ezt az alapértelmezett nevet egy egyedi azonosítóra. Kerülni kell az olyan nevet, amely valamilyen személyes adatot tartalmazza, hiszen ez a név mindenki számár látható lehet, amikor vezeték nélküli hálózatot keres.

Alapértelmezett jelszó : A vezeték nélküli hálózati eszköz egy jelszó megadását várja, amikor beállításait módosítani szeretné. Általában az intelligens wifi eszközök egy alapértelmezett, gyárilag beállított jelszóval rendelkeznek. Pl. a Linksys termékek gyári jelszava: **admin.** Az illegális hálózati csatlakozást keresők megpróbálhatnak ezzel az alapértelmezett jelszóval belépni, és ha ezt nem cseréli le, megváltoztathatják az alap beállításait. Alapvető biztonsági kérdés, hogy ezt a gyári jelszót mihamarabb meg kell változtatni.

MAC cím szűrés : Tipikus védelmi szolgáltatás a MAC (fizikai) cím szűrési funkció , amely egy az eszközhöz rendelt MAC cím figyelését illetve azonosítását jelenti. (Fontos tudni, hogy mint az egyéb más wifi védelmi eljárás, ez sem ad tökéletes védelmet, hiszen léteznek már olyan szoftverek, melyek a MAC cím klónozás(másolás) módszerével egy ismert MAC cím "bőrébe bújva" intéznek támadást.)

Titkosítás bekapcsolása : A titkosítás a hálózaton terjedő adatok védelme érdekében fontos eljárás. A Wi-Fi Protected Access (WPA/WPA2) a Wired Equivalency Privacy (WEP) titkosítási eljárások a vezeték nélküli kommunikáció elterjedt biztonsági megoldásai. A WPA/WPA2 titkosítási eljárást használó vezeték nélküli hálózatok biztonságosabbak, mint a WEP-pel védettek, mert a WPA/WPA2 eljárás a titkosításhoz dinamikus kulcsot használ. Az AP-n átmenő adatok biztonsága érdekében használja az eszköz által felkínált, legmagasabb biztonsági szintet képviselő eljárást amit a készülék még ismer. A WEP egy régebbi titkosítási eljárás, amelyet csak abban az esetben érdemes használni, ha a hálózatban olyan eszközök is vannak, amik nem támogatják a WPA -t.

A hálózati biztonság növelésének lehetőségei

A vezeték nélküli hálózatok biztonsági eljárásai semmit sem érnek, ha a szolgáltatást igénybe vevő eszközök, munkaállomások nem biztonságosak.

- Minden munkaállomást védjük külön jelszóval.

A különlegesen fontos, kiemelt kockázatot jelentő fájlokat külön is védjük jelszóval. A Jelszavait rendszeresen változtassa meg.

- Használjon antivírus és személyes tűzfal programokat.

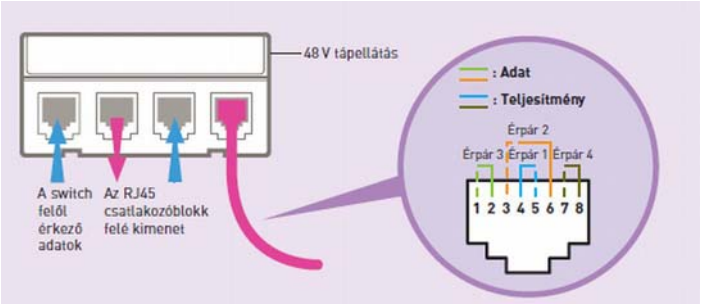
2. POWER OVER ETHERNET INJEKTORRAL MŰKÖDŐ WI-FI HOZZÁFÉRÉSI PONT

A PoE, (Power over Ethernet] technológia alkalmazása olyan esetekben merül fel amikor az eszközök pl. wifi AP-k olyan körülmények között kell, hogy működjenek ahol az eszköz hálózati táplálása nem megoldott. Pl. túlságosan távol van az eszköztől a hálózati táplálás lehetősége, olyan helyre kellett felszerelni az AP-t (elsősorban a rádiófrekvenciás jelterjedés miatt) ahová már nem volt megoldható a tápfeszültség eljuttatása.

Tehát a PoE egy olyan technológia, amely lehetővé teszi a készülékek számára, hogy a működésükhöz szükséges áramot az Ethernet csavart érpáras kábelt használó adathálózaton keresztül kapják.

A hozzáférési pontokba integrált POE Modul lehetővé teszi, hogy egyetlen kábellel lássuk el az RJ45-ös csatlakozóaljzatot és a WiFi hozzáférési pontot is. Az Ethernet kapcsolat segítségével lehetővé válik, hogy 12 hozzáférési pontig a csavart érpáron 48 Volt és adat kerüljön továbbításra.

A Legrand hálózati rendszerei között található olyan megoldás, amely az RJ45-ös csatlakozóaljzaton keresztüli hálózati táplálást biztosítja.



10. ábra PoE kilépési pont bekötése[1]

A PoE kilépési pontján a csavart érpár szállítja az információt és a tápfeszültséget (48 V) annak érdekében, hogy a hozzáférési pontot árammal, illetve adattal is ellássa.

Ha a LAN hálózaton keresztül nem lehetséges energiaellátás [PoE, Power over Ethernet], akkor tápegységet kell használni.

A kommunikációs igények fokozatos növekedése mellett a PoE lehetővé teszi, hogy a VoIP igényeinek is megfeleljünk.

TANULÁSIRÁNYÍTÓ

1. A "Szakmai információtartalom" (tananyag) részben leírtak feldolgozását kezdje azzal, hogy felméri az oktatási intézményében működő wifi eszközöket.

2. A felmérés térjen ki a wifi hálózat hatótávolság, adatátviteli sebesség, hálózati kapacitás, mozgási (roaming) lehetőség és szolgáltatásminőség tulajdonságokra.

3. A felmért eszközök működési paramétereiről, műszaki jellemzőiről gyűjtsön adatokat az internetről. Konzultáljon a szakmai tanárával, hogy a wifi hálózat hatókörének kiterjesztésére milyen igények merültek már fel.

4. Tegyen javaslatot arra az eszközre, amely megoldja a megfogalmazott igényt, határozza meg a legmegfelelőbb technológiát és az AP helyét.

A szakmai információtartalom feldolgozása után a következő feladatok elvégzésére kell felkészültnek lennie:

[1] Forrás : Legrand katalógus

- Megismeri és értelmezi az elkészült hálózati tervdokumentációt
- Azonosítja az adatátviteli hálózati berendezéseket a hálózati tervdokumentáció alapján
- A hálózati tervdokumentáció szerint elvégzi az egyes elemek csatlakoztatását
- Meggyőződik a hálózati csatlakozási pont működőképességéről.
- Teszteli a csatolókártyán csatlakoztatott perifériás eszközök üzemképességét, működési paramétereit
- Teszteli az alaplapi integrált eszközök közül a hálózati eszközöket, a működési jellemzőkre vonatkozó ellenőrzést végez.

Ha valamelyik feladat elvégzéséhez szükségét érzi, olvassa újra a tananyagot, illetve ha nem talált kellő mennyiségű ismeretet az ajánlott szakirodalomban, keressen további információt.

ÖNELLENŐRZŐ FELADATOK

1. feladat

Sorolja fel azokat a lépéseket amelyek nélkülözhetetlenek egy biztonságos AP telepítése során.

MEGOLDÁSOK

A címelem tartalma és formátuma nem módosítható.

1. feladat

- Alapértelmezett értékek megváltoztatása , SSID , jelszó megadása
- Hitelesítés beállítása
- Titkosítás beállítása
- MAC cím, forgalom szűrés beállítása

IRODALOMJEGYZÉK

FELHASZNÁLT IRODALOM

Joseph Davies: Biztonságos vezeték nélküli hálózatok, Microsoft Windows alatt az IEEE 802.11 szabvány szerint . Szak kiadó 2005.

AJÁNLOTT IRODALOM

www.Cisco.com

www.linksys.hu

A(z) 1174-06 modul 026-os szakmai tankönyvi tartalomeleme felhasználható az alábbi szakképesítésekhez:

A szakképesítés OKJ azonosító száma:	A szakképesítés megnevezése
33 523 01 1000 00 00	Számítógép-szerelő, -karbantartó

A szakmai tankönyvi tartalomelem feldolgozásához ajánlott óraszám:
15 óra

A kiadvány az Új Magyarország Fejlesztési Terv
TÁMOP 2.2.1 08/1-2008-0002 „A képzés minőségének és tartalmának fejlesztése” keretében készült.
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Kiadja a Nemzeti Szakképzési és Felnőttképzési Intézet
1085 Budapest, Baross u. 52.
Telefon: (1) 210-1065, Fax: (1) 210-1063

Felelős kiadó:
Nagy László főigazgató