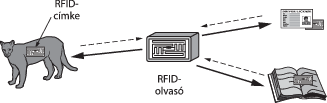
**Az RFID és a szenzorhálózatok**

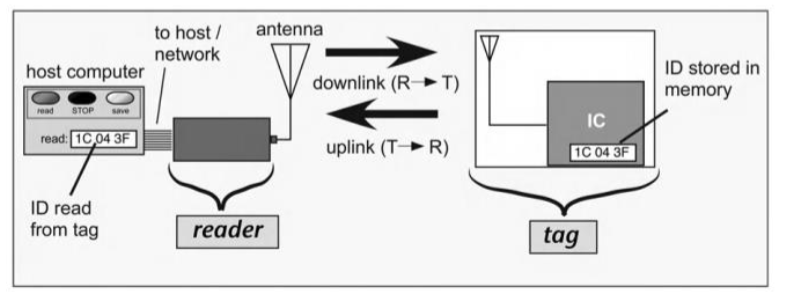
A **rádiófrekvenciás azonosítással** (**Radio Frequency IDentification –** **RFID**) a mindennapi tárgyak is részévé válhatnak egy számítógép-hálózatnak.

Egy RFID-címke (RFID tag) úgy néz ki, mint egy postai bélyeg méretű matrica, ami felragasztható (vagy beépíthető) egy tárgyra, hogy azt követni lehessen. Az objektum lehet egy tehén, egy útlevél, egy könyv vagy egy raklap is. A címke egy egyedi azonosítóval ellátott kis mikrochipből és egy antennából áll, mely a rádiófrekvenciás jeleket veszi. A követési pontokon telepített RFID-olvasók megtalálják a címkéket, amikor azok az olvasók hatósugarába érnek, és lekérdezik a bennük tárolt információt azonosságellenőrzését, az ellátási lánc kezelését, időmérést versenyeken, valamint a vonalkódok felváltását.

Több típusa is van az RFID-nak, és mindegyik különböző tulajdonságokkal rendelkezik, a legtöbb RFID-címkének nincs szüksége sem elektromos csatlakozóra, sem akkumulátorra. Ehelyett a működésükhöz szükséges összes energiát az RFID-olvasóból jövő rádióhullámok formájában kapják meg. Ezt a technikát **passzív RFID**-nak nevezzük, hogy megkülönböztessük a (kevésbé gyakori) **aktív RFID**-tól, amelynél a címkének van saját áramforrása.

**1.36. ábra - Az RFID hálózatba köti a mindennapi objektumokat**





Az RFID gyakori formája az **UHF RFID** (**Ultra-High Frequency RFID –** **ultranagyfrekvenciás**vagy **ultrarövidhullámú RFID**). Raklapokon és bizonyos jogosítványokon használják. A címkék több méterről is képesek kommunikálni azáltal, hogy megváltoztatják az olvasó jelének visszaverődését, és az olvasó venni tudja ezt a visszavert jelet. Ezt a működési módot **visszaverődésnek** (**backscatter**) nevezik.

Egy másik népszerű típus a **HF RFID** (**High Frequency RFID –** **nagyfrekvenciás** vagy **rövidhullámú RFID**). Ez 13,56 MHz-en működik, és valószínűleg ezt találhatjuk meg egy útlevélben, hitelkártyában, könyveken és érintésmentes fizetési rendszerekben. A HF RFID hatótávolsága rövid, jellemzően legfeljebb egy méter, mert a fizikai elve az ***indukción*** alapul a visszaverődés helyett. Léteznek még további RFID-típusok is, melyek más frekvenciákat használnak, például az **LF RFID** (**Low Frequency RFID –** **kisfrekvenciás**vagy **hosszúhullámú RFID**), amelyet még a HF RFID előtt fejlesztettek ki, és állatok nyomon követésére használtak. Valószínűleg ilyen típusú RFID-t találnánk meg a macskánkban.

**Szenzorhálózatok:**

Szenzorcsomópontok kis számítógépek, gyakran mindössze kulcstartónyi méretben, melyek érzékelőkkel rendelkeznek a hőmérséklet, a rezgés és más környezeti tulajdonságok mérésére. Sok csomópontot helyezünk el a vizsgálandó környezetbe. Jellemzően saját tápforrással rendelkeznek, de energiához juthatnak a napból vagy a mozgásukból is. Mint az RFID esetében, az elégséges energia biztosítása itt is kulcskérdés, és a csomópontoknak nagy odafigyeléssel kell kommunikálniuk ahhoz, hogy az érzékelőikkel rögzített információt el tudják juttatni egy külső gyűjtőpontba. A megszokott stratégia az, hogy a csomópontok önszerveződő hálózatot alkotnak, és továbbítják egymás üzeneteit, ahogy az 1.37. ábra is mutatja. Ezt a fajta rendszert **többugrásos hálózatnak** (**multihop network**) nevezik.

A szenzorhálózatokat azért telepítik, hogy a fizikai világ bizonyos paramétereit monitorozzák. Eddig nagyrészt csak tudományos kísérletezéshez használták ezeket, például madarak élőhelyének, vulkanikus tevékenységeknek, zebrák vándorlásának a megfigyelésére, de az üzleti felhasználásukra sem kell már sokat várnunk: használhatók lesznek az egészségügyben, berendezések rázkódásának felügyeléséhez vagy fagyasztott, hűtött, illetve romlandó termékek útjának követésére.

**Bluetooth:**

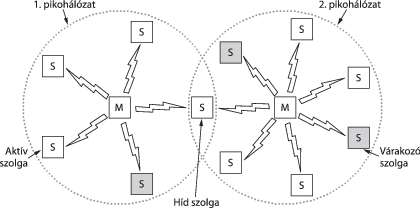
Az Ericsson 1994-ben indította el azt a fejlesztést, hogy mobiltelefonjait hogyan lehetne más eszközökkel (például laptopokkal) vezetékek nélkül kapcsolatba hozni. Tehát olyan vezeték nélküli szabvány kidolgozása volt, amely lehetővé teszi a számítástechnikai eszközök, kommunikációs eszközök és egyéb kiegészítők összekapcsolását rövid hatósugarú, kis teljesítményű, olcsó rádiós adó-vevők segítségével. A projekt a **Bluetooth** nevet kapta.

Jelenleg már mindenféle elektronikus eszköz használja a Bluetooth-t, a mobiltelefonoktól és a laptopoktól a fejhallgatókig, nyomtatókig, billentyűzetekig, egerekig, játékkonzolokig, karórákig, zenelejátszókig, navigációs eszközökig és így tovább. A Bluetooth-protokoll lehetővé teszi ezeknek az eszközöknek, hogy felderítsék egymást és egy **párosítás** (**pairing**) nevű folyamat keretében egymáshoz csatlakozzanak, és biztonságosan vigyenek át adatot.

**A Bluetooth felépítése**

A rendszer alapegysége a **pikohálózat**(**piconet**), mely egy mester (master) csomópontból és legfeljebb hét darab, 10 méteres távolságon belül levő aktív szolga (slave) csomópontból áll. Ugyanabban a (nagyméretű) helységben több pikohálózat is lehet egyszerre, sőt egy híd csomópont – amely több pikohálózatban is részt vesz – révén azok össze is köthetők, amint az a 4.34. ábrán is látható. Az egymással összekötött pikohálózatokat **szórt hálózatnak**(**scatternet**)is nevezik.

**4.34. ábra - Két pikohálózat összekapcsolásával egy szórt hálózatot kapunk**



A pikohálózat hét aktív szolga csomópontja mellett legfeljebb 255 várakozó (parked) csomópont lehet a hálózatban. Ezek olyan eszközök, melyeket a mester alacsony teljesítményű állapotba vitt, hogy csökkentse az akkumulátoraik igénybevételét. Várakozó állapotban egy eszköz semmit sem tehet, leszámítva a mester aktivációs vagy jelzőfény jelére való válaszadást.

A mester vezérli az órát, és eldönti, hogy melyik eszköz melyik időszeletben kommunikálhat. A kommunikáció mindig csak a mester és egy szolga között folyhat; a szolgák közvetlenül nem érintkezhetnek egymással.

A Bluetooth meghatároz konkrét támogatandó alkalmazásokat, és mindegyik számára külön protokollkészletet biztosít. Jelenleg 25 alkalmazás van, melyeket **profilnak**(**profile**) is neveznek.

Például, az interkom profil lehetővé teszi két telefon walkie-talkie-szerű összekapcsolását.

A fejhallgató (headset) és a kéz nélküli (hands-free) profilok beszédhang kommunikációt biztosítanak a fejhallgató és a bázisállomása között, és kéz nélküli telefóniára használható például autóvezetés közben.

Más profilok jó minőségű beszéd- és videofolyam átvitelére valók, mondjuk egy hordozható zenelejátszóról a fejhallgatókra vagy digitális kameráról tv-re.

Az emberi interfészeszköz (human interface device) profilja billentyűzetek és egerek számítógéphez csatlakozására valók.

Más profilok arra szolgálnak, hogy egy mobiltelefon vagy másmilyen számítógép fogadhasson képeket fényképezőgéptől vagy küldhessen képeket nyomtatóra.

Ez egy kis teljesítményű rendszer, 10 méteres hatósugárral, a 2,4 GHz-es ISM-sávban.

A sáv 79 darab, egyenként 1 MHz-es csatornára van osztva, frekvenciaugrásos szórtspektrumot használ. Lehet akár 1600 ugrás másodpercenként az időszeletek felett 625 s-os tartózkodási idővel (dwell time). A pikohálózat összes csomópontja – követve a résidőzítést és a mester által diktált álvéletlen ugrási sorozatot – egyszerre végzi a frekvenciaugrásokat, kihagyja azokat a csatornákat, ahol van más rádiófrekvenciás jel. Ez a folyamat csökkenti a káros zavarást, és **adaptív frekvenciaugrásnak** (**Adaptive Frequency Hopping**) nevezik.

A kapcsolatmenedzser protokoll egy **kapcsolatnak**(**link**) nevezett logikai csatornát állít fel, hogy kereteket vigyen át a mester és a szolga eszközök között, amelyek felfedezték egymást. Ezután egy párosítási folyamat következik, hogy mielőtt a csatornát használják, megbizonyosodjanak arról, hogy a két eszköznek megengedett az egymással való kommunikáció.

Az új, **egyszerű, biztonságos párosítási módszer** lehetővé teszi, hogy a felhasználók megerősítsék azt, hogy mindkét eszköz ugyanazt a jelszót használja, vagy hogy megfigyeljék az egyik eszközön a jelszót, és bevigyék a másikba. Ez a módszer biztonságosabb, mert a felhasználóknak nem kell választaniuk vagy beállítaniuk egy jelszót. Nekik csupán egy hosszabb, az eszköz által létrehozott jelszót kell megerősíteniük. Természetesen ez nem használható olyan korlátozott be- és kiviteli képességű eszközökön, mint egy fejhallgató.

Amint a párosítás megtörtént, a kapcsolatmenedzser protokoll felépíti az adatkapcsolatot. Felhasználói adatok szállítására két fő kapcsolattípus létezik. Az első az **SCO**-kapcsolat(**Synchronous Connection Oriented**–**szinkron összeköttetés-alapú**). Ezt valós idejű adatok esetén, például telefonos kapcsolatoknál használják. Ehhez a kapcsolattípushoz mindkét irányban egy rögzített időszeletet rendelnek. Az SCO-kapcsolatok időérzékeny természetéből adódóan a rajtuk átküldött kereteket sosem küldik újra. Ehelyett a megbízhatóság növelése érdekében hibajavítás alkalmazható.

A másik lehetőség az **ACL**-kapcsolat (**Asynchronous Connection-Less**–**aszinkron összeköttetés nélküli kapcsolat**). Ezt a kapcsolattípust a szabálytalan időközönként érkező csomagkapcsolt adatokhoz használják. A keretek elveszhetnek, ilyenkor esetleg újra kell adni azokat. Egy szolgának legfeljebb egy ACL-kapcsolata lehet a mesterével.

Bluetooth (2,4 GHz, 10 méteres hatótávolság): protokol ISM (Industrial, Scientific and Medical)

sávban működik (ezt a sávot bárki szabadon használhatja),

de nagyon kis jelteljesítménnyel

Bluetooth hálózat felépítése:

Master egységek (csak 1 lehet)

Slave egységek (aktív lehet 7, várakozó 255).

A Slaveket csak Master szólíthatja meg, egymással nem kommunikálnak.

Csak akkor küldenek adatot, ha a Master megszólítja őket.

3 kommunikációs csatorna áll rendelkezésükre.

1. Kapcsolatfelvételre szolgál (fix frekvencia)

2. Párosítás (fix frekvencia, de másik frekvencián)

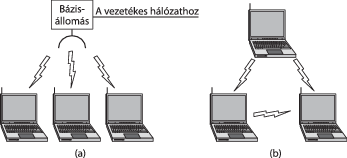
3. Adatátvitel (frekvencia ugrásos)

**Wifi**

A vezeték nélküli szabványt 802.11-nek nevezték el, ennek az egyik gyakori beceneve a **Wi-Fi.**

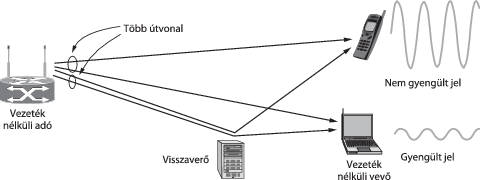
A WIFI rendszerek olyan szabadon felhasználható sávokban működnek, mint az **ISM** (**Industrial, Scientific and Medical –** **ipari, tudományos és orvosi**) sávok (például 902–928 MHz; 2,4–2,5 GHz; 5,725–5,825 GHz). Ezt a spektrumot bármilyen eszköz használhatja, ha betartja azt a szabályt, hogy úgy korlátozza az adó teljesítményét, hogy más eszközök is működhessenek a környezetében. Természetesen ez azt is jelenti, hogy a 802.11 rádióknak esetleg vetélkedniük kell a vezeték nélküli telefonokkal (cordless phones), garázsajtó-nyitókkal és mikrohullámú sütőkkel.

A 802.11 hálózatok alkotóelemei a kliensek, például noteszgépek és mobiltelefonok, valamint az épületben elhelyezett **AP**-k (**Access Point –** **hozzáférési pontok**). A hozzáférési pontokat gyakran nevezik **bázisállomásnak**(**base station**) is. A hozzáférési pont a vezetékes hálózathoz csatlakozik, és a kliensek közötti összes kommunikáció egy-egy hozzáférési ponton keresztül zajlik.



A 802.11 adatátvitelt nehezíti, hogy a vezeték nélküli átviteli feltételek a környezet legkisebb változásával is módosulhatnak. A 802.11 által használt frekvenciákon a rádiójeleket a szilárd testek visszaverhetik, így a jelek (több útvonal mentén) többször is megérkezhetnek a vevőhöz. A visszhangok kiolthatják vagy felerősíthetik egymást, a vett jel nagyfokú ingadozását okozva. Az így létrejövő interferencia jelenség az úgynevezett **többutas terjedés miatti jelgyengülés** vagy **féding**(**multipath fading**), mely az 1.34. ábrán figyelhető meg.

**1.34. ábra - Jelgyengülés többutas terjedés esetén**



Az információt több, független útvonalon történő elküldése.

Mivel a vezeték nélküli technológiák természetüknél fogva adatszórásos átviteli közeggel dolgoznak, a 802.11-es rádióknak is meg kell küzdeniük azzal a problémával, hogy az egy időben küldött adások ütközni fognak, ami zavart okozhat a vételben. Ennek a problémának a kiküszöbölésére a 802.11 a **CSMA**- (**Carrier Sense Multiple Access –** **vivőjel-érzékeléses többszörös hozzáférés**) módszert használja, mely a klasszikus vezetékes Ethernetből vesz ötleteket.

Az adás megkezdése előtt a számítógép mindig vár egy rövid, véletlenszerű hosszúságú ideig, és elhalasztja az adást, ha azt hallja, hogy valaki más már éppen ad. Ezzel a módszerrel sokkal kisebb a valószínűsége annak, hogy két számítógép egyszerre adjon. Mindazonáltal ez mégsem működik annyira jól, mint a vezetékes hálózatok esetében.

Minden ütközés után a küldő egyre hosszabb, de továbbra is véletlenszerű hosszúságú időt vár, majd újraküldi a csomagot. Ennek és más nehézségek ellenére a gyakorlatban elegendően jól működik ez a módszer.

**Biztonság.**

Mivel a vezeték nélküli adás adatszórással történik, a közelben levő számítógépek könnyen megkapják a nem nekik szánt csomagokat. Ennek megelőzésére a 802.11 szabvány egy titkosító eljárást is tartalmazott, melyet **WEP** (**Wired Equivalent Privacy –** **vezetékessel egyenértékű titkosság**) néven ismerhetünk. A titkosító eljárás hibás volt, és hamarosan fel is törték. Azóta újabb, eltérő kriptográfiai módszereket alkalmazó algoritmusok váltották fel a 802.11i szabvány formájában, melyet **Wi-Fi Protected Access** (**Wi-Fi védett hozzáférés**) névvel is illetnek (kezdetben ez a **WPA** volt, de mára a **WPA2** leváltotta).

WIFI:

vezetéknélküli szabvány elnevezése (a szabvány: 802.11)

Szintén ISM sávokban működik(900MHz, 2,4GHz, 5,7GHz)

Felépítése:

1. Bázisállomás/Access Point (hozzáférési pont)

kapcsolódik a vezetékes hálózathoz

2. Kliensek vezeték nélküli kapcsolattal csatlakoznak hozzá.

Mikrohullám az adatátviteli frekvencia tartomány, ezért mikrohullámok

fizikai jellemzői miatt (részben elnyelődik, részben visszaverődik):

többutas terjedés lesz. Bizonyos tárgyakról visszaverődik a jel, interferencia jelenség

lép fel a másik elektromágneses hullámmal (kioltják egy mást,

torzul a jelalak), gyengül a jel

Versenyhelyzet: amikor több adó egyidőben/egyszerre szeretne adni, elnyomják egymást.

Ennek a problémának a kezelésére találták ki a CSMA protokollt.

CSMA (Carrier Sense Multiple Access) protokoll:

Ha érzékelik az adók, hogy többen is adtak egy időben, akkor véletlen

ideig várakoznak és akkor újra megpróbálnak adni.

Biztonság:

titkosított a WIFI elérése, mind a információ, mind a hozzáférés miatt.

WEP - nagyon könnyen feltörték

WPA2 a jelenlegi titkosítás