Traadita kohtvõrk (Wireless Area Network)

Traadita kohtvõrgu komponendid

Kohtvõrgu loomiseks on hädavajalik **lõppkasutajale mõeldud riistvara** tööjaamad, kaasaskantavad arvutid, pihuarvutid jne. Need sisaldavad endas kasutaja ja võrgu vahel paiknevat **tarkvara**. Viimane sõltub suuresti sellest, millises võrgu osas arvuti paikneb. Kõige olulisemat rolli mängib siin kõrgetasemeline personaalarvuti, kuhu on installeeritud võrgutoetusega operatsioonisüsteem. Kõige lihtsamatel juhtudel töötab sama arvuti ka juurdepääsupunktina, võimaldades erinevatel traadita kohtvõrgu adapterit omavatel tööjaamadel võrguteenuseid kasutada. Esineb olukordi, kus server ise ei tegutse juurdepääsupunktina. Säärasel juhul on vajalik lüüside kasutamine. Lüüsarvuti ise, mis on varustatud vahevara, võib tööjaamadega info vahetuseks kasutada mitte TCP/IP-d, vaid mõnda traadita võrgu jaoks sobivamat protokollistikku. Pealegi esineb säärases võrgus aeg-ajalt sidekatkestusi, mis lüüside olemasolul serverile nähtamatuks jäävad. Vähem oluline pole ka asjaolu, et säärase lahenduse kasutamisel ei pea terminal ühenduse avatuna hoidmiseks "eluspüsimise" pakette saatma. Sellega tegeleb lüüsarvuti ise.

Et luua toimiv traadita kohtvõrk, peavad kõik tööjamad olema varustatud sobiva **võrgukaardi** ja **antenniga**. Viimast iseloomustatakse väljundvõimsuse, ribalaiuse ja levisuunaga. Levisuund määrab omakorda katteala. Mitmesuunaline antenn saadab kiirgust välja igas suunas. Suundantenni korral on aga signaali tugevus sama võimsuse korral märksa suurem. Võimsus ja signaali tugevus määravad maksimaalse levikauguse. Traadita võrkude korral on saatevõimsus suhteliselt väike, alla ühe vati.

Ribalaiuseks nimetatakse seda sagedusspektri osa, mida signaal levimiseks kasutab. Näiteks on telefonisüsteemi ribalaius jämedates piirides 0 ja 4 KHz vahel. Samas ei saa unustada, et bitikiirus ja ribalaius on üsnagi tihedalt seotud. Mida suurem on bitikiirus seda suuremat riba on tööks vaja.

Traadita kohtvõrgu probleemid

Interferents

Läbi õhu loodud sidekanalit võivad mõjutama hakata nii atmosfääris esinevad looduslikud mürad kui ka teiste samalaadsete süsteemide poolt õhku paisatav kiirgus. Säärast nähtust, kus signaalid üksteist mõjutavad, nimetatakse interferentsiks. Viimane võib olla kahesugune: suunaga sissepoole, mille korral TKV-s võivad ilmneda harmoonilised signaalid, tekitatuna sellesama TKV poolt. Samuti võivad esineda erinevad häired, mis on põhjustatud näiteks mikrolaineahjudest, mis töötavad samas sagedusvahemikus (S-ribas e. 2,4 GHz) nagu TKV-gi. Säärasel juhul on takistatud signaalide saatmine/vastuvõtt selles TKV-s, lisaks võivad ilmneda mitmesugused bitivead saatel või vastuvõtul.

Samas võib aga TKV mõjutada teisi töötavaid süsteeme (interferents suunaga väljapoole). Viimane võib põhjustada mitmeid probleeme, kuna kannatada võivad olulised sidekanalid.

Interferents on tundmatu nähtus avalikult laialipihustatud spektris, sest võimused seal on alla ühe vati ja seadmed peavad olema üksteisele väga lähedal.

Energiatarbimine

Võrgukaardid on suhteliselt suure voolutarbega ja seetõttu tuleb kaasaskantava arvuti kasutamisel suhteliselt tihti akusid laadida. Probleemi leevendamiseks ei hoita saatjat kogu aeg töös, vaid see

lülitatakse sisse vaid juhul, kui süsteemi poolt antakse korraldus info saateks. Valmisolekuresiim vähendab voolutarbimist kuni poole võrra.

Omavaheline sobivus

On ülimalt oluline, et erinevate firmade toodang omavahel kokku sobiks ja töötava süsteemi moodustaks. Seetõttu on välja töötatud standard IEEE 802.11, mis peaks omavahelist ühilduvust suurendama ja tagama erinevate komponentide koostöö.

Võrguturve

TKV-s on paratamatu, et signaal levib väljapoole TKV-d haldava organisatsiooni piire. Väljaspool on aga juba võimalik pealtkuulamise teel kätte saada enamik võrgus liikuvat informatsiooni. Loomulikult peab sissetungijal olema konkreetsele võrguosale juurdepääsuõigus.

Samuti on võimalik ka nö. "elektroonne sabotaaž": keegi võib sihilikult püüda halvata TKV töö, keelates teistel selle kasutamise. Asi on nimelt selles, et kui üks tööjaam andmeid saadab, peavad teised ootama. Seega võib keegi tuua TKV-sse tööjaama, mis pidevalt ainult andmete saatmisega tegelebki, sundides kõiki ülejäänuid ootama. Probleemid on lahendatavad, kui lubada ligipääsu vaid kindlatele tööjaamadele. Enamik TKV-sid nõuab igas tööjaamas teatava võrgukoodi paigaldamist; alles seejärel on võimalik selles TKV-s liikuvaid andmeid "kuulata".

Ühendusprobleemid

Ühendusprobleemid tekivad, kui kasutada traadita kohtvõrgus sama protokollistikku, mis tavalises kohtvõrguski. Näiteks kipub TCP/IP-baasil loodud TKV-s ühendus katkema. Eriti ilmneb see olukordades, kus terminal asub katteala piiril. Suurem probleem on isegi adresseerimine. Tänu TKV-le on terminalid mobiilsed ning ühest alamvõrgust teise liikudes ei pruugi nad enam võimelised olema ühendust jätkama.

Paigaldamine

Kohtvõrgu loomisel tuleb arvestada mitmete erinevate faktoritega. Seinad, laed ja muud füüsilised objektid põhjustavad signaali sumbumist. Seega tuleks enne TKV paigaldamist kindlasti läbi teha erinevad levitestid. Samuti võivad süsteemi tööd mõjutada lähedalasuvad raadiojaamad ja muud saateseadmed. Samuti ei saa märkimata jätta, et TKV võib ise häirida teiste süsteemide tööd.

Tervis

Pole võimalik üheselt öelda, kas TKV on tervisele kahjulik või mitte. Siiski on teada, et TKV peaks olema turvalisem kui enamik mobiiltelefone, sest tema töövõimsus jääb 50 ja 100 mW vahele, samal ajal kui mobiiltelefoni väljundvõimsus jääb 600 mW ja 3 vati vahele.

Raadiosidel põhinev TKV

Kasutab andmete edastamiseks raadiosidel põhinevat tehnoloogiat, moduleerides signaali vastavalt andmetele ja kiirates seda teataval töösagedusel vabasse ruumi.
Süsteemi positiivseks küljeks on võimalus ühendada omavahel otsenähtavusest väljas olevaid kasutajaid. Samuti levib raadiosignaal väikese sumbumise hinnaga läbi takistuse (seinad ja laed).

Samas võib aga tekkida häireid teiste samalaadsete seadmete töös, seda eriti juhul, kui vastavaid eelnevaid uuringuid tehtud ei ole. Loomulikul on raadioside puhul alati olemas pealtkuulamisoht, mida annab muidugi vältida, kasutades näiteks signaali eelnevat kodeerimist.

Kuna tegemist on raadiosidega, eraldatakse TKV jaoks kindlad sagedusvahemikud, milles võrk pakette üle kanda võib. Ameerikas kasutatakse kolme vahemikku: 902–928 MHz (e. 26 MHz riba); 2,40–2,4835 GHz (e, 83,5 MHz riba) ja 5,725–5,850 GHz (e. 125 MHz riba). Mujal maailmas on kasutusel 2,4 GHz vahemik.

Andmete edastamine traadita kohtvõrgus on sarnane ISO avatud süsteemide mudelile. Ka siin esineb nn. füüsiline kiht, millel toimub andmeülekanne. Samas on aga ka traadita kohtvõrgus hoolitseda sünkroniseerimise ja pakettide veaparanduse eest. Viimastega tegeleb ISO-OSI mudeli teine kiht, mis IEEE 802.11 standardi kohaselt on nimetatud meedia juurdepääsu kontrollkihiks. Tänu viimasele on võimalik ühte meediat jagada mitme erineva terminali vahel. Pakettide eduka kohaletoimetuse eest vastutab kandevsageduse jälgimise protokoll. Just see protokoll on vastutav, et andmeid edastab vaid üks arvuti korraga; teised masinad peavad ootama sageduse vabanemist. Tööjaamad teostavad ka pidevat vigadekontrolli, kui paketis vigu ei esine, saadetakse lähtepunkti tagasi kinnitus; kui avastati viga, vastutab samuti kandevsageduse jälgimise protokoll paketi uuestisaatmise eest.

Andmeülekanne laialipihustatud spektris

Andmeülekanne ise on ISO-OSI mudeli kohaselt esimese, ehk füüsilise kihi ülesanne. Laialipihustatud spektri korral “paisatakse” signaal üle laiema sagedusriba. Säärase moduleerimisviisi kõige suuremaks miinuseks on riba raiskamine, kuid samal ajal on signaal märksa vähem tundlikum mitmetele elektrilistele müradele. Müra mõjutab vaid väikest osa kasutatavast ribast, põhjustades vaid väheseid bitivigu signaali demodulatsioonil.

TKV-s kasutatakse kahte laialipihustatud spektriga moduleerimisviisi: hüpleva sagedusega ja otsejärjestusega.

Hüpleva sagedusega laialipihustatud spekter

Hüpleva sageduse korral toimub signaali moduleerimine kandevsagedusega, mis “hüppab” ühelt sageduselt teisele. Hüplemise järjekord ei ole juhulik, see on määratud hüplemiskoodiga. Loomulikult peab korrektse vastuvõtu tagamiseks vastuvõtja samuti sama hüplemiskoodi kasutama, et kuulata vastavat sagedust täpselt õigel ajahetkel. Standardite kohaselt peavad tootjad kasutama 75 või enamat sagedust ühe kanali kohta. Samuti on määratud ka nn. paiksusaeg — 400 ms. Paiksusaeg näitab, kui kaua võib andmeid ühel sagedusel (ehk kahe hüppe vahel) edasi kanda.

Kui ülekandemehhanism avastab signaali ülekandel teataval sagedusel segavad signaalid, kordab ta saadet teisel sagedusel uuesti.

Kasutades seda tehnikat, on võimalik ühel sagedusel tööle panna mitmeid erinevaid saatjaid tingimusel, et kasutataks erinevaid hüplemiskoode. Koodide kogumit, mille tulemusena erinevad jaamad ei saada mitte kunagi pakette ühel sagedusel (s.t. nende hüplemiskoodid ei kattu kunagi) nimetatakse ortogonaalseks koodide kogumiks.

Maksimaalne andmeedastuskiirus hüpleva kandevsagedusega moduleerides jääb alla 2 Mb/s.

Otsejärjestusega laialipihustatud spekter

Antud juhul ei kasutata hüplevat kandevsagedust, vaid signaali moduleeritakse spetsiaalse bitijärjestusega, mida nimetatakse šifreerimiskoodiks. Minimaalne kood on 10, tavaliselt kasutatakse koodi 20. Esialgsed andmebitid asendatakse vastavustabeli alusel uutega.

Kitsaribaline modulatsioon

Andmete ülekandmiseks võib kasutada ka kitsaribalist modulatsiooni, mis on analoogne teiste raadiosideseadmete tööga. Sellisel juhul suunatakse kogu saatevõimsus kitsasse sagedusvahemikku. Tulemuseks on sagedusriba äärmiselt efektiivne kasutamine, samas võib aga väiksemgi müra hävitada kogu signaali. Et seda ei juhtuks, on vajalik kitsaribalise modulatsiooni korral vastava litsentsi olemasolu. Litsentsi saajale antaks tagatis, et keegi teine ei tööta lähikonnas samal sagedusel. Kui see aga peakski juhtuma, on juba vastavate organisatsioonide ülesanne probleem lahendada.

Infrapunasel valgusel põhinev TKV

Infrapunavalgus kasutab sagedusi, mis on madalam kui spektrivärvidel, kuid samal ajal siiski kõrgem raadiolainete sagedusest. Selle klassi tooted töötavad 820 nm lainepikkuse juures, kuna sellel lainepikkusel on õhus sumbumine kõige väiksem. Kuna infrapunane valgus ei levi läbi seinte, on tagatud pakettide levimine vaid hoone sees. Seega pole võimalik väljaspool ehitist TKV-s osaleda ja seda pealt kuulata. Samas on aga seda lahendust võimatu kasutada mobiilsete terminalide juures, kuna võrgu katteala on piiratud otsenähtavusega. Infrapunasel valgusel põhinev TKV ei karda aga teisi müraallikaid, sest nende vahel ei teki interferentsi. Maksimaalne andmeedastuskiirus selle lahenduse puhul on 1–4 Mb/s.

Infrapunavalgusel põhineva TKV riistvara koosneb kahest osast: adapterist ja kiirgurist. Viimane on sarnane raadiosidel baseeruvas TKV-s kasutatava antenniga.

Kuna infrapunast valgust on väga hästi suunatav, eristatakse hajutatud ja punkt-punkt TKV ühendust. Esimesel juhul kasutatakse signaali hajutamiseks ruumi lage, mis sel hetkel toimib peeglina. Signaal saadetakse suunaga lakke, et ta sealt peegeldudes jõuaks teise terminali vastuvõtjasse. Ka eetri jälgimine toimub laelt peegelduvate signaalide "vaatamisega". Kui peegeldusi ei ole, on eeter vaba, ja saade võib toimuda. Enne info tegelikku saatmist saadetakse siiski välja kindel koodijada, mis vastuvõtja tähelepanu tõmbab.

Punkt-punkt ühendusel korral kasutatakse andmete edastamiseks märkringi (token ring) põhimõtet, kusjuures seadmete vahekaugus võib olla maksimaalselt 75 jalga. Märkring tagab, pakettide edastamise vaid ühe jaama poolt korraga. Märk, mis tegelikult on kindel bitijada, liigub mööda ringi. Kui tööjaam soovib andmeid edastada, peab ta ootama, kuni märk temani jõuab. Alles siis on jaamal õigus andmeid välja saata. Andmed liiguvad samuti mööda ringi, mida kõik jaamad kuulavad, jõudes lõpuks vastuvõtjani, kes need ka läbi töötab. Kui andmete ülekandmine on lõpetatud, vabastab saatja märgi, andes nii võimaluse uuele tööjaamale pakettide väljasaatmiseks.

Vahelduvvooluvõrgu baasil töötav (T)KV

Andmete edastamiseks kasutatakse olemasolevat vahelduvvoolu võrku ja selle kaabeldust. Seega ei saa öelda, et tegemist on täiest traadita ühendusega, kuid kuna täiendavaid kaableid ei ole vaja paigaldada, võib seda lahendust siiski ka TKV-na vaadelda.

Kuigi võiks arvata, et vahelduvpinge hakkab signaali segama, ei vasta see siiski tõele. Põhjus on selles, et vahelduvvool kasutab teist sagedust. Paigaldatavad filtrid ei luba alla 60 Hz sagedusega võnkumisi vastu võtta. Lahendus oleks ideaalne, kuna elektrivõrgu kaudu on põhimõtteliselt võimalik "liikuda" suurte vahemaade taha, kuid elektrisüsteem sisaldab elektriliselt sidestamata osi (transformaatorid), mis omakorda toimivad filtritena kõrgemate sagedusvõnkumiste suhtes ja blokeerivad need. Seega tähendaks vahelduvvooluvõrgu baasil töötav kaugvõrk lisasildade paigaldamist alajaamadesse, mis võimaldaks transformaatoritest "mööda hiilida". Palju efektsema lahenduse annab raadiosidel põhineva võrgu kasutamine.

Andmeedastuskiirused jäävad siin 1 ja 2 Mb/s vahele.

Nii infrapunasel valgusel kui ka vooluvõrgu baasil töötavad TKV-d ei suuda siiski rahuldavaid tulemusi anda. Seetõttu on määravaks ja üldkasutatavamaks muutunud raadioside.

IEEE 802.11 topoloogia

TKV peamine ehituskivi on teenuste baaskogum (basic service set). Üks teenuste baaskogum määrab katteala, mille ulatusse jäävad tööjaamad on täielikult TKV-ga ühendatud. Jaam võib ühe teenuste baaskogumi piires vabalt liikuda, kuid niipea, kui tööjaam lahkub antud kogumist, et ole ta enam võimeline teiste baaskogumisse jäänud jaamadega vahetult suhtlema. Eristatakse veel iseseisvat teenuste baaskogumit, millel ei ole mingisugust tuumvõrku ja mis koosneb vähemalt kahest tööjaamast.

Lisaks baasteenuste kogumile eksisteerib ka teenuste laiendatud kogum, mis koosneb mitmest baaskogumist. Jaam võib liikuda ka teenuste laiendatud kogumi piires. Seega esineb kolme tüüpi liikumist:

- Mitteliikumine, kus jaam ei liigu või liigub vaid sama baaskogumi piires.
- Baaskogumiliikumine, kus jaam liigub ühest baaskogumist ühes laiendatud kogumis teise baaskogumisse samas laiendatud kogumis.
- Laiendatud kogumi liikumine, kus jaam liigub ühest baaskogumist ühes laiendatud kogumis teise baaskogumisse mõnes teises laiendatud kogumis.

Tuleb kindlasti tähele panna, et antud standard ei garanteeri ühenduse püsimajäämist laiendatud kogumi liikumise korral.

TKV võrku kuulub lisaks tööjaamadele kindlasti ka juurdepääsupunkt (access point), mis kujutab endast aadressi omavat jaama. Viimases asub levisüsteemide (distribution system) töökeskkond jaamade jaoks, mis asuvad erinevate baaskogumites. Levisüsteem ise aga ongi väravaks, mis ühendab erinevaid baaskogumeid ühes laiendatud kogumis. Ühendamine ise toimub ikkagi läbi juurdepääsupunkti. Tänu sellele jäävad üksikud teenuste baaskogumid ja teenuste laiendatud kogumid loogilise ühenduse kihi jaoks märkamatuks.

IEEE 802.11 teenused

Eristatakse tööjaamas teenuseid ja levisüsteemi teenuseid. Esimeste hulka kuuluvad

- Autentimine
  Kõik selle standardi alla kuuluvad tööjaamad peavad olema seotud teenuste baasvõrguga

või laiendatud võrguga. Enne teise jaamaga ühenduse loomist peavad nad turvalisuse eesmärgil läbima autentimisprotseduuri. Siingi eksisteerib kaks võimalust: avatud süsteemi põhine autentimine ja jagatud võtme põhine autentimine. Esimesel juhul saadab jaam, kes soovib saada juurdepääsu võrku, autentimist korraldava kaadri, mis sisaldab saatja jaama identifikaatorit. Vastuvõtja saadab tagasi kaadri teatega, kas identifikaator oli äratuntav või mitte. Teisel juhul eeldatakse, et iga jaam on saanud (väljaspool IEEE 802.11 võrku) salajase jagatud võtme. Jaamade autentimine toimub läbi salastatud võtme.

- Deautentimine
  Kui jaam soovib lõpetada ühenduse teise jaamaga, käivitatakse deautentimise teenus. See teenus kujutab endast märguannet, mida ei ole võimalik ignoreerida. Jaamad saadavad taas autentimist korraldava kaadri (või kaadrite kogumi mitmete jaamade jaoks) soovitamaks autentimisinfo kustutada.
- Privaatsus
  Privaatsusteenus, mis kehtib kõigi andmekaadrite ja mõnede autentimist korraldavate kaadrite kohta. Teenus põhineb IEEE 802.11 standardis kirjeldatud "juhtmega sarnaneva privaatsuse" (wired equivalent privacy) algoritmil, mis vähendab märgatavalt pealtkuulamisest tulenevat ohtu. Algoritm teostab nimelt teadete krüpteerimist.
- MJK teenuste andmeühikute kättetoimetamine

Levisüsteemi teenused:

- Ühendamine
  Iga jaam peab algselt käivitama juurdepääsupunktiga ühendamise teenuse. Enne seda pole jaamal võimalik levisüsteemi kaudu andmeid saata. Ühendamine kinnistab jaama konkreetse levisüsteemi külge. Tasub märkida, et juurdepääsupunkt võib olla korraga ühenduses mitme tööjaamaga, kuid tööjaam saab olla korraga ühendatud vaid ühe juurdepääsupunktiga. Ühendamine on esimene samm võimaldamaks tööjaamal liikuda ühest teenuste baaskogumist teise.
- Lahtiühendamine
  Jaam või juurdepääsupunkt peab käivitama lahtiühendamise teenuse aktiivse ühendatuse lõpetamiseks. See teenus on siiski vaid märguanne, mis tähendab, et teine osapool võib lahtiühendamisest ka keelduda. Tööjaamad peaksid end lahti ühendama enne võrgust lahkumist. Juurdepääsupunkt peaks lahtiühendamisprotseduuri käivitama enne tema hoolduseks kõrvaldamist.
- Levitamine
  Iga jaam, kes saadab levisüsteemi kaudu ükskõik milliseid meedia juurdepääsu kontrollimise kaadreid, kasutab leviteenust. 802.11 standard ei määratle üheselt, kuidas levisüsteem andmeid kätte toimetab. See teenus võimaldab levisüsteemil vaid kindlaks teha, millist teenuste baaskogumit kasutada.
- Integratsioon
  Teenus võimaldab meedia kontrollimise kaadrite vahetamist levisüsteemi ja IEEE 802.11 standardile mittevastava kohtvõrgu vahel. Integratsioonifunktsiooni ülesandeks on teostada kõik vajalikud teisendused.
- Taasühendamine
  Teenuse abil on võimalik ühenduse asukohta muuta, vahetades näiteks kasutatavat juurdepääsupunkti. Selle tulemusena on levisüsteem teadlik juurdepääsupunktide ja tööjaamade omavahelisest sidumisest tööjaama liikumisel ühest baaskogumist teise antud laiendatud kogumi piires(!). Samuti on selle teenuse abil võimalik muuta olemasoleva ühenduse parameetreid, kusjuures tööjaam jääb ikkagi seotuks sama juurdepääsupunktiga. Teenuse tellijaks on alati mobiilne jaam.

Meedia juurdepääsu kontrollimise kiht (MJK-kiht)

Juurdepääs võrku on tagatud kahel viisil: multijuurdepääsuga kandevsageduse kuulamise ja kokkupõrgete vältimisega (carrier sense multiple access with collision avoidance — CSMA/CA. IEEE 802.11 viitab sellele võimalusele kui levi koordineerimise funktsioonile) ja prioriteetidel põhineva juurdepääsuga. Viimane sisaldab konfliktidevaba juurdepääsuprotokolli, mis on kasutatav võrgulahenduste puhul, mis sisaldavad lisaks juurdepääsupunktile ka punkti koordinaatoreid. 802.11 standardis on see kajastatud kui punkti koordineerimise funktsioon.

Levi koordineerimise funktsioon (LKF) MJK kihil

Esmane ühendusi koordineeriv funktsioon, mis tagab automaatse meedia jagamise. Antud juhul kasutab MJK kiht nii füüsilist kui ka virtuaalset kandevsageduse kuulamise mehhanismi, et teha kindlaks kas eeter on vaba või ei ole. Iga füüsiline kiht annab võimaluse kanali kontrollimiseks. Kontrolli tulemused saadetakse edasi MJK kihile kui osa vajalikku informatsiooni eetri hõivatuse üle otsustamisel.

MJK kasutab samas ka virtuaalseid protokolli poolt pakutavaid võimalusi kanali seisukorra üle otsustamisel. Selle võimalus on antud kaadris asuva kestvuse väljaga. Kestvuse väli näitab jaama poolset prognoosi eetrit kasutada. MJK jälgib kestvuse välja kõigis MJK kaadrites ja asendab tööjaamas oleva võrgupaigutusvektori väärtuse suuremaga, kui see hetkel oli. Võrgupaigutusvektor sarnaneb taimerile, mille algväärtus on võrdne MJK kaadri kestvuse väljaga, hakates järjest vähenema. Kui vektori väärtus on saanud võrdseks nulliga, võib jaam hakata pakette saatma.

Virtuaalne ja füüsiline kuulamine annab piisava hulga informatsiooni kanali hõivatuse kohta. Kui hoolimata eelnevatest arvestustest on kanal ikkagi hõivatud, käivitab MJK protokoll juhuliku tagasitõmbumise algoritmi (Lisa 1)

Lisa 1.

The backoff time is calculated by the formula

```
backoff time = random() * aSlotTIme
```

Random() is a pseudo-random integer drawn from a uniform distribution over the interval [0; CW] in which CW (collision window) is an integer within the range of values of the Management Information Base (MIB) attributes aCWmin and aCWmax. The random number drawn from this interval should be statistically independent among stations. aSlotTime equals a constant value found in the station's MIB.
Actually the CW increases exponentially to minimize collisions and maximize throughput both low and high network utilizations. Under low utilization the station doesn't have to wait very long before transmitting the data. On the first or second attempt it can successfully use the medium for transmitting. If the utilization is high the protocol holds stations back for longer periods of time to avoid the probability of collisions. Under high utilization the CW increases to relatively high values. This mechanism does a good job for avoiding collisions but the stations will experience substantial delays while waiting to transmit frames

Veaparandus

Veaparandusel kasutatakse automaatset kordamise süsteemi. Et korraldada uuestisaatmiste arvu, teeb MJK koordinaator vahet pikkadel ja lühikestel kaadritel. Lühikeste kaadrite (lühemad kui MIB-i atribuut `aRTSThreshold`) uuestisaatmine toimub kuni katsete arv jõuab MIB-i väärtuseni `aShortRetryLimit`. MJK koordinaator saadab suuri kaadreid analoogiliselt, põhinedes MIB-i atribuudil `aLongRetryLimit`. Kui limiit on täis, tühistab tööjaam kaadri.

Punkti koordineerimise funktsioon (PKF) MJK kihil

Pakub konfliktivaba kaadrite transporti. Antud juhul asub punkti koordinaator juurdepääsupunktis, mis annab ülevaate kõigist kaadrite liikumisest jaamade vahel. Kõik tööjaamad jälgivad punkti koordinaatorit, seadistades konfliktivaba perioodi algul vastavalt temale oma võrgupaigutusvektori väärtust.

Konfliktivaba perioodi algul on punkti koordinaatoril võimalus saavutada eetri üle kontroll. Perioodi algul kuulab koordinaator eetrit, mille järel saadetakse välja märguandesignaal, mis sisaldab endas elementi `CF Parameter Set`. Kui jaamad märguandesignaali kätte saavad, uuendavad jaamad endas sisalduva võrgupaigutusvektori väärtust. Selle tulemusena tekitatakse konfliktivaba periood, mille käigus jaamad ei saa (tänu võrgupaigutusvektori nullist erinevale väärtusele) pakette saata.

Pärast märguandesignaali saatmist saadetakse PKF-i poolt üks järgnevatest kaadritest:

- Andmekaader, mis on suunatud ühele kindlale tööjaamale. Kui PKF ei saa vastuvõtjalt kinnitust, võib ta saata kinnitamata kaadri (pärast teatavat intervalli).
- Koordineerimise funktsiooni küsitluskaader, mis on samuti suunatud kindlale tööjaamale ning mille tulemusena see tööjaam saab õiguse saata välja ühe kaadri ükskõik millisesse sihtpunkti. Kui jaamal ei ole ühtegi kaadrit saata, on ta kohustatud edastama nullandmetega kaadri. Kui jaam ei saanud kinnitust kaadri eduka vastuvõtmise kohta, peab ta ootama uut koordineerimise funktsiooni küsitluskaadrit, et paketi saatmist korrata.
- Koordineerimise funktsiooni küsitluskaader koos andmetega. Kombineeritud kaader kahest eelmisest, mis vähendab võrgu koormust.
- Koordineerimise funktsiooni lõppkaader, millega antakse märku konfliktivaba perioodi lõppemisest TKV-s. Kaader saadetakse välja, kui muutuja `CFPFurRemaining` on aegunud või kui PKF-il pole enam ühtegi kaadrit saata ega ühtegi jaama küsitleda.

Samas on jaamadel võimalus olla küsitletav või mitte. Küsitletavust saab muuta, saates juurdepääsupunkti PKF-le taasühendamise kaadri. PKF haldab nimekirja küsitlemist lubavatest masinatest.

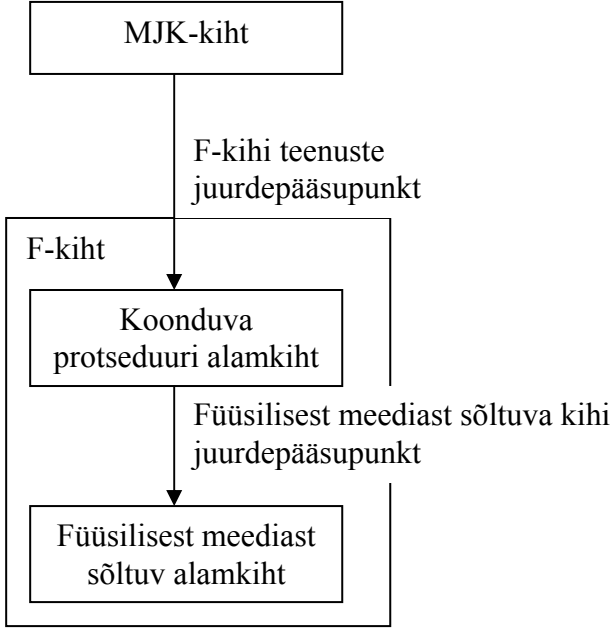
Füüsiline kiht (F)

Arhitektuur

Füüsiline kiht koosneb tegelikult mitmest erinevast alamosast, mis omavad kindlat ülesannet pakettide edastamisel:

- Füüsilise kihi juhtimine
  Pakub antud kihil juhtimis-korraldamisfunktsioone.
- F-kihi koonduva protseduuri alamkiht (PHY-layer convergence procedure sublayer)
  Meedia juurdepääsu kontrollkiht suhtleb F-kihi koonduvate protseduuridega läbi F-kihi teenuste juurdepääsupunkti. MJK-kihi korralduse peale moodustab koonduva protseduuri alamkiht MJK-protokolli andmeühikud. Samuti teostab see alamkiht eetrist tulnud andmete edasitoimetamist MJK-kihile. F-kihi koonduvad protseduurid lisavad MJK-kihi andmekaadrile täiendavaid välju, mis on vajalikud F-kihi saatjatele-vastuvõtjatele. 802.11 standardis leiab see kaader kajastamist kui F-kihi koonduva protseduuri protokolli andmeühik (PHY-layer convergence procedure protocol data unit). Kaadri struktuur võimaldab asünkroonset andmeedastust kahe jaama vahel.

- Füüsilisest meediast sõltuv alamkiht (Physical medium dependent sublayer)
  Eelmise alamkihi juhtimise all tegeleb see alamkiht otseselt kaadrite saatmise ja vastuvõtmisega. Et seda teenust pakkuda, peab see alamkiht suhtlema vahetult traadita meediumiga (s.o. õhuga) ja teostama seega vajaliku modulatsiooni-demodulatsiooni. koonduva protseduuri alamkiht ja meediast sõltuv alamkiht suhtlevad omavahel läbi vastava füüsilisest meediast sõltuva alamkihi teenuste juurdepääsupunkti.



Hüpleva sagedusega laialipihustatud spektri (HSLPS) F-kiht

- Mitte eriti kallis
- Madalaima energiatarbimisega
- Kõige taluvam mürade suhtes
- Madalaimad võimalikud andmekiirused üksikutest F-kihtidest
- Maksimaalne võimsus, kui kasutada mitut F-kihti
- Väiksem riba kui otsejärjestuse puhul, kuid siiski suurem kui infrapunast valgust kasutades

802.11 standard sätestab kanalitekomplekti, mis on jagatud üle 2,4 GHz sageduse. Kanalite arv sõltub geograafilisest asukohast. Põhja-Ameerikas ja Euroopas on see 79, Jaapanis 23. Kanalid on "pihustatud" üle mitme erineva sagedusvahemiku. Põhja-Ameerikas ja Euroopas on see 2,402–2,480 GHz, Jaapanis 2,473–2,495 GHz. Iga kanal omab ribalaiust 1 MHz.

Samuti on ära määratud hüpete järjekord ja hüpete skeemid. Standardiga on ära määratud kolm skeemi, mis sisaldavad erinevaid sagedusi. Minimaalne hüppe kaugus on Põhja-Ameerikas ja enamikus Euroopas 6 MHz, Jaapanis 5 MHz.

HSLPS-i sageduse moduleerimise funktsioon

Füüsilisest meediast sõltuv alamkiht suudab andmeid edastada 1 või 2 Mb/s, sõltuvalt modulatsioonist. Antud alamkiht kasutab kahetasemelise Gaussi sageduse tõstmise võtmega (two-level Gaussian shift key) moduleerimist, et saavutada edastuskiirus 1 Mb/s. Antud võtme idee on kandevsageduse sageduse muutmine, mis peegeldab erinevaid kahendsümboleid. Selle tulemusena muutub signaalis määravaks sagedus, kuna sellesse on kodeeritud kogu paketis sisalduv info. Kuna müra mõjutab üldjuhul signaali amplituudi, mitte sagedust, vähendab säärane moduleerimine võimalikku interferentsi halba mõju.

Modulaator saadab kahendinfot, tõstes või vähendades kandevsageduse sagedust natukene üles või allapoole kesksagedust (Fc) antud hüppe juures:

`Saatesagedus = Fc + fd,` et saata loogiline "1"
`Saatesagedus = Fc - fd,` et saata loogiline "0"

Fc on seega antud hüppe juures olev kesksagedus (muutub iga hüppega!) ja fd on sageduse muut. Fd väärtus peaks olema suurem kui 110 kHz. Nominaalne standardi poolt pakutav väärtus on 160 kHz.

Et teostada ülekannet 2 Mb/s, kasutab füüsilisest meediast sõltuv alamkiht neljatasemelist Gaussi sageduse tõstmise võtit. Selle moduleerimisviisi puhul ei kasutata mitte ühte andmebitti lähtealusena, vaid vaadeldakse kahebitilisi kombinatsioone 00, 01, 10 ja 11, mis saabuvad F-kihi koonduva protseduuriga alamkihilt. Kuna iga bitipaar on saadetud kiirusega 1 Mb/s, tähendab see seda, et tegelik bitikiirus on 2 Mb/s. Säärasel juhul peab saatja loomulikult kiirgama välja signaali neljal erineval sagedusel. Kuna kasutatakse samu valemeid, eksisteerib lihtsalt kaks erinevat signaali muutu fd, mida vajadusel saatjas kasutatakse.

Saatja väljundvõimsus on piiratud 100 mW. Kõik füüsilisest meediast sõltuvad alamkihid peavad toetama vähemalt 10 mW saatevõimsust.

Otsejärjestikuse laialipihustatud spektri (OJLPS) füüsiline kiht

- Kõige kulukam
- Vajab kõige rohkem energiat
- Kõrgeimad võimalikud andmeedastuskiirused ühe kihi kohta, kui võrrelda HSLPS-iga
- Vähe geograafiliselt eraldiseisvaid raadiorakke tänu piiratud kanalite arvule
- Suurem riba võrreldes hüpleva sageduse ja infrapunavalgusel põhinevate F-kihtidega

OJLPS-i korral toimub kõigepealt andmepaketi "pihustamine" üle baassageduse ning seejärel pihustatud andmete modleerimine kindlale sagedusele.

Saatja pihustab andmepaketti, kasutades näilise müra koodi üle kahendlisaja. Näilise müra järjekord antud standardi puhul on Barkeri järjestus: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1. Nagu näha, koosneb see pluss ja miinus ühtedest. Tulemus on otsejärjestusega laialipihustatud spektri signaal, mis omab kõrgemat andmeedastuskiirust kui originaalsignaal. Seega, kui sisendisse tuli pakett 1 Mb/s, siis tulemuseks on 11 Mb/s pihustatud signaal. Jäänud on vaid modulaatori töö, mis muudab signaali analoogsignaaliks valitud kanali töösagedusel.

Moduleerimisel saadab OJLPS füüsilisest meediast sõltuv alamkiht esmase paketi välja kiirusel 1 või 2 MB/s, kasutades selleks kahte andmekiirusest sõltuvat modulatsioonitüüpi. 1 Mb/s korral kasutatakse diferentsiaalset kahetise faasi muutumise võtmega (differential binary phase shift keying) moduleerimist. Idee kohaselt muudetakse kandevsageduse faasi, peegeldades sellega erinevaid kahendsümboleid. Kuna andmeid kannab edasi signaali faas ja mürad üldiselt faasi ei mõjuta, on taas vähendatud interferentsi mõju. Modulaator muudab faasi, sõltuvalt F-kihi koonduva protseduuri alamkihilt tulevale infole.

Kahemegabitise kiiruse korral kasutatakse diferentsiaalset neljatise faasi muutumise võtmega (differential quadrature phase shift keying) moduleerimist. Sellisel juhul vaadeldakse sisendis kahte andmebitti (00, 01, 10, 11) korraga.

Kui mitmese juurdepääsuga koodi jagamine (code division multiple access) kasutab erinevaid pihustamise järjekordi, mis võimaldavad paljudel kasutajatel ühel sagedusel töötada, siis otsesageduslik laialipihustamine kasutab ühte pihustamisjärjestust, kuid võimaldab kasutajatel valida erinevaid töösagedusi.

OJLPS-i F-kiht kasutab tööks sagedusvahemikku 2,4 –2,4836 GHz. Standard määratleb OJLPS-i töö kuni 14 kanalil:

Kanali	Sagedus	USA ja	Ülejäänud	Hispaa-	Prant-	Jaapan

nr.	(GHz)	Kanada	Euroopa	nia	susmaa	
1	2.412	+	+			
2	2.417	+	+			
3	2.422	+	+			
4	2.427	+	+			
5	2.432	+	+			
6	2.437	+	+			
7	2.443	+	+			
8	2.447	+	+			
9	2.452	+	+			
10	2.457	+	+	+	+	
11	2.462	+	+	+	+	
12	2.467		+		+	
13	2.472		+		+	
14	2.484					+

Saatevõimsused OJLPS-i puhul on USA-s 1000 mW, Euroopas 100 mW ja Jaapanis 10 mW. Tegelik võimsus on suurem, kuna kasutatakse suundantenne ja muud vastavaid tehnikaid. Standard määrab ka seda, et kõik füüsilisest meediast sõltuvad alamkihid peavad toetama vähemalt 1 mW saatevõimsust.

Võrreldes eelnevate F-kihtide tüüpidega iseloomustab infrapunavalgusel põhineva TKV lahenduse F-kihti odavus, hea mürakindlus ja raske pealtkuulatavus, kuna signaal ei levi läbi seinte. Samas peab aga olemas olema peegelduspunkt (nt. lagi), mille tulemusena kõik jaamad juurdepääsupunktiga ühendust saavad pidada. Samas puudub aga regulatsiooni infrapunasageduste kasutamise osas.

Lisa 1: Inglisekeelne materjal

Wireless Network Concerns

- Radio signal interference

The process of transmitting and receiving radio and laser signal through the air makes wireless systems vulnerable to atmospheric noise and transmissions from other systems. In addition wireless networks can interfere with other nearby wireless networks and radio wave equipment. Inward direction — WLAN can experience inward interference either from harmonics of transmitting systems or other products using similar radio frequencies. For example microwave ovens that work in S band (2,4 GHz) that many WLANs use to operate. This results the transmission block from other stations or bit errors. Outward direction — WLAN system may disrupt other working systems such as navigation system. Interference is uncommon with WLANs operating in the public spread spectrum band because the output power is so little (less than 1 watt). Because of that the transmission components must be very close.

- Power management

The NICs significantly decrease the amount of time that is available before recharging the batteries. Usually the interface keeps radio off most of the time and when the transmission request occurs wakes it up. The sleep mode utilizes approximately 50 % less power.

- System interoperability

The products from different vendors must operate together. The standard IEEE 802.11 should increase the compatibility among multi-vendor wireless systems.

- Network security

WLANs intentionally propagate data over an area that may exceed the limits of the area the organization physically controls. Someone can passively retrieve the information that moves in WLAN using the same wireless NIC from the distance without being noticed by the security. The intruder must of course obtain the network access code is necessary to join the cell.
There is also possibility for electronic sabotage: someone may purposely jam the radio-based network keeping others using it. If one station is transmitting the others must wait. So someone may use a station that constantly transmits data to the network. The current transmission puts all other stations on hold thereby making the network inoperable.
Restricting access to the data solves the problem. Most products require the network code establishment that is set within each workstation. A wireless station will not process the data until the code is the same as in a network.

- Connection problems

Using the same protocols in a wireless network as in the wired network causes connection problems. TCP/IP in a wireless networks is susceptible to losing connections. This is especially seen when the appliance is operating in an area with marginal network coverage. There may also occur addressing problems. When the appliance is moved from one subnet to another it loses the capability to reestablish the connection.

- Installation issues

There are several factors that influence the radio-based network coverage. Walls, ceilings and other physical object cause the signal to attenuate. They even may cause to change their paths of transmission. Therefore the propagation tests should always being preformed before installing the WLAN system. The other radio transmitters located nearby may also influence the whole system. Not to mention that it is essential to consider that the WLAN itself may interfere with other already installed systems.

- Health risks

There is no conclusive answer to the question whether the WLAN is safe or not. It is said that it appears to be even safer than the cellular phones because their operating power level is between 50 and 100 mw when cellular phones produce 600 to 3 watts of output power.

WLAN Components

- End-user appliances

These are the interface between the user and the network. The most common appliances are desktop workstations, laptop computers, PDAs and all other handheld devices.

- Network software

There is different software that reside on different parts of the network. The most important part is the high-end PC where the network operating system is installed. In most simple case the same PC server provides the wireless network hosting services (which means it acts as an access point) for all the other workstations equipped with wireless NICs.
There may be cases where the server itself does not act as an access pont. In that case the gateway equipped with a middleware is found in the network. The gateway may communicate with terminals via wireless-friendly protocol that is not like TCP/IP. In wireless networks there may always occur outages in communication. With gateway these outages are transparent to the main server. Last but not least, the terminal (in most cases laptop) does not have to send the keep-alive packets to keep the connection open. It's done by gateway.

- Network interface card
- Antenna

Propagation pattern, gain, transmit power, bandwidth. Propagation pattern defines its coverage. Omni directional antenna transmits its power to all directions. Directional antenna concentrates most of its power in one direction. Directional antenna has more gain (degree of amplification) than the omni directional in the same power level. The combination of transmit power and the gain of the antenna defines the distance the signal will propagate. With wireless networks the transmit power is relatively low, typically one watt or less.
Bandwidth is the effective part of the frequency spectrum that the signal propagates. The telephone system operates over a bandwidth roughly from 0 to 4 KHz. Data rates and bandwidth are highly proportional: the higher data rates the more bandwidth is needed.

Logical architecture

The most popular is the seven-layer Open System Interconnect Reference Model (OSI), developed by the International Standards Organization (ISO). ISO-OSI layers:

1. Physical Layer — Provides the transmission of bits through a communication channel by defining electrical, mechanical and procedural specifications.
2. Data Link Layer — Ensures synchronization and error control between two entities.
3. Network Layer — Provides the routing of packets through routers from source to destination. Such protocols as IP operate at this layer.
4. Transport Layer — Provides mechanisms for the establishment, maintenance and orderly termination of virtual circuits while shielding the higher layers from the network implementation details. Such protocols as TCP operate at this layer.
5. Session Layer — Establishes, manages and terminates sessions between applications.
6. Presentation Layer — Negotiates data transfer syntax for the Application Layer and performs translations between different data types if necessary.
7. Application Layer — Establishes communications with other users and provides such services as file transfer and email to the end users of the network.

The wireless networks operate only on the bottom of three layers. Only WWAN networks perform Network Layer functions as well.

Radio-based LANs

+: The possibility to connect users without having a line of sight and propagation through walls and other constructions with little attenuation.
-: Management with other electromagnetic propagations. The interference may occur if no proper investigations are made beforehand. Data receiving by unauthorized users from outside the areas controlled by the organization. The solution is signal scrambling.

Medium Access Control

Data Link Layer function in WLAN: Enables multiple appliances to share the common transmission medium via a carrier sense protocol. It enables a group of wireless computer to share the same frequency and space. This protocol ensures that only one computer transmits the data at a time while all the others must wait until the transmission is ended. Wireless networks handle the error control by having each station check incoming data for alerted bits. If the destination station does not detect errors it sends an acknowledgement back to the source station. If there were any errors this protocol ensures that the packet is resent.

Spread Spectrum Modulation

Physical Layer function. Spread spectrum "spreads" the signal over a wider band of frequencies. It doesn't conserve bandwidth but the data signal is made by much less susceptible to electrical noise. The noise will only interfere with a small portion of the spread spectrum signal, which causes fewer errors when the signal is demodulated. There are two spreading techniques: frequency hopping and direct sequence.

Frequency hopping spread spectrum

It modulates the data signal with a carrier signal that hops from frequency to frequency. The order is determined by hopping code. For proper receiving the receiver must use the same hopping code and listen the right frequency at the right time. Defined by standards the manufacturers are required to use 75 or more frequencies per transmission channel with maximum dwell time (the time spent to a particular frequency during the frequency hop) of 400 ms. If the radio encounters interference in one frequency it will retransmit the signal on another frequency. Maximum data rates using this technique are up to 2Mbps.
Using this technique it is possible for several operating radios to use the same frequency band, assuming they have different hopping patterns. The set of patterns that never use the same frequencies at the same time are orthogonal.

Direct Sequence Spread Spectrum

The signal is combined with a higher data rate bit sequence, called chipping code. It increases the signal's resistance to interference. The minimum code is 10. Commonly 20 is used. The original data bits are replaced accordingly to mappings.

Operating Frequencies

In USA the 902-928MHz (26 MHz of bandwidth), 2,40-2,4835 GHz (83,5 MHz) and 5,725-5,850 GHz (125 MHz) are used. In all other parts of the world the 2,4 GHz is accepted.

Narrowband Modulation

Used by conventional radio systems. They concentrate all their transmit power within a narrow range of frequencies. The idea is to conserve as much bandwidth as possible. In this case the noise would corrupt most of the signal. To avoid this problem it is required that each user operating on narrowband frequencies obtains the proper license. If the interference occurs the FCC resolves the problem.

Peer-to-peer wireless LANS, multiple-cell WLANs.

Infrared Ligh-Based WLANs

Infrared uses the frequency, which is lower than spectral colors, but higher than radio waves. Products operate around 820 nm wavelengths where the attenuation by the air is the least. Infrared does not propagate through opaque objects (walls etc.). This keeps data "behind the walls". Common noise sources do not interfere with the light signal. But it is not suitable for mobile applications because of a limited coverage.
Equipment consists of two parts: the adapter and transducer. The last one is similar to the antenna with radio-based LAN.

Diffused IrWLAN

Uses ceiling as a reflection point. Uses carrier sense protocols to share access to the ceiling. Before data transmission the source sends the proper sequence of code that grabs the receiver's attention. Data rates are between 1 to 4 Mbps.

PP IrWLAN

Maximum distance 75 ft. The PP IrWLAN uses token ring interface boards. This ensures that only one station speaks at a time. The token, which is a distinctive group of bits, circulates the ring. If a station wishes to transmit data it must first wait its turn to receive the token and then transmit the data. The capturing of the token ensures that no other station is transmitting. The data circulates the ring and the appropriate destination will sense its address and process the data. Once finished, the sending station will forward the token to the next station down line.

Carrier Current LANs

The data rates are between 1 to 2 Mbps. The AC does not affect the signal because they use different frequencies. The interface has filters that will prevent the lower 60 Hz frequency from

being received. The installation is easy, but electrical transformers will block higher frequency data signals.

Wireless PP Networks

Radio-Based Wireless PPN

Spread spectrum products that operate under 1 watt power can reach single hop transmission distances up to 30 miles. The actual distance of course depends on environmental conditions and terrain. Data rates are between 4 and 5 Mbps for the shorter-range products operating over 2-3 mile links. Products that operate over 30-mile link transmit at much lower data rates and in addition they use either spread spectrum or a narrowband modulation. It is important to know that the signals that travel from one building to another are out of the jurisdiction of the company and so may get interfered from other stations working nearby. To prevent this effect the narrowband modulations should be used.

Laser-Based Wireless PPN

The data rates are extremely high — 10 Mbps Ethernet or 4/16 Mbps token ring. To maintain safe operation, laser links typically range less than a mile. Most laser work under Class III, which can cause eye damage under some circumstances. Weather also influences the transmission distance. A fairly heavy rain (3-4 in per hour) would attenuate the signal approximately 6 dB per kilometer. Using the laser system the interference is practically impossible. Even high microwave frequencies are far away fro laser light and interfering laser beam is unlike. It should be pointed directly to the receiver. Usually it won't happen unless someone purposely would want to harm the system.

IEEE 802.11 Topology

BSS is a basic building block that wireless networks utilize. It provides a coverage area whereby stations of the BSS remain fully connected. A station is free to move within BSS, but it can no longer communicate directly with other stations if it leaves BSS.

Independent Basic Service Set IBSS

Standalone BSS that has no backbone infrastructure and consists of at least two wireless stations. This is an ad hoc network.

Extended Service Set ESS

Mobility types under ESS:

- No-transition: Stations that do not move and stations that move within local BSS.
- BSS-transition: Stations that move from one BSS in on ESS to another BSS within the same ESS.
- ESS-transition: Stations that move from a BSS in one ESS to a BSS in different ESS.

The standard does not guarantee that a connection will continue when making an ESS-transition.
Distribution system is an element that interconnects BSSs within the ESS via access points.
Access point is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC layer.

IEEE 802.11 Services

Station services

- Authentication

All 802.11 stations whether they are part of the BSS or ESS network, must use the authentication service prior to establishing a connection with another station with which they will communicate. (Security reasons.)
Open system authentication: The station that wants to be authenticated sends an authentication management frame containing the sending station's identity. The receiving station sends back a frame alerting whether it recognizes the identity of the authenticating station.
Shared key authentication: It assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key.

- Deauthentication

When a station wishes to disassociate with another station, it invokes the deauthentication service. This is a notification that cannot be refused. Stations perform deauthentication by sending an authentication management frame (or group of frames to multiple stations) to advise the termination of authentication.

- Privacy

The privacy service, applying to all data frames and some authentication management frames, is based on the 802.11 Wired Equivalent Privacy (WEP) algorithm that significantly reduces risks if someone eavesdrops on the network. This algorithm performs message encryptions.

- MSDU delivery

Distribution system services

- Association

Each station must initially invoke the association service with an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point. Each station can associate with one access point only but each access point can associate with multiple stations. This is the first step providing the capability for a station to be mobile between BSSs.

- Disassociation

A station or access point may invoke disassociation service to terminate an existing association. This service is a notification; therefore neither party may refuse termination. Stations should disassociate when leaving the network. Access point should do this when it is being removed for maintenance
.

- Distribution

A station uses the distribution service every time it sends MAC frames across a distribution system. The 802.11 standard does not specify how the distribution system delivers the data. This service provides the distribution system only the information to determine the proper BSS.

- Integration

It enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN. The integration function performs all required translations.

- Reassociation

Changes the current state of association. It enables a station to transition its association from one access point to another. This keeps the distribution system informed of the current mapping between access point and station as the station moves from BSS to BSS within ESS. It also enables changing the association attributes of an established association while the station remains associated with the same access point. The mobile station always initiates the reassociation service.

Medium Access Control Layer (MAC)

Access to the network is gained using one of the two modes:

- Carrier-sense multiple access with collision avoidance (CSMA/CA). IEEE 802.11 refers to this as distributed coordination function (DCF).
- Priority-based access: Contention-free access protocol usable on infrastructure network configurations containing a controller called a point coordinator within the access points. 802.11 refers to this as point coordination function (PCF).

Distributed Coordination Function

Primary coordination function used for automatic sharing of the wireless medium using compatible PHYs. Uses CSMA/CA protocol for sharing the wireless medium.

Carrier sense mechanism

The MAC uses both physical and virtual carrier sense mechanism to determine whether the medium is idle. Every PHY layer provides a physical means of sensing the channel. The results are forwarded to MAC layer as a part of the information factored when deciding the status of the channel.

The MAC coordination also carries out the virtual sense protocol based on the reservation information found in the duration field of all frames. This information announces to all other stations a station's impending use of the medium. MAC coordination will monitor the duration field in all MAC frames and place this information in the station's Network Allocation Vector (NAV) if the value is greater than the current NAV value. The NAV operates like a timer starting with the value equal to the duration field from the MAC frame and counting down to the zero. When NAV reaches to zero, the station can transmit the data.
The physical channel assessment and NAV provide sufficient information about the channel status. If the channel is still busy, the MAC protocol implements a random backoff algorithm.

The backoff time is calculated by the formula backoff time = random() * aSlotTIme.
Random() is a pseudo-random integer drawn from a uniform distribution over the interval [0; CW] in which CW (collision window) is an integer within the range of values of the Management Information Base (MIB) attributes aCWmin and aCWmax. The random number drawn from this interval should be statistically independent among stations. aSlotTime equals a constant value found in the station's MIB.
Actually the CW increases exponentially to minimize collisions and macimize throughput both low and high network utilizations. Under low utilization the station doesn't have to wait very long before transmitting the data. On the first or second attempt it can successfully use the medium for transmitting. If the utilization is high the protocol holds stations back for longer periods of time to avoid the probability of collisions. Under high utilization the CW increases to relatively high

values. This mechanism does a good job for avoiding collisions but the stations will experience substantial delays while waiting to transmit frames

Error correction

The process called automatic repeat-request (ARQ) is used. To regulate the number of retransmissions the MAC coordination differentiates between the short and long frames. For short frames (with the length less than the MIB attribute aRTSThreshold), retransmissions continue until the number of attempts reaches the MIB value aShortRetryLimit. The MAC coordination retransmits long frames similarly based on the MIB attribute aLongRetryLimit. After reaching the retry limit, the station discards the frame.

Access spacing

The standard defines several spacing intervals (defined in the MIB) that defer a station's access to the medium and provides various levels of priority. Each interval defines the time from the end of the last symbol of the previous frame to the beginning of the first symbol of the next frame. The following describes each of the interframe space (IFC) intervals:

- Short IFS (SIFS): The SIFS is the shortest of the interframe spaces, providing the highest priority level by allowing some frames to access the medium before others. Such frames are ACK (acknowledgement) frame, CTS (clear to send) frame and the second or subsequent MSDU of a fragment burst. These frames require expedient access to the network to minimize frame retransmissions.
- PCF IFS (PIFS): The PIFS is the interval that stations operating under the point coordination function use to gain access to the medium. This provides priority over frames sent by distributed coordination function. These stations can transmit contention-free traffic if they sense the medium is idle. This interval gives point coordination function-based stations a higher priority of access than DCF-based stations for transmitting frames.
- DCF IFS (DIFS): All stations according to the distributed coordination function use the DIFS interval for transmitting data frames and management frames. This spacing makes the transmission of these frames lower priority than PCF-based transmissions.
- Extended-IFS (EIFS): All DCF-based stations use the EIFS interval as a waiting period when frame transmission results in a bad reception of the frame due to incorrect FCS value. This interval provides enough time for receiving station to send an ACK frame.

Point Coordination Function (PCF)

Provides contention-free frame transfer. In this case, the point coordination resides in the access point to control the transmission of frames from stations. All stations obey the point coordinator by setting their NAV value at the beginning of each contention-free period. Stations can optionally respond to a contention-poll however.

At the beginning of the contention-free period, the point coordinator has an opportunity to gain control over the medium. The point coordinator follows the PIFS interval as a basis for accessing the medium. Therefore it may be able to maintain control during the contention-free period by waiting a shorter time between transmissions than stations operating under the distributed coordination function.

The pint coordinator senses the medium at the beginning oh each contention-free period. If the medium is idle after the PIFS interval, the point coordinator sends a Beacon frame that includes the CF Parameter Set element. When stations receive the beacon, they update their NAV with the CFPMaxDuration value found in the CF Parameter Set. This value communicates the length of the

contention-free period to all stations and prevents stations from taking control of the medium until the end of the period.

After sending the Beacon frame, the point coordinator then transmits one of the following frames after waiting at least one SIFS interval:

- Data frame: Directed from point coordinator to a particular station. If the coordinator does not receive ACK frame from the recipient, the coordinator can retransmit the unacknowledged frame during the contention-free period after the PIFS interval.
- CF Poll frame: The coordinator sends this frame to a particular station, granting the station to transmit one frame to any destination. If it has no frame to send, it must send a Null data frame. If the sending station does not receive an ACK frame it must wait another CF Poll frame before it can retransmit the data frame.
- Data+CF Poll frame: The coordinator sends a data frame to the station and polls that same station for sending a contention-free frame. Reduces overhead of the network.
- CF End frame: Identifies the end of the contention-free period. This happens if the CFPFurRemaining time expires or the point coordinator has no further frames to transmit and no stations to poll.

Stations have an options of being pollable. Station can change its pollability by issuing a Reassociation Request frame. The point coordinator maintains a list of pollable stations that may receive a poll during the contention-free period.

Authentication And Privacy

- Open system authentication. The station sends its identification as a plain text part of the authentication frame over the network and receives a authentication frame from authenticating station with an answer to the authentication request.
- Shared key authentication:

1. A requesting station sends an Authentication frame to another station;
2. When a station receives Authentication frame, the station will reply with Authentication frame containing 128 octets of challenge text that the WEP services generate.
3. The requesting station will then copy the challenge text into an Authentication frame, encrypt it with a shared key and then send the frame to the responding station.
4. The receiving station will decrypt the value of the challenge text using the same shared key and compare it to the challenge text sent earlier. If a mach occurs, the responding station will reply with an authentication indicating a successful authentication.

Private Frame Transmissions

To offer this transmission the 802.11 standard defines optional WEP. The WEP generates secret shared encryption keys that both source and destination stations use to alter frame bits to avoid disclosure to eavesdroppers. This process is also known as symmetric encryption.

1. At the sending station, the WEP encipherment first runs the unencrypted data located in the Frame Body field of a MAC frame through an integrity algorithm that generates a four-octet integrity check value that is sent with the data and checked at the receiving station to guard against unauthorized data modification.
2. The WEP process inputs the secret shared encryption key into a pseudo-random number generator to create a key sequence with length equal to the plaintext integrity check value.
3. WEP encrypts the data by using ‘bitwise XOR’ on the ‘plaintext’ and integrity check value with the key sequence to create ‘ciphertext’. The pseudo-random number generator makes key distribution much easier because only the shared key must be made available to each station, not the variable length key sequence.

4. At the receiving station, the WEP process deciphers the 'chiphertext' using the shared key that generates the same key sequence used initially to encrypt the frame.
5. The station calculates an integrity check value and ensures it matches the one sent with the frame. If the integrity check fails, the station will not hand the MSDU off to the LLC.

Physical (PHY) Layer

Architecture

- Physical Layer management: Provides management functions to the layer.
- Physical Layer convergence procedure (PLCP) sublayer: The MAC Layer communicates with PCLP via primitives through the Physical Layer service access point (SAP). When MAC Layer instructs, the PCLP prepares MAC protocol data units (MPDUs) for transmission. The PLCP also delivers incoming frames from the wireless medium to the MAC Layer.

  The PCLP appends fields to the MPDU that contain information needed by the Physical Layer transmitters and receivers. The 802.11 standard refers to this composite frame as a PLCP protocol data unit (PPDU). The frame structure of a PPDU provides for asynchronous transfer of MPDUs between stations.
- Physical medium dependent (PMD) sublayer: Under the direction of the PLCP, the PMD provides actual transmission and reception of Physical Layer entities between two stations via the wireless medium. To provide this service, the PMD interfaces directly with the wireless medium (the air) and provides modulation and demodulation of the frame transmissions. The PLCP and PMD communicate via primitives to govern the transmission and reception function.

MAC Layer →/PHY SAP/ → PLCP Sublayer → /PMD SAP/ → PMD Sublayer

Frequency Hopping Spread Spectrum (FHSS) Physical Layer

- Lower cost
- Lowest power consumption
- Most tolerant to signal interference
- Lowest potential data rates from individual physical layers
- Highest aggregate capacity using multiple physical layers
- Less range than direct sequence but greater range than infrared

FHSS PMD Sublayer Frequency Hopping Function

The 802.11 standard defines a set of channels that are evenly spaced across the 2.4 GHz ISM band. The number of channels depends on geography. In North America and Europe it's 79, in Japan 23.

The channels spread across a band of frequencies. In North America and Europe it's 2.402-2.480 GHz, in Japan 2.473-2.495 GHz. Each channel is 1 MHz wide.

The FHSS-based PMD transmits PPDUs by hopping from channel to channel according to a particular pseudo-random hopping sequence that uniformly distributes the signal across the operating frequency band. After the hopping sequence is set in an access point, stations automatically synchronize to the correct hopping sequence. The standard specifies that in North America and most of the Europe it's 78 and in Japan 12. The sequences avoid prolonged

interference with one another. This enables designers to collocate multiple PMDs to improve performance.

When designing WLAN the hopping sequences and hopping sets must be selected. The standard defines 3 sets that contain different sequences. The minimum hop distance in North America and most of the Europe is 6 MHz, in Japan 5 MHz.

FHSS Frequency Modulation Function

FHSS PMD transmits binary data at either 1 or 2 Mbps using a specific modulation type for each, depending on the data rate. The PMD uses two-level Gaussian frequency shift key (GFSK) modulation for transmitting data streams at 1 Mbps. The concept of GFSK is to vary the frequency of the carrier frequency to represent different binary symbols. Thus, changes in frequency maintain the information content of the signal. Noise usually affects the amplitude of the signal not the frequency. So this modulation reduces potential interference.

The modulator transmits the binary data by shifting the transmit frequency slightly above or below the center operating frequency (Fc) for each hop:
Transmit frequency = Fc + fd for sending a logic 1
Transmit frequency = Fc – fd for sending a logic 0
Fc is the operating center frequency for the current hop and fd is the amount of frequency deviation. The value of fd shall be greater than 110 KHz. The nominal value provided by the standard is 160 KHz.

For transmitting data streams at 2 Mbps, the FHSS PMD uses four-level GFSK modulation. For this modulation the input to the modulator are combinations of two bits (00, 01, 10, 11) coming form PLCP. Each of these pairs is sent at 1 Mbps, meaning each bit is sent at 2 Mbps. In this case the transmitter can transmit at four possible frequencies. To perform this operation the modulator will transmit on the operating center frequency with a frequency deviation equal to fd. Two values of fd move the transmit frequency above Fc and two below.

The maximum amount of transmitter output power is limited to 100 milliwatts. All PMDs must support at least 10 milliwatts transmit power.

Direct Sequence Spread Spectrum (DSSS) Physical Layer

- Highest cost
- Highest power consumption
- Highest potential data rates from individual physical layers as compared to frequency hopping
- Lowest aggregate capacity using multiple physical layers than frequency hopping
- Smallest number of geographically separate radio cells due to a limited number of channels
- More range than frequency hopping and IR PHY Layers

DSS PMD Operation

The DSSS physical layer multiplies the radio frequency carrier by a pseudo-noise digital signal. The resulting signal appears as noise if plotted in the frequency domain. The wider bandwidth of the direct sequence enables the signal power to drop below the noise threshold without loss of information.

As with FHSS the DSSS physical layer operates within 2.4 to 2.4836 GHz frequency ranges. The standard specifies operation of DSSS on up to 14 channels of different frequencies:

Channel No.	Frequency	US and Canada	Europe	Spain	France	Japan
1	2.412	+	+			
2	2.417	+	+			
3	2.422	+	+			
4	2.427	+	+			
5	2.432	+	+			
6	2.437	+	+			
7	2.443	+	+			
8	2.447	+	+			
9	2.452	+	+			
10	2.457	+	+	+	+	
11	2.462	+	+	+	+	
12	2.467		+		+	
13	2.472		+		+	
14	2.484					+

DSSS Spreading Sequence

The general idea is to first digitally spread the baseband data frame (PPDU) and then modulate the spread data to a particular frequency.
The transmitter spreads the PPDU by combining PPDU with a pseudo noise (PN) code via the binary adder. The PN sequence for direct sequence systems consists of a series of plus and minus 1s. The specific PN code for this standard is Barker sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1.
The output of the binary adder is a DSSS signal that has a higher-rate signal than the original data signal. If the input was 1 Mbps PPDU, the result is an 11 Mbps spread signal at the output. The modulator then translates the baseband signal into an analog signal at the operating transmit frequency of the chosen channel.

When CDMA (code division multiple access) uses multiple spreading sequences to enable multiple users operate on the same frequency. DSS always uses on e spreading sequence, but enables users to choose among several transmission sequences.

DSSS Frequency Modulation

A balanced modulator modulates the spread PPDU by combining the spread PPDU with a carrier set at the transmit frequency. The DSSS PMD transmits the initial PPDU at 1 or 2 Mbps using different modulation types, depending on the chosen data rate. For 1 Mbps it uses differential binary base shift keying (DBPSK) modulation.

The concept of this modulation is to vary the phase of the carrier frequency to represent different binary symbols. Thus, changes in phase maintain the information content of the signal. Noise usually doesn't affect the phase of the signal. The modulator shifts the phase based on the input coming from PLCP.

For 2 Mbps transmission the PMD uses differential quadrature phase shift keying (DQPSK) modulation to send data at 2 Mbps. In this case the input to the modulator contains two bits.

The transmit power in US is 1000 mW, in Europe 100 mW, in Japan 10 mW. The actual power is higher because of the gaining techniques used (directional antennas etc.)
The standard specifies that all PMDs must support at least 1 milliwatt transmit power.

Infrared (IR) Physical Layer

- Lowest cost
- Highest tolerance to RF signal interference
- Lowest range compared to spread spectrum radio systems
- Most resistive to eavesdropping because the room contains the infrared light signals
- Must operate in areas where a ceiling is present (indoors) to act as a reflection point for the infrared signals
- Accepted worldwide without frequency regulation

IR Physical Medium Dependent (PMD) Sublayer

Uses a non-directed transmission that eliminates the need for line-of-sight operation – diffused infrared. The transmission range is between 10 and 20 meters because the ceiling is used as a reflection point. The physical layer transmits its signals in 850-950 nanometers range at maximum of 2 watts peak optical power level.

For 1 Mbps the IR uses 16-pulse position modulation (PPM) technique. This technique varies the position of a pulse to represent different binary symbols. (Like a phase shift keying.)

For 2 Mbps the IR PMD uses 4-PPM.
Both modulation tables use gray code, which ensures that there is only a single bit error in the data if a pulse of the transmitted signal gets out of position by one time slot.