#2 Wireless LANy

Úvod

- klasické LAN technológie (Ethernet, Token Ring) využívajú ako prenosové médium medené vodiče - káble
- tieto tvoria podstatnú časť nákladov na samotnú sieť (nosnou časťou bývajú samotné aktívne prvky)
- pri zmene topológie – znovu ďalšie náklady
- toto je jeden z dôvodov na vznik tzv. bezdrôtových sietí (WLAN-ov)
- ďalším dôvodom sú mobilné stanice, napr. notebooky, ktoré vyžadujú prístup na sieť aj počas pohybu

- pri WLANoch sa ako prenosové médium využívajú rádiové vlny, resp. infrared vlny
- WLANy umožnujú vytvárať dva druhy topológií
  - **ad-hoc** (na požiadanie, podľa aktuálnej potreby) -napr. spojenie dvoch notebookov napriamo cez IR porty
  - **infrastructure** – spojenie dvoch, resp. viacerých zariadení prostredníctvom centrálnej prepájacej stanice (niečo ako BTS pri mobilných telefónoch). Takáto stanica spravidla zabezpečuje spojenie s ďalšími stanicami a často aj prepojenie na pevnú, drôtovú sieť (prístup k serverom a pod.)

Prenosové médiá

Rádiové vlny

- využíva sa prenos pomocou rádiových vĺn (podobne ako pri šírení rozhlasu, televizie, mobilných telefónov a pod.)
- kvôli vzájomnému rušeniu je prideľovanie frekvenčných pásiem koordinované
- toto prenosové médium trpí nasledovnými neduhmi:
  - útlm signálu (path loss)
    - zariadenia sú schopné fungovať iba pre určitý SNR – čím zložitejšie a drahšie zariadenie, tým menší signál je potrebný (oproti šumu)
    - čím viac zariadení, tým nižšia cena (dobrým príkladom sú mobily)
  - channel interference
  - multipath (prijímač prijíma viaceré signály z toho istého zdroja)
    - intersymbol interference (kvôli rôznym delayom)
    - Rayleigh fading (odrazené vlny vedia zrušiť priamy signál)
      - tomu sa zabraňuje buď dvomi anténami (vzdialenými o ¼ vlnovej dĺžky) alebo úpravou prijímača – adaptívny ekvalizér (opočítava od prijatého signálu hodnotu ekvivalentnú odrazeným)

Infrared

- používa sa infrared pásmo
- na vysielanie sa používajú buď Laserové diódy alebo LED-ky, na príjem spravidla fotodiódy
- dva druhy topológií – point-to-point (spojenie napriamo bod-bod), alebo difúzny mód (point-to-multipoint)

Prenosové schémy

pri rádiových vlnách sa používajú tieto prenosové schémy:

- direct sequence spread spectrum
- frequency-hopping spread spectrum
- single-carrier modulation
- multi-carrier modulation

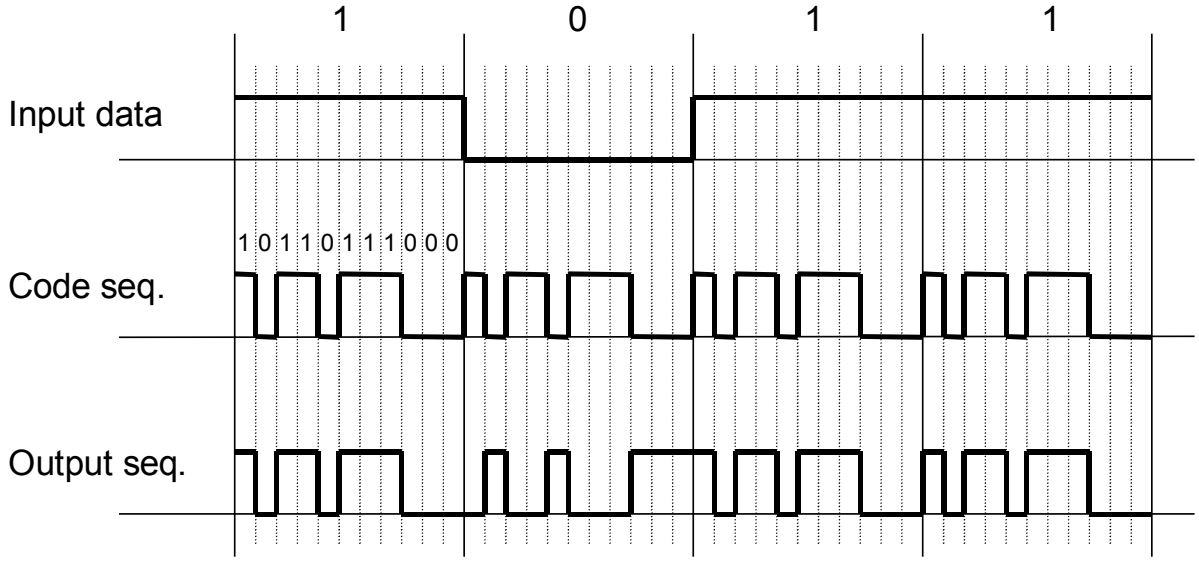
Direct Sequence Spread Sprectrum

- prvé systémy kvôli cene použili dostupné komponenty – tieto však pracujú v používanom pásme
- je to tzv. ISM band (idustrial, scientific and medical)

- v tomto pásme pracujú napr. mikrovlnné rúry :-)
- aby sa ale nové WLANy nerušili s ostatnými (už existujúcimi) systémami v tomto pásme, museli použiť vhodnú prenosovú schému
- uplatnenie našla technika, pôvodne vojenská – tzv. **spread spectrum**
- existujú dve základné metódy tejto techniky – a to direct-sequence a frequency-hopping

princíp DSSS

generovanie Spread spectrum sekvencie



- zdrojové data sú exclusive-OR-ované s pseudonáhodnou binárnou sekvenciou
- zdrojová jednotka ponecháva sekvenciu (tu 10110111000), zdrojová nula ju neguje
- výstupná postupnosť obsahuje teda oveľa viac bitov, a teda aj vo frekvenčnej oblasti bude zaberať viac miesta – rozprestrie pôvodné spektrum – preto názov „spread spectrum“
- takto stačí použiť menší vysielací výkon, a teda aj odstup signálu od šumu môže byť veľmi malý (dokonca sa dá vysielať pod hranicou šumu) – a teda takémuto systému ani nevadí rušenie ostatných, koexistujúcich systémov
- tu uvedená postupnosť 11-ich bitov (10110111000) je tzv. Barkerova sekvencia, má výborné autokorelačné vlastnosti
- pojmy:
  - **spreading sequence** (pseudonáhodná kódová postupnosť)
  - **chip** (jeden bit v spreading sekvencii – v horeuvedenom príklade je ted 11 chipov)
  - **chipping rate** (výsledná prenosová bitová rýchlosť)
  - **spreading factor** (počet bitov/chipov v spreading sekvencii
  - **processing gain**
    - zisk, v dB – ráta sa ako 10xlog(spreading faktoru), t.j. pri spreading faktore 100 bude zisk 20dB (teda keď bude spreading sekvencia 100-bitová)
    - ak je napr. systém navrhnutý pre prácu pri SNR=10dB, a processing gain je tiež 10dB, tak systém s DSSS môže pracovať aj s výkonom signálu na úrovni šumu
- normálne sa pre moduláciu používa BPSK, resp. QPSK

- pri WLANoch
  - všetci členovia WLANu poznajú kódovú sekvenciu (a samozrejme centrálnu frekvenciu:)
  - pred samotným vysielaním dát sa vysiela preambula a start of header (kvôli synchronizácii)
  - preto prijímač po demodulácii najprv hľadá známu kódovú (pseudonáhodnú) postupnosť – aby sa zosynchronizoval
  - pretože stanice, ktoré patria do danej WLANy (zdieľajú rovnaké frekvenčné pásmo a poznajú kódovú postupnosť) môžu pristupovať na spoločné prenosové médium naraz (mohli by naraz vysielať aj viacerí a vzájomne sa zrušiť) **musia používať osobitnú MAC metódu**, aby si navzájom neprekážali

Frequency-hopping Spread Sprectrum

- pásmo je rozdelené na tzv. kanály
- vysielač preskakuje medzi jednotlivými kanálmi, vždy vysiela na danom kanále iba chvíľu
  - buď odvysiela niekoľko bitov ja jednom kanále a až potom preskočí na ďalší – tzv. **slow frequency-hopping**
  - alebo počas vysielania jedného bitu stihne preskákať cez niekoľko kanálov – tzv. **fast frequency-hopping**
- poradie preskakovania medzi kanálmi je pseudonáhodné – tzv- **hopping sequnce**
- čas strávený na jednom kanále – **chip period**, rýchlosť preskakovania – **chipping rate**
- hlavná výhoda oproti Direct sequence je v tom, že sa dajú (vhodne) vybrať také kanály, ktoré sú menej rušené inými systémami v tom istom (ISM) pásme (napr. mikrovlnnými rúrami:)

- samozrejme fast frequency hopping je odolnejší (oproti slow freq. hopping) voči takýmto rušivým zdrojom (pretože sa prípadne poruší iba časť jednej sekvencie, t.j. iba časť jedného informačného bitu), ale je aj zložitejší a teda drahší (hlavne samotná synchronizácia prijímača na skoky je oveľa náročnejšia)

Single-carrier modulation

- klasická metóda modulácií nosnej
- nepoužívajú sa kombinácie s modulovaním amplitúdy – kvôli cene a náročnosti na spotrebu energie
- spravidla sa používa QPSK a jej modifikácie
- pre rýchlosti 1 až 2 Mbps
- multipath efekt spôsobuje výraznú intersymbolovú interferenciu (ISI) – preto musia byť použité rel. komplikované ekvalizačné obvody

Multi-carrier modulation

- najprv sa pôvodný tok dát o vysokej rýchlosti rozdelí na niekoľko pomalších
- každý z nich je následne modulovaný samostatne – na samostatnú pod-nosnú (klasickou single-carrier moduláciou)
- ISI je na pomalších rýchlostiach menej výrazná – netreba ekvalizačné obvody
- Frequency-selective fading je však stále – ovplyvní však iba niektoré frekvencie
- používa sa FEC – spravidla konvolučné kódy
- jednotlivé pod-nosné sú spravidla násobkom prvej (f_1, $2f_1$, $3f_1$, $4f_1$, $5f_1$,...), - vtedy sa táto prenosovná schéma označuje ako **orthogonal frequency division multiplexing (OFDM)**

- pred samotným vysielaním sú všetky osobitne zmodulované pod-nosné ešte skombinované do jedného signálu pomocou Rýchlej Fourierovej transformácie (FFT).

Infrared

Direct modulation

- of-off keying (OOK) s použitím napr. Mangester encoding (0=01, 1=10)
- pulse-position modulation (PPK) – pozícia pulzu určuje hodnotu sekvencie (napr. vstupná postupnosť sa rozdelí na štvorice bitov, a potom bude možných 16 pozícií pulzu – každá bude udávať hodnotu vstupnej dvojice bito (pre „1101“ to bude pulz na 13-tej pozícii)
- limitované pre rýchlosti 1 – 2Mbps

Carrier modulation

- FSK a PSK
- dosiahnuteľné rýchlosti 2 – 4Mbps (lebo potom sa silne prejavuje ISI)
- pri rozdelení pásma na viacero pod-nosných možno zvýšiť rýchlosť až na 10Mbps

Prístupové metódy

- ako sme spomenuli, viaceré stanice zdieľajúce to isté pásmo a prenosovú schému musia nejakým rozumným spôsobom riešiť prístup na toto spoločné médium – zdieľanie spločného média

- je to obdobný problém ako pri klasických LANoch, až na pár nových komplikácií
- možné prístupy

CDMA

- **code-division multiple access**
- pri spread spektrum systémoch
- pásmo možno zdieľať na základe rôznych spreading/hopping sekvencií
- pri direct sequence sa môžu jednotlivé stanice zatieniť
- každá stanica by musela mať svoju vlastnú kódovú postupnosť a ostatní by o tom museli vedieť – pri (W)LANoch ťažko administrovateľné (okrem toho dostatok „dobrýc“, vzájomne sa málo rušiacich kódov je limitovaný)

CSMA/CD

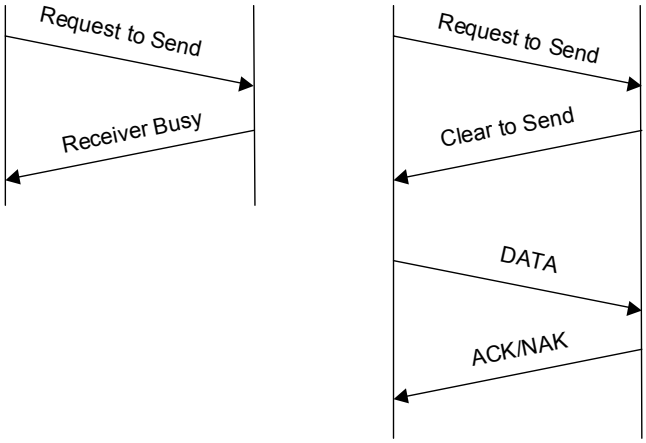
- na rozdiel od klasického Ethernetu, kde je táto metóda použitá tu nemožno naraz vysielať aj prijímať (preto samotná detekcia kolízie je dosť ťažko realizovateľná)
- preto bola táto metóda modifikovaná nasledovne
  - najprv všetci počúvajú, či je ticho
  - pred samotným vysielaním dát sa vysiela tzv. **comb**
  - comb je pseudonáhodná sekvencia, ktorej jednotky sa vysielajú, a počas jej núl sa prepína do prijímacieho módu a počúva, či náhodou nevysiela aj niekto iný
  - keď počas počúvania (nuly) zistím, že vysiela aj niekto iný, tak prestanem vysielať
  - takto sa spravidla dá eliminovať kolízia (samozrejme, najlepšie je „vygenerovať“ si náhodnú postupnosť so samými jednotkami a tak „odstaviť“ ostatných:)
  - samozrejme, keď si dvaja vygenerujú rovnakú postupnosť, tak dôjde ku kolízii
  - cieľom je použiť čo najkratšiu postupnosť, aby bola doba určená na detekciu kolízie čo najkratšia („hluchá doba“ – nevyužívaná efektívne – na prenos samotných dát) a na druhej strane dostatočne dlhú, aby bola vysoká pravdepodobnosť detekovania kolízie

CSMA/CA

- **CSMA with collision avoidance**
- stanice počúvajú, pokiaľ sa vysiela, tak čakajú až kým je ticho
- môžu teda začať vysielať iba keď je ticho, vždy si však pred samotným vysielaním nastavia pseudonáhodný interval, o ktorý počkajú – takto je zabezpečené, že dvaja (s dosť vysokou) pravdepodobnosťou nezačnú vysielať naraz

- ďalší problém, špecifický pre WLANy je fakt, že prijímacia stanica (adresát) nemusí byť v dosahu odosieľateľa
- preto sa pridáva 4-cestná handshake procedúra (načo zbytočne vysielať 1500B, keď je adresát aj tak mimo rádiový (infrared) kontakt?)
- pred samotným vyslaním údajov sa pošle RTS (request-to-send) a prijímacia stanica odpovie buď CTS (clear-to-send) alebo aj nemôže prijímať, tak RxBUSY (receiver-busy). Až potom nasleduje vyslanie DATA, ktoré prijímač potvrdzuje ACK, resp. v prípade chybne prijatého rámca NAK. Samozrejme, všade sú prítomné timeouty.
- pre WLANy sa takto modifikovaná MAC metóda nazýva **distributed foundation wireless MAC (DFW MAC)** – je použiteľná ako pre CSMA/CD, tak pre CSMA/CA.

princíp výmeny správ DFW MAC



TDMA a FDMA

- sú tiež možné aj tieto, pre telekomunikácie klasické metódy zdieľania spoločného média

Ďalšie funkcie MAC podvrstvy pri WLANoch

- medzi MAC funkcie patrí
  - fragmentation
    - pri WLANoch je potrebné fragmentovať na menšie časti, pretože médium je oveľa chybovejšie (BER = 10^{-3} až 10^{-5}) - v porovnaní napr. s koaxiálnym káblom (10^{-9} až 10^{-11})
  - flow control
    - je potrebné sa prispôsobovať fyzickej vrstve, podľa toho, ako sa jej darí odvysielať žiadané rámce (pomocou signálov na interfejse – RTS, CTS)
  - error control
    - je možné zahrnúť samoopravné kódy do DFW MAC (potom to je hybridné ARQ)
  - multiple rate handling
    - spravidla fyzická vrstva poskytuje niekoľko možných prenosových rýchlostí
    - DSSS – 1 až 2 MBPS, Infrared 1,2,4 alebo 10Mbps
    - rýchlosť je volená podľa aktuálnej chybovosti média – začína sa na najnižšej rýchlosti, postupne sa skúšajú lepšie, pokiaľ dochádza k retransmisiám, tak sa rýchlosť znovu znižuje
    - samozrejme na zmene rýchlosti sa musí dohodnúť vysielacia stanica s prijímacou – to sa deje pomocou výmeny riadacich rámcov

Štandardy pre WLANy

- **IEEE 802.11**
  - FHSS, 1, 2Mbps
  - DSSS, 1, 2Mbps
  - Direct modulated Infrared, 1, 2Mbps
- **IEEE 802.11a**
  - OFDM 6, ... 54Mbps
- **IEEE 802.11b**
  - HR/DSSS 1, 2, 5.5 ...11Mbps

  IEEE
  - Carrier modulated Infrared 4 Mbps
  - Multi Sub-Carrier modulated Infrared 10 Mbps

- **ETSI HiperLAN**
  - single carrier offset QPSK, 10 - 20Mbps

IEEE 802.11

základné vlastnosti:

- špecifikácia MAC a PHY pre wireless spojenie fixných, portable a moving stations v rámci local area
- prostredníctvom rádiových a infrared vĺn
- využíva CSMA/CA
- MAC podporuje prevádzku ako pre access point tak aj pre individuálne stanice
- protokol zahŕňa
  - autentikáciu
  - association and reassociation služby
  - procedúry pre enkrypciu/dekrypciu (optional)
  - power management (hlavne pre mobilné stanice)
  - point coordination function pre time-bounded transfer of data
- PHY
  - FHSS 1, 2Mbps
  - DSSS 1, 2Mbps
  - infrared 1, 2Mbps

Rozdielnosť oproti klasickým LAN

a) využíva médium, ktoré nemá pevné hranice
b) nie sú chránené vocí vonkajším signálom
c) komunikujú cez oveľa menej spoľahlivé médium (vysoko chybové)
d) ich topológia je dynamická
e) trpia stratou konektivity, t.j. nemožno jednoznačne predpokladať, že adresát (prijímač) je vždy v dosahu
f) samotné šírenie je časovo premenlivé a často aj nesymetrické

Ďalšie požiadavky na WLANy:

- umožniť komunikáciu nielen pre fixné stanice, ale aj pre ***mobile*** as well as ***portable*** stations
  - *portable* station je taká, ktorú je možné premiestňovať, ale počas používania je fixne umiestnená
  - *mobile* stations využíva prístup k sieťovým prostriedkom aj počas pohybu
- z technického hľadiska vzhľadom na šírenie vĺn a zmeny podmienok, je vhodné považovať pri návrhu všetky stanice za mobilné
- brať do úvahy Power management (hlavne pri mobilných staniciach, ktoré sú napájané z batérií)
- IEEE 802.11 by sa mala pre vyššie vrstvy [logical link control (LLC)] tváriť rovnako ako iné IEEE 802 špecifikácie (napr. 802.3). Z toho vyplýva, že už 802.11 sa musí vysporiadať s mobilitou staníc (aby to zostalo skryté pre LLC)

Architektúra – komponenty:

BSS – basic service set. sú to aspoň dve napriamo komunikujúce stanice (**STA**), využívajúce jednu koordinačnú funkciu (jednu prístupovú metódu). Pokiaľ neobsahuje žiadne iné komponenty (DS, AP), tak sa nazýva **independent BSS (IBSS).** Často je vytvorená bez predošlého plánovania, iba práve podľa aktuálne potreby – preto je často označovaná ako ***ad hoc networ*k**.

BSS môže tvoriť časť rozšírenej formy siete, ktorá je postavená z viacerých BSS. Tieto sú prepojené prostredníctvom tzv. ***distribution systému* (DS).**

IEEE 802.11 robí rozdiel medzi samotným prenosovým wireless médiom (WM) a médiom distribučného systému (DSM). DS poskytuje pre mobilné stanice služby spojené s mapovaním cieľových adries a umožňuje spojitú komunikáciu aj pri prechode z jednej BSS (bunky) do druhej. DS nemusí byť wireless – kľudne môže môže byť použitá klasická 802.x technológia.

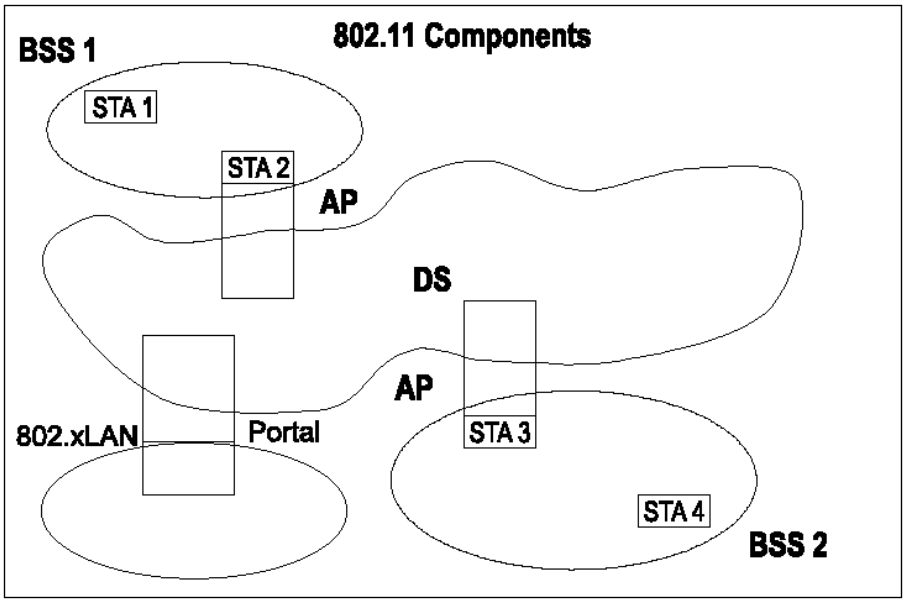
An access point (AP) je stanica, ktorá poskytuje prístup do DS (poskytuje DS službu, okrem toho, že je STA)

DS a BSSs umožňujú vytvárať rôzne veľké a rôzne zložité siete. Takéto komplexné siete sa nazývajú ***extended service set* (ESS)** network.

ESS sa pre LLC tvári rovnako ako IBSS, stanice (hlavne mobilné) sa v rámci ESS môžu premiestňovať a pritom komunikovať tak, že pre LLC je to transparentné.

Častým prípadom je pripojenie WLAN siete do existujúcej, klasickej wired LAN. To je možné vďaka tzv. ***portálu***, čo je logický bod, kde sú rámce (MSDU) z integrovanej klasickej (nie IEEE 802.11) LAN siete prekladané do IEEE 802.11 DS.

nasledovný obrázok znázorňuje vzťahy medzi jednotlivými komponentmi WLAN sietí:



Služby (services)

- IEEE 802.11 explicitne nešpecifikuje detaily DS
- špecifikuje iba služby, ktoré má táto časť architektúry poskytovať ostatným komponentom siete
- The IEEE 802.11 MAC sublayer využíva 3 typy správ (pomocou nich realizuje služby)
  - d*at*a
  - *managemen*t
  - *control* (see
- definuje dva druhy služieb (obe kategórie su používané MAC podvrstvou)
  - station service (SS) – určené na prenos údajov medzi STAs
  - distribution system service (DSS) – určené na LAN access a confidentiality

station services (SS)

- služby, ktoré poskytuje stanica (STA):

a) Authentication

Authentication is used instead of the wired media physical connection. If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established.

It provides link-level authentication between STAs. It does not provide either end-to-end (message origin to message destination) or user-to-user authentication.

b) Deauthentication

Act of deauthentication shall cause the station to be disassociated. Deauthentication is not a request; it is a notification. Deauthentication shall not be refused by either party.

c) Privacy

Privacy is used to provide the confidential aspects of closed wired media. IEEE 802.11 provides the ability to encrypt the contents of messages. This functionality is provided by the privacy service. IEEE 802.11 uses the WEP mechanism to perform the actual encryption of messages.

d) MSDU delivery

distribution system services (DSS)
- služby, ktoré poskytuje distribučný systém (DS):

a) Association
Before a STA is allowed to send a data message via an AP, it shall first become associated with the AP. At any given instant, a STA may be associated with no more than one AP. An AP may be associated with many STAs at one time.

b) Disassociation
The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassoci-ation is a notification, not a request. Disassociation cannot be refused by either party to the association.

c) Distribution
preposielanie prišlých rámcov cez DS na správny AP, a ten ďalej prevysiela do svojho WM. Prebieha na základe databáz v jednotlivých AP, ktoré sa tvoria na základe Association, Deassociation a Reassociation služieb. Štandard samotný nešpecifikuje ako, iba hovorí, že to treba.

d) Integration
If the distribution service determines that the intended recipient of a message is a member of an integrated LAN, the "output" point of the DS would be a portal instead of an AP. The Integration function is responsible for accomplishing whatever is needed to deliver a message from the DSM to the integrated LAN media (including any required media or address space translations).
A samozrejme aj opačným smerom, z Integrovanej LAN do DS.

e) Reassociation
The reassociation service is invoked to "move" a current association from one AP to another.

Multiple logical address spaces
WM, DSM, a pripojená wired LAN môžu byť rozdielne fyzické médiá, a teda aj môžu používať rôzne druhy adresovania. IEEE 802.11 špecifikuje iba WM adresovanie – kompatibilné s ostatnými IEEE 802 48-bit addresnými schémami.
Samotná implementácia DS je ponechaná na výrobcoch, tento štandard ju nešpecifikuje.

MAC management protokol je realizovaný výmenou *MAC management protocol data unit (MMPDU)* medzi peer MAC entitami.

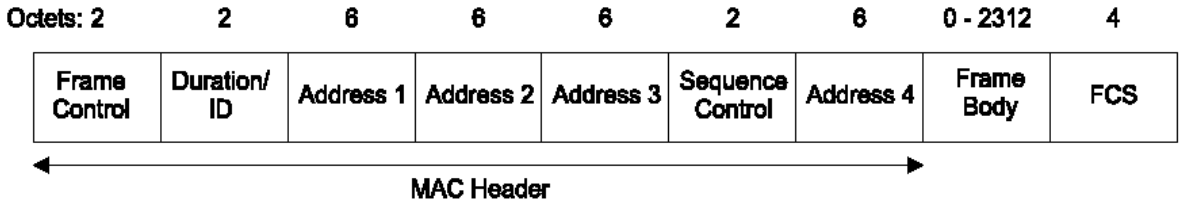
Služby poskytované MAC podrstvou

Asynchronous data service
This service provides peer LLC entities with the ability to exchange MAC service data units (MSDUs). Such asynchronous MSDU transport is performed on a best-effort connectionless basis. There are no guarantees that the submitted MSDU will be delivered successfully.
Broadcast and multicast transport is part of the asynchronous data service provided by the MAC. Due to the characteristics of the WM, broadcast and multicast MSDUs may experience a lower quality of service, compared to that of unicast MSDUs. All STAs will support the asynchronous data service. Because operation of certain functions of the MAC may cause reordering of some MSDUs, there are two service classes within the asynchronous data service (a LLC si môže vybrať, ktorú práve potrebuje)

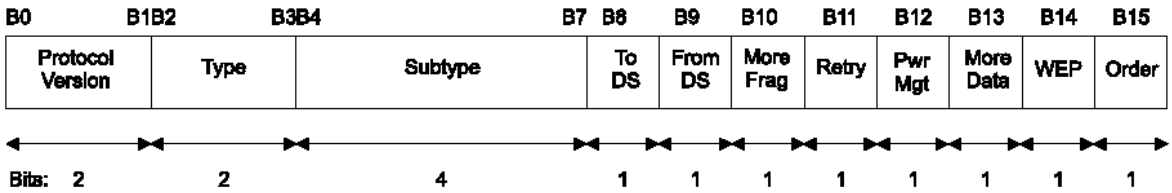
Security services
Security services in IEEE 802.11 are provided by the authentication service and the WEP mechanism. The scope of the security services provided is limited to station-to-station data exchange. The privacy service offered by an IEEE 802.11 WEP implementation is the encryption of the MSDU. Táto služba je transparentná pre LLC.

MSDU ordering
The services provided by the MAC sublayer permit, and may in certain cases require, the reordering of MSDUs. The MAC does not intentionally reorder MSDUs except as may be necessary to improve the likelihood of successful delivery based on the current operational ("power management") mode of the designated recipient station(s). If a higher-layer protocol using the asynchronous data service cannot tolerate this possible reordering, the optional StrictlyOrdered service class should be used.

MAC frame formats



Frame Control field



Duration/ID field
The Duration/ID field is 16 bits in length. The contents of this field are as follows:
a) In control type frames of subtype Power Save (PS)-Poll, the Duration/ID field carries the association identity (AID) of the station that transmitted the frame in the 14 least significant bits (lsb), with the 2 most significant bits (msb) both set to 1. The value of the AID is in the range 1–2007.
b) In all other frames, the Duration/ID field contains a duration. For frames transmitted during the contention-free period (CFP), the duration field is set to 32 768.
Whenever the contents of the Duration/ID field are less than 32 768, the duration value is used to update the network allocation vector (NAV) according to the procedures defined in Clause 9.

Address fields
There are four address fields in the MAC frame format. The usage of the four address fields in each frame type is indicated by the abbreviations BSSID, DA, SA, RA, and TA, indicating basic service set identifier (BSSID), Destination Address, Source Address, Receiver Address, and Transmitter Address, respectively. Each Address field contains a 48-bit address.

Sequence Control field
The Sequence Control field is 16 bits in length and consists of two subfields, the Sequence Number and the Fragment Number. The Sequence Number field is a 12-bit field indicating the sequence number of an MSDU or MMPDU. The Fragment Number field is a 4-bit field indicating the number of each fragment of an MSDU or MMPDU.

Frame Body field
The Frame Body is a variable length field that contains information specific to individual frame types and subtypes. The minimum frame body is 0 octets. The maximum length frame body is defined by the maximum length (MSDU + ICV + IV), where ICV and IV are the WEP fields defined in 8.2.5.

Frame types

Control frames	Data frames	Management frames
Request To Send (RTS) frame format	Data	Beacon frame format
Clear To Send (CTS) frame format		IBSS Announcement Traffic Indication Message (ATIM) frame format
Acknowledgment (ACK) frame format		Disassociation frame format
Power-Save Poll (PS-Poll) frame format		Association Request frame format
CF-End frame format		Association Response frame format
CF-End + CF-Ack frame format		Reassociation Request frame format
		Reassociation Response frame format
		Probe Request frame format
		Probe Response frame format
		Authentication frame format
		Deauthentication

Authentication and privacy

Autentikačné služby

- IEEE 802.11 definuje dva podtypy pre autentikačnú službu:
  - *Open System*
  - *Shared Ke*y.

Autentikáci prebieha vždy medzi práve dvomi zariadeniami – unicastom, buď medzi dvomi STA, alebo STA a AP.

Open System authentication

- v podstate je to nulová autentikácia
- ľubovoľné STA vyžadujúce autentikáciu sa stane autentikovaným ak má prijímacia strana nastavené *dot11AuthenticationType* na *Open System authentication*.
- prebieha v dvoch krokoch
  - identity assertion and request for authentication
  - authentication result
- ak je výsledok „successful“, tak sú obe STAs vzájomne autentikované
- na samotnú autentikáciu tak postačujú dva druhy frejmov

Shared Key authentication

- podporuje autentikáciu podľa toho, či dané STA pozná, resp. nepozná zdieľaný tajný kľúč (shared secret key)
- secret key neposiela v clear texte, vyžaduje však použitie WEP (WEP option musí byť implementované)
- predpokladom je, že shared secret key je doručený do STA cez bezpečný kanál (samotný 802.11 to nerieši:)
- na samotnú autentikáciu sú potrebné 4 druhy frejmov

Wired Equivalent Privacy (WEP) algoritmus

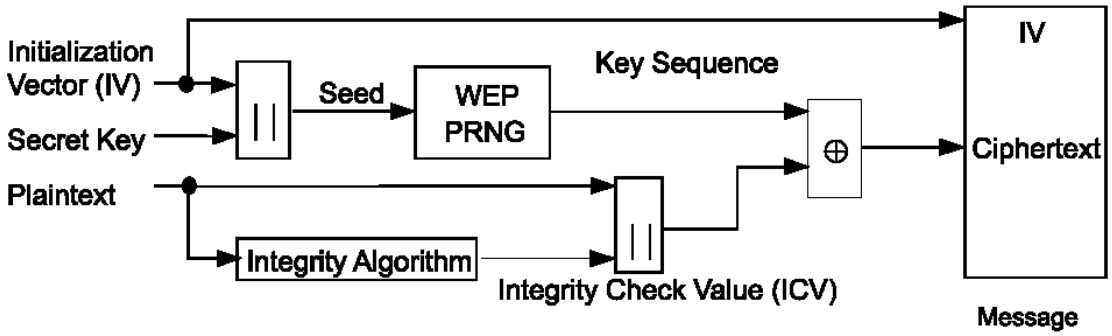
Úvod

- pre wireles-y je typické odpočúvanie (eavesdropping)
- preto 802.11 špecifikovalo mechanizmus na dosiahnutie obdobnej úrovne utajenosti ako pri klasických wired LANoch pomocou tzv. *Wired equivalent privacy (**WEP**)*
- úroveň utajenosti dát záleží na algoritme, ktorým sú distribuované enciphering/deciphering kľúče
-

WEP princíp

- WEP využíva simetrické šifrovanie (ten istý secret key pre šifrovanie aj dešifrovanie)
- secret key je prenášaný osobitným, externým mechanizmom

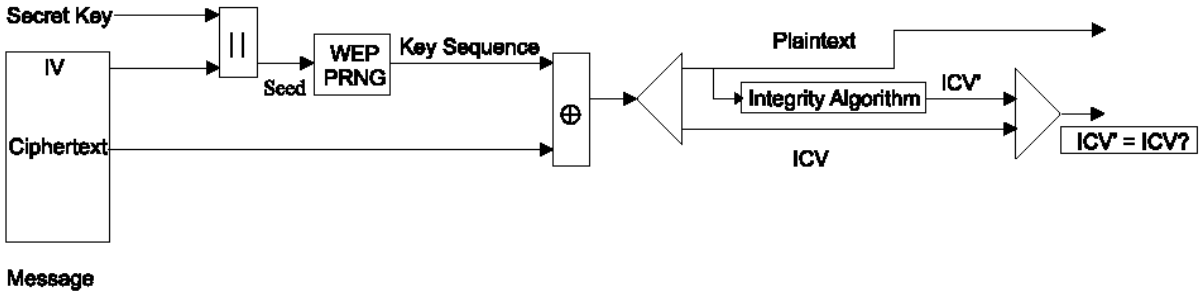
blokový diagram šifrovania pri WEP



- secret key je zreťazený s *initialization vector* (IV) a výsledkom je *seed*
- seed vstupuje do PRNG (pseudo-random generator) a výsledkom je *key sequence k,* ktorého dĺžka je rovná dĺžke prenášaného *plain textu* zväčšeného o *integrity check value* (ICV - 4-bajtové CRC)
- šifrovanie potom spočíva v spojení týchto dvoch reťazcov (XOR-om) do výsledného *ciphertextu*
-

- kritickým komponentomje WEP PRNG, pretože tranformuje rel. krátky secret key na sekvenciu potrebnej dĺžky
- toto zjednodušuje management pri výmene kľúčov medzi STAs
- WEP používa RC4 PRNG algorithm od firmy RSA Data Security, Inc.
- vďaka IV sa použiteľnosť kľúčov predlžuje (lebo stačí meniť IV, a šifrovacia postupnosť je vždy iná)
- možno ho meniť ľubovoľne často, v príncípe môže byť nové pre každý nový frejm
- WEP sa vzťahuje na Frame body časť rámca

blokový diagram dešifrovania pri WEP



- postup pri dekryptovaní je zrejmý zo schémy
- pokiaľ sa pri kontrole ICV nerovná ICV‘ tak sa vyššej vrstve dáta ďalej neposunú (lebo sú pokazené:)

MAC sublayer functional description

- MAC podvrstva zabezpečuje nasledovné služby
  - prístupové metódy DCF a PCF a ich koexistenciu
  - fragmentáciu a defragmentáciu
  - multirate support

Distributed coordination function (DCF)

- základná prístupová metódy, založená na *carrier sense multiple access with collision avoidance* (CSMA/CA)
- je implementovaná na všetkých STAs, či už sú použité v rámci IBSS, alebo infrastructure network konfigurácii
- samotné CSMA/CD rozširuje o použitie RTS a CTS rámcov, a pozitívnych potvrdení (ACK) rámcov
- Carrier sense mechanizmus je kombináciou dvoch metód:
  - fyzickej (klasicky, počúva a vie)
  - virtuálnej – tzv. *network allocation vector (**NAV**)*, čo je predikcia na základe informácií v CTS/RTS rámcoch

Point coordination function (PCF)

- je to optional prístupová metóda
- použiteľná iba pri infrastructure network konfigurácii
- využíva tzv. Point coordinator (PC), ktorým je obyčajne AP, a ten rozhoduje, ktorá STA môže práve vysielať – polluje stanice
- je to tzv. *contention-free* prístupová metóda (tu nedochádza ku kolíziám)
- môže koexistovať súčasne so stanicami pristupujúcimi pomocou DCF, pretože používa kratšie IFS (interframe space), t.j. časovú medzeru, ktorú stanice musia ponechať medzi jednotlivými vysielaniami – „skôr sa vtlačí“ medzi slušné, stochasticky pristupujúce stanice pracujúce algoritmom CSMA/CA (DCF)

Fragmentation

- fragmenuje na malé časti, aby sa zvýšila pravdepodobnosť doručenia správy v nespoľahlivom prostredí
- broadcast/mutlicast rámce sa nikdy nefragmentujú

- samotné malé frejmy môžu byť posielané ako burst v rámci DCF získania média, pri PCF metóde je každé posielané samostatne

Defragmentation

- každý fragmen nesie dostatok informácií na poskladanie pôvodného rámca (Frame type, Source address, Destination address, Sequence control field a More fragment indicator)

Multirate support

- niektoré PHY disponujú možnosťou multirate data transfer-u
- umožňujú tak dynamicky prepínať medzi jednotlivými rýchlosťami a tak optimálne využívať prenosové médium
- samotný spôsob prepínania nie je definovaný v tomto štandarde, ale je definovaná množina pravidiel, ktoré musia byť dodržané, aby bola možná koexistencia viacerých implementácií
- (napr. všetky control frames musia byť vysielané na základnej rýchlosti, aby jej rozumeli všetky STA, rovnako sa to týka broadcastových rámcov...)

Ďalšie funkcie MAC podvrstvy

- synchronizácia
- power management

PHY - fyzická vrstva

FHSS PHY

- frequency hopping spread spectrum pre 2,4 GHz ISM (industrial, scientific and medical) band
- pre každú krajinu sú definované kanály, z ktorých sú vytvorené viaceré hopping sekvencie
- hop rate je ponechaný na jednotlivé zodpovedné organizácie (spravujúce frekvenčné pásma)
- definuje dve funkcie
  - physical medium dependent (PDM)
  - physical layer convergence function
- špecifikuje FHSS PHY pre 1Mbps - 2-level GFSK (Gaussian frequency shift keying)
- špecifikuje FHSS PHY pre 2Mbps - 4-level GFSK (Gaussian frequency shift keying)

DSSS PHY

- direct sequence spread spectrum pre 2,4 GHz ISM (industrial, scientific and medical) band
- je definovaných 14 kanálov (centrálnych frekvencií) – najviac ich možno používať v Amerike, najobmedzenejšie je použitie v Japonsku
- processing gain má byť väčší ako 10dB, preto používa 11-bitový chip PN kód (t.j. baseband signál je chipovaný na 11Mhz) – pomocou Barkerovej sekvencie 10110111000
- špecifikuje FHSS PHY pre 1Mbps - DBPSK
- špecifikuje FHSS PHY pre 2Mbps - DQPSK

Infrared

- 850 – 950 mn
- diffuse infrared transmission (nie na priamu viditeľnosť, stačia odrazy)
- 1 pulz trvá 250ns
- využíva základné prechody pulzov a pulse position moduláciu (PPM)
- samotná rýchlosť je uvedená na začiatku rámca – v poli DR (data rate) a podľa toho sa potom prispôsobí vysielač aj prijímač v ďalších poliach (vysiela sa stále rovnako rýchlo, iba sa kóduje rozdielne:
  - pre basic rate 1Mbs je použitá 16-PPM (4bity/(16x250ns) = 4bity/4μs = 1Mbps)
  - pre extended (optional) rate 2Mbps je použitá 4-PPM (2bity/4x250ns) = 2bity/1μs = 2Mbps)

OFDM PHY (IEEE 802.11a)

- definuje orthogonal frequency division multiplexing (OFDM) systém
- pre použitie v 5GHz pásme (unlicensed national information structure (U-NII) band)
- poskytuje prenosové rýchlosti 6, 9, 12, 18, 24, 36, 48, a 54 Mbit/s, pričom 6, 12 a 54 sú povinné

- systém používa 52 pod-nosných, ktoré sú modulované BPSK, QPSK, 16-QAM alebo64-QAM.
- je použitý Forward error correction coding (convolutional coding) s rýchlosťami 1/2, 2/3, alebo ¾

HR/DSSS PHY (IEEE 802.11b)

- high rate direct sequence spread spectrum systém
- pásmo 2,4Ghz (ISM)
- k pôvodnej špecifikácii okrem rýchlostí 1 a 2Mbps pridáva 5,5Mbps a 11Mbps
- na dosiahnutie vyššej rýchlost sa ako modulačná schéma používa 8-chip complementary code keying (CCK)
- chipping rate je 11 MHz, čo je rovnaké ako pri pôvodnom 802.11 DSSS – zaberá teda rovnaké pásmo
- používa rovnaký formát preambuly a hlavičky – preto môžu vzájomne koexistovať
- okrem toho pridáva ešte niektoré vylepšenia – ale iba ako optional