KOMPIUTERIŲ TINKLAI

8 paskaita

Bevieliai lokalūs tinklai (WLAN)

Maršrutizavimo kartojimas

- Kas yra maršrutizavimo lentelė ir kam ji naudojama?
- Kuo skiriasi statiniai ir dinaminiai maršrutai?
- Kokias metrikas naudoja maršrutizavimo algoritmai, kad nustatytų optimalų kelią iki paskirties tinklo?
- Kuo skiriasi maršrutizavimo protokolai RIP, OSPF?

Istorija

1971 m. buvo sukurtas pirmasis bevielis duomenų perdavimo tinklas **ALOHAnet**.

Tinklo kūrėjas - Havajų universiteto profesorius Norman Abramson.

Pirmąjį tinklą sudarė 7 kompiuteriai, esantys 4 skirtingose salose, kurie komunikavo su centriniu kompiuteriu, esančiu Oaho saloje nenaudodami telefoninio tinklo.

Bevieliai tinklai

Privalumai

- Lengvas tinklo diegimas,
- Didelis prieinamumas
- Paprastas plėtimas
- Paskirstytas (Ad-hoc) arba centralizuotas tinklo modelis
- Prieiga prie terpės - kolizijų išvengimas

Trūkumai

- Jautrūs įvairiems trukdžiams:
  - Buitiniai elektroniniai prietaisai
  - Pastatų konstrukcijoms
- Mažesnis duomenų perdavimo greitis nei laidinių tinklų
- Reikalingas tiesioginis tinklo įrenginių matomumas

Radio bangos

Radio bangos (100 KHz - 300 GHz) **– tai pagrindinė šiuo metu naudojamų belaidžių tinklų perdavimo priemonė.**

Nuo radio bangų dažnio priklauso tokie rodikliai, kaip: ryšio nuotolis, informacijos perdavimo greitis, ryšio priklausomybė nuo oro sąlygų.

Dažnių diapazonai, skirti duomenų perdavimui:

136-174 MHz,

400-512 MHz,

820-960 MHz,

2,4GHz, 5GHz,

10-12 GHz,

30-35 GHz ir didesni.

Kuo didesnis dažnis, tuo didesnis gali būti duomenų perdavimo greitis, mažesnis nuotolis, aukštesni reikalavimai tiesioginiam matomumui ir didelis jautrumas, oro permainomis.

Antena

Kiekvienas bevielis tinklo įrenginys turi anteną.

Antenos gali būti:

- **Parabolinės** - kryptinės
- **Izotropinės** ($\lambda/4$ ilgio tiesus laidininkas) – nekryptinės

Kryptinės antenos perduoda radio bangas tam tikra kryptimi.

Nekryptinės antenos skleidžia bangas aplink save tam tikru spinduliu, sudarydamos zoną, kurioje gali bangas priiminėti kiti tinklo įrenginiai.

Sujungimai

Taškas-taškas

Tai toks dviejų įrenginių sujungimas, kai jie sujungiami vienas su kitų lyg tai būtų padaroma laidu.

Radio relejinė linija

Tai modifikuotas taškas-taškas sujungimas, kai į vieną liniją sujungiama keletą bokštų su parabolinėmis antenomis. Tokios linijos naudojamos magistraliniuose telekomunikaciniuose tinkluose.

Sujungimai

Vienas - Daug

Tai toks sujungimo būdas, kai vienas siųstuvas sujungia su keletu imtuvų. Siųstuvas vadinamas bazine stotimi.

Dažniausiai bazinė stotis yra taškas, per kurį imtuvai patenka į kitus tinklus, todėl ji dar vadinama **prieigos tašku** (access point).

Daug - Daug

Tai decentralizuotas sujungimų būdas, kai sudaroma bendra elektromagnetinių bangų terpė, kur kiekvienas įrenginys yra ir siuntėjas ir gavėjas (ad-hoc tinklai).

Plačiajuostis signalas

Radio signalas, naudojamas diskretinių duomenų perdavimui nėra vienalytis t.y. naudojami tam tikra dažnių juosta, bei sikritingų dažnių signalų moduliacijos dažninė ir fazinė.

Naudojama tokios signalo kodavimo technikos:

- Ortogonalus dažninis multipleksavimas (OFDM)
- Spektro plėtimas šuoliuojančiais dažniais (FHSS)
- Tiesinės sekos spektro sklaidos technologija (DSSS)

Bevieliai lokalūs tinklai

Bevieliais tinklais laikomi tokie duomenų perdavimo tinklai, kuriuose duomenų perdavimui naudojamos elektromagnetinės bangos.

Bevielius lokalius tinklus apibrėžia tokie IEEE standartai:

- **IEEE 802.11** – žinomas kaip **WiFi**, bangos dažnis 2,4 GHz (12 kanalų) arba 5 GHz (40 kanalų), CSMA/CA perdavimo būdas
- **IEEE 802.15** – Wireless Personal Area Network (WPAN), žinomas kaip **Bluetooth**.
- **IEEE 802.16** – Worldwide Interoperability for Microwave Access, žinomas kaip **WiMax**.

IEEE 802.11

802.11 standartas – tai bevielių lokalių tinklų technologijos standartas, nustatantis signalo perdavimo metodus fiziniame OSI lygmenyje.

1997 m. standartas nustatė 3 perdavimo būdus:

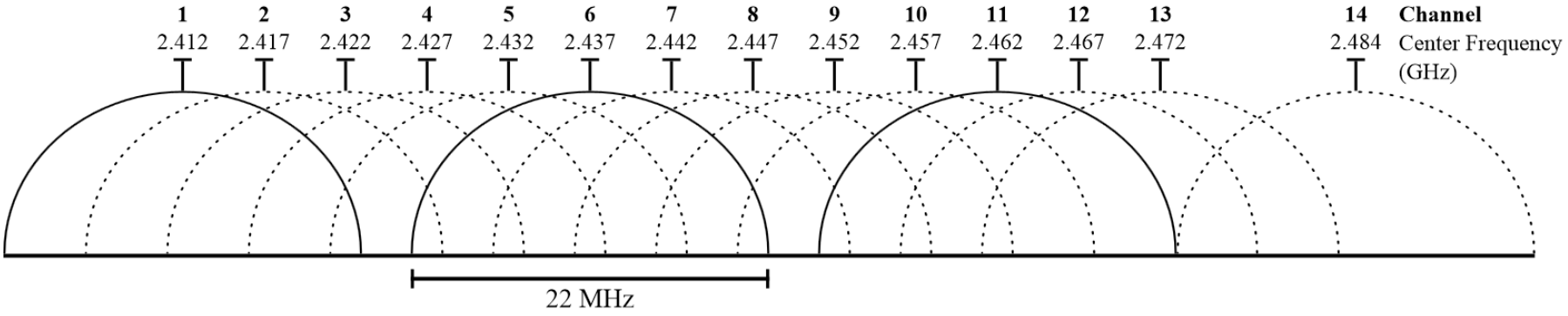
- 850 nm infraraudonieji spinduliai (1 ir 2 Mbps)
- 2,4GHz DSSS bangos (1 ir 2 Mbps)
- 2,4GHz FHSS bangos (1 ir 2 Mbps)

Lokalaus bevielio tinklo diametras nuo 100 iki 300 metrų. Diametro dydis priklauso nuo siųstuvo **galingumo**.

IEEE 802.11

1999 ir 2003, 2009 m. standartas buvo papildytas:

- 802.11a – 5GHz, OFDM, iki 54 Mbps
- 802.11b – 2.4GHz, iki 11 Mbps
- 802.11g – 2.4GHz, OFDM, iki 54 Mbps
- 802.11n – greitis 600 Mbps, ECC, 4 kanalinis perdavimas, palaikoma kadrų agregacija, saugumas.



Topologija

Bazinių paslaugų rinkinys (BSS) – tai tinklo įrenginiai ir jų sukurtas bevielis tinklas. Čia nėra tinklo valdymo. Kiekvienas BSS turi savo ID.

I**šplėstinis bazinių paslaugų rinkinys** (ESS) – tai aibė sujungtų BSS. Prieigos taškas sujungia paskirstytas sistemas. Kiekvienas ESS turi ID, vadinamą SSID (32 baitai).

Paskirstytos sistemos (DS) sujungia prieigos taškus ir ESS. Paskirstytų sistemų tikslas – sujungti bevielius tinklus ir plėsti jų dydį.

Bevielio tinklo topologijos:

- Taškas-taškas vieno BSS rėmuose
- Vienas BSS su prieigos tašku
- Atskiri BSS sujungti dviem prieigos taškais

Perdavimo rėžimai

Bevieliuose tinkluose MAC lygis realizuojamas naudojant tokius rėžimus:

- Paskirstytas DFC (Distributed Coordination Function)
- Centralizuotas PCF (Point Coordination Function)

Bevieliuose tinkluose naudojamas CSMA/CA metodas, pagal kurį kiekvienas kadras turi būti patvirtintas. Jei per tam tikrą laiką negaunamas patvirtinimas, laikoma, kad įvyko kolizija.

DFC rėžimas

DFC rėžimo etapai:

- Prieš perduodant kadrą, vykdomas terpės klausimasis
- Aptikus laisvą terpę, laukiama tam tikras tarpkadrinis laikas (IFS)
- Jei per IFS nebuvo užtimta terpė, laukiamas tam tikras taimerio slotų skaičius. Slotų skaičius apskaičiuojamas naudojant eksponentinį atidėjimo dvejetainį algoritmą.
- Sloto dydis lygus 28 mks (FHSS) arba 1 mks (DSSS).
- Jei per laukiamų slotų skaičių terpė lieka neužimta, tuomet vykdomas kadrų perdavimas.

PCF rėžimas

PCF rėžimas naudojamas, kai BSS tinklas turi prieigos tašką. **Išskiriami tokie PCF etapai:**

- Tinklo įrenginiai prieš siųsdami kadrą stebi terpę. Kai terpė būna laisva, prieš siunčiant būtina palaukti tam tikrą laiko intervalą (SIFS, PIFS, DIFS).
- Po to perduodamas kontrolinis kadras, rodantis, kad įrenginys ketina perduoti duomenis, po kurio prasideda duomenų kadro perdavimas.

Centralizuotas valdymo metodas PCF:

- Naudojamas specialus kadras, kurį gavęs įrenginys gali perduoti duomenų kadrą.

Saugumas

Kadangi prie bevielės duomenų perdavimo terpės gali bet kas prisijungti, todėl paprastai perduodami duomenys tokiame tinkle šifruojami.

Dažniausiai naudojamai tokie šifravimo algoritmai:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access**,** *IEEE 802.11i*)
- WPA2 (Wi-Fi Protected Access 2)

WEP

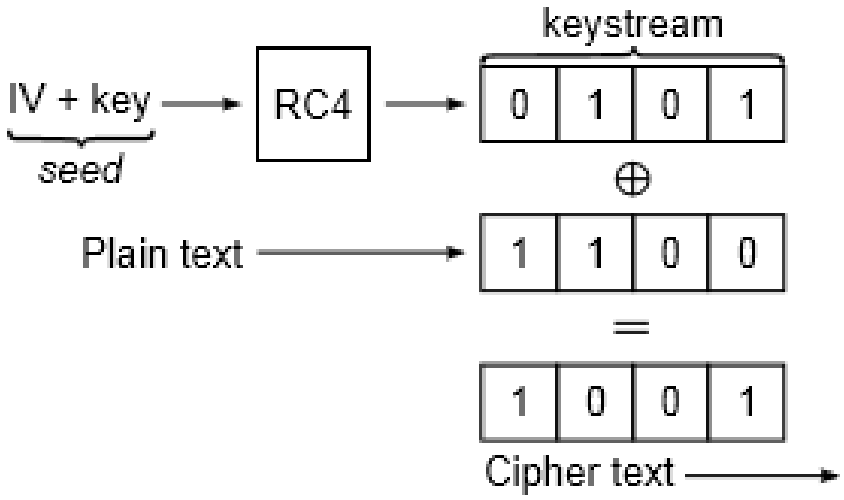
Wired Equivalent Privacy (**WEP**) – tai duomenų šifravimo algoritmas, apibrėžtas IEEE 802.11 standarte ir naudojamas bevieliuose tinkluose nuo 1999.

WEP naudoja 10 arba 26 šešioliktainių skaičių raktą (64, 128 bitus).

Standartinis 64-bitų WEP algoritmas naudoja 40 bitų raktą, kuris sujungiamas su 24 bitų inicializacijos vektoriumi (IV) ir suformuoja RC4 raktą.

WEP raktas įvedamas kaip 10 šešioliktainių simbolių (10x4bitai). Pridėjus 24-bitų IV, gaunamas 64-bit WEP raktas.

WEP



WEP autentifikacijai naudojami du metodai:

- Atvirų sistemų autentifikacija (Open System authentication)
- Bendro rakto autentifikacija (Shared Key authentication)

WEP protokolas nesaugus, dar 2001 m. jis buvo nulaužtas (*pvz. galima pasinaudoti programa aircrack-ng*).

WPA

Wi-Fi Protected Access (**WPA**) ir **Wi-Fi Protected Access II** (**WPA2**) yra du saugos protokolai ir saugos programos, sukurtos Wi-Fi Aljanso. Šie protokolai buvo sukurti, kaip atsvara nesaugiam WEP protokolui.

WPA tapo *IEEE 802.11i* standartu 2003 m.

WPA2 buvo įtrauktas į *IEEE 802.11i* standartą 2004 m.

WPA naudoja Temporal Key Integrity Protocol (TKIP), pagal kurį kiekvienam paketui dinamiškai generuojamas skirtingas 128 bitų raktas. Tai žymiai saugiau nei WEP.

WPA2 (saugesnis protokolas) naudoja naują stiprų AES šifravimo protokolą.

Tapatybės valdymas

WPA apibrėžia dviejų tipų tapatybės valdymo sistemas:

- **WPA-Personal** arba dar vadinamą *WPA-PSK* (Pre-shared key). Ji sukurta namų vartotojams ir mažoms įmonėms ir nereikalauja autentifikacijos serverio. Kiekvienas įrenginys autentifikuojamas prieigos taške naudojant tą patį 256-bitų raktą, sugeneruotą iš slaptažodžio.
- **WPA-Enterprise** dar vadinamas *WPA-802.1X*. Šis autentifikacijos metodas sukurtas įmonėms ir jis realizuojamas naudojant RADIUS serverį. Extensible Authentication Protocol (EAP) yra naudojamas autentifikacijai.

RADIUS

RADIUS (angl. *Remote Authentication Dial In User Service*) - tinklo protokolas, leidžiantis centralizuoti **autentifikacijos** (prieigos), **autorizacijos** ir **apskaitos** valdymą tinklo naudotojams arba įrenginiams.

Autentifikacija

Kai tinklo naudotojas arba įrenginys atpažįstamas kaip teisingas ir prijungiamas prie tinklo, įvyksta **autentifikacija**.

Autorizacija

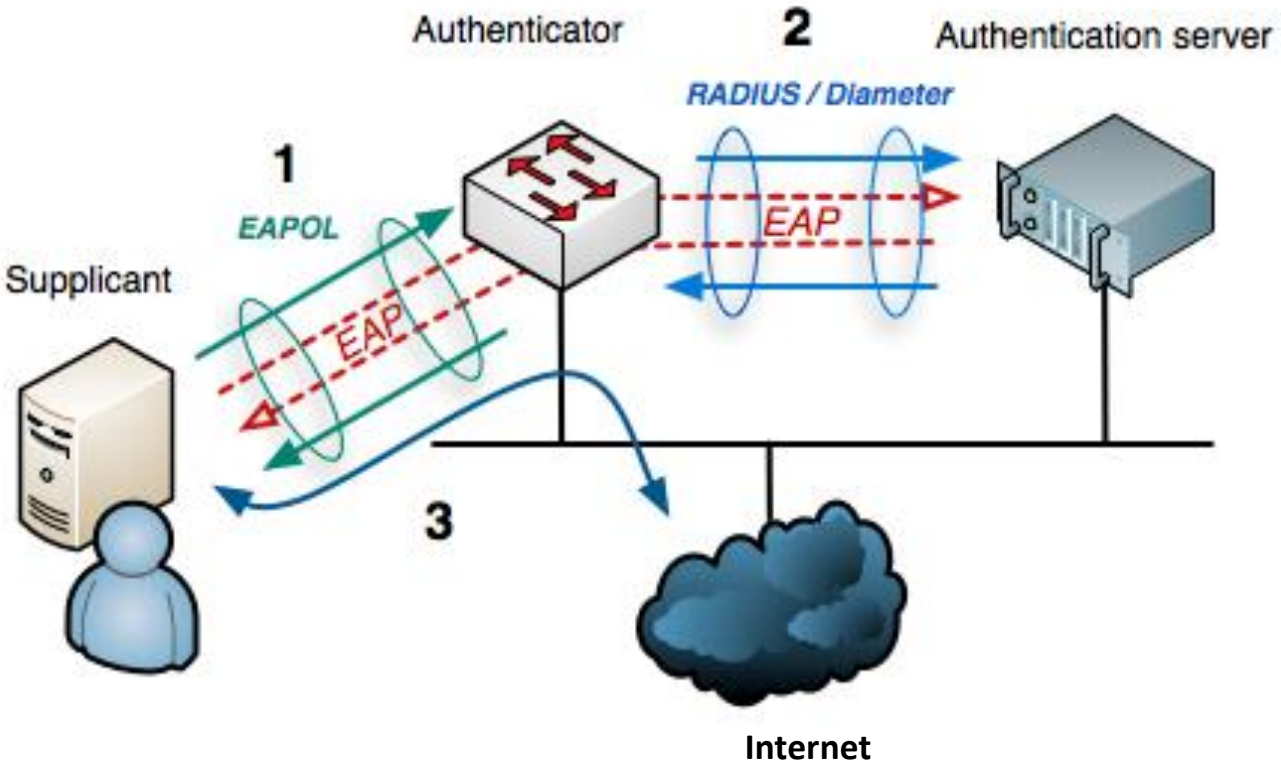
Autentifikavus naudotoją, RADIUS tarnybinė stotis nustato, kokios prieigos teisės yra suteiktos naudotojui.

Apskaita

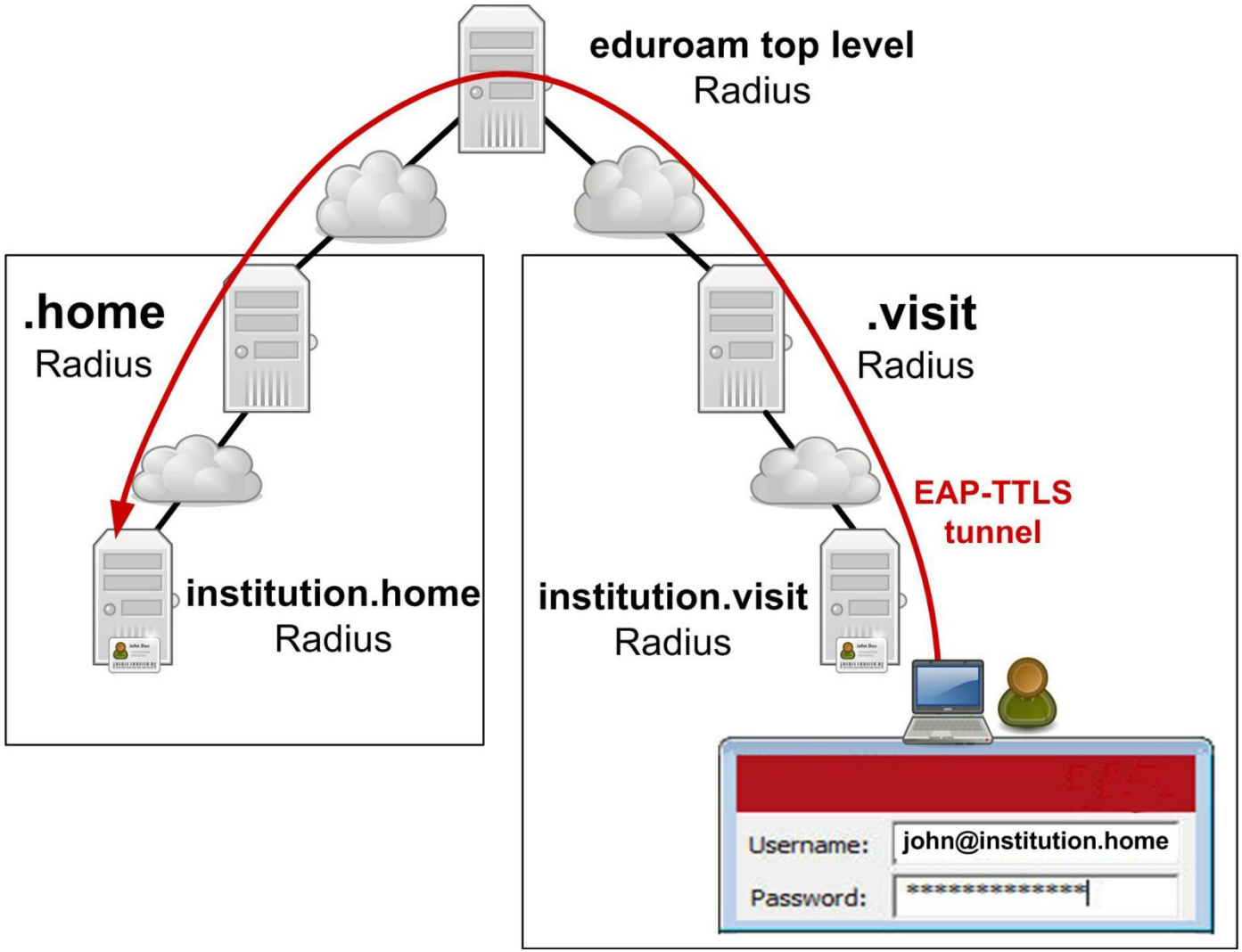
Įrašai apie įvykius (pvz. sėkmingą ar nesėkmingą vartotojo autentifikaciją, autorizaciją, atsijungimą) bei sėkmingo prisijungimo statistika (pvz. prisijungimo metu persiųstas duomenų kiekis) registruojami ir saugomi tarnybinės stoties apskaitos žurnale, t. y. vyksta **apskaita**.

Prieigos valdymas

Prieigos valdymas pagal IEEE 802.1X standartą, kuris nustato autentifikacijos mechanizmą, panaudojant EAP protokolą.



Naudotojų autentifikacija



Bluetooth

Bluetooth technologija specifikuota IEEE 802.15.1 standarte (1994 m).

Bluetooth technologija skirta mažiems personaliniams tinklams PAN (diametras 10-100 m.)

Bluetooth tinkle gali būti iki 255 įrenginių, tačiau tik 8 įrenginiai vienu metu gali perduoti duomenis.

Bluetooth tinkle vienas įrenginys yra pagrindinis, kiti jam pavaldūs (master-slave).

Bluetooth įrenginiai dirba 2.4 GHz dažnių diapazone.

Teorinis duomenų perdavimo greitis:
1 (ver.1), 3 (ver.2) , 24 (ver.3) Mbps.

Prisijungimas prie Bluetooth

Pagrindinis Bluetooth tinklo įrenginys vykdo įrenginių apklausą. Jei aptiktas kitas įrenginys nori prisijungti prie tinklo, pradedamas autentifikacijos procesas – siunčiami prisijungimo kodai.

Jei kodai patvirtinami, įrenginys prijungiamas prie tinklo.

Bluetooth tinkle perduodami duomenys šifruojami.

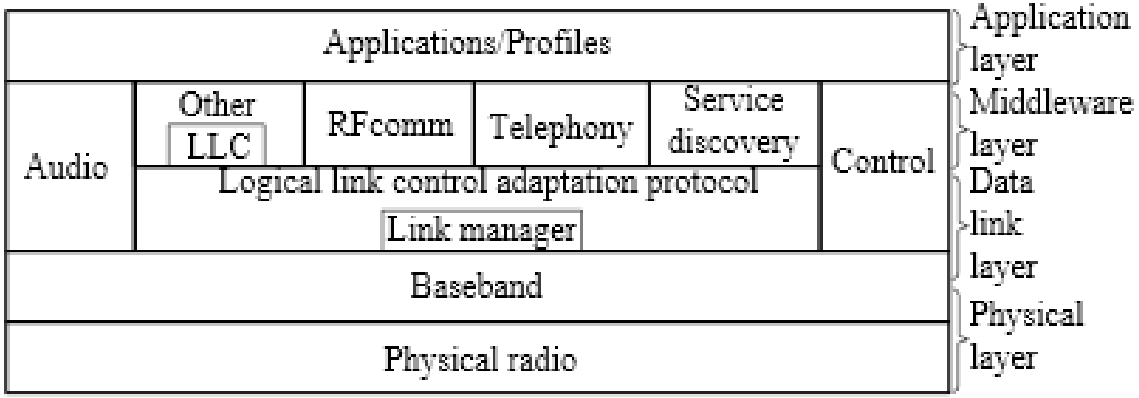
Kolizijų išvengimui tinkle naudojamas CDMA metodas.

Bluetooth protokolų stekas

Bluetooth turi savo originalų protokolų steką dėl išskirtinumo dirbant su paprastais tinklo įrenginiais (telefonais, PDA, ausinė, klaviatūra, pelė ir t.t.). Jie apima fizinį ir MAC lygius.

Bluetooth protokolų steką sudaro tokie lygmenys:

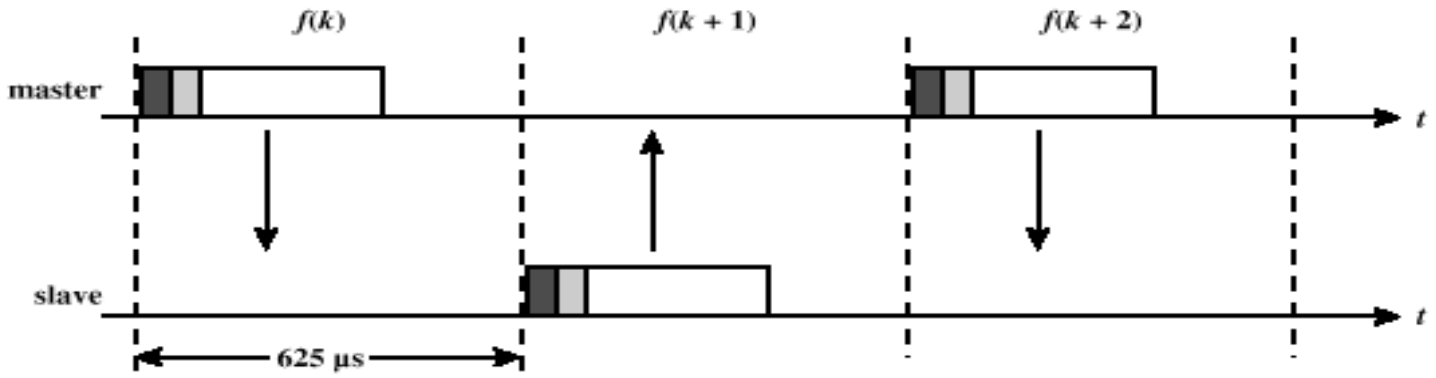
- Fizinių radio signalų
- Bazinių dažnių diapazono
- Kanalų dispečerio
- LLC adaptacijos
- Valdymo



Bluetooth

- Bluetooth naudoja 625 μs slotų kanalus. A Time-Division Duplex (TDD) schema naudojama full duplex rėžimui. Informacija apsikeičiama siunčiant kadrus. Kiekvienas kadras perduodamas skirtingu dažniu. Kadro persiuntimas paprastai trunka vieną laiko slotą, bet gali užimti iki 5 slotų.

- Slotai gali būti rezervuoti sinchroniniam perdavimui. Bluetooth palaiko asinchroninius duomenų kanalus, iki trijų sinchroninių balso kanalų ir kanalą, kuris gali dirbti sinchroniniu ir asinchroniniu būdu.



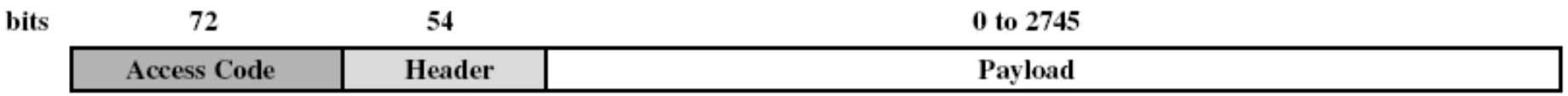
Bluetooth kadrai

Bluetooth dirba 2.4 - 2,4835 GHz dažnių diapazone.

Kanalo plotis 1 MHz, kanalų skaičius 79 (JAV ir kt. šalys).

Bluetooth keičia dažnį tokiu principu:

- 2.402 + *k* MHz, kur *k* =0, …, 78
- 1,600 šuolių per sekundę dažniu.



Bluetooth kadrai

Bluetooth kadro laukai:

- Duomenų laukas skirtas duomenims talpinti
- Prieigos kodas naudojamas indentifikuoti PAN. Kiekvienas įrenginys turi unikalų 6 baitų adresą. Tinklo adresui naudojami 3 žemesnieji baitai.
- Kadro antraštėje yra:
  - MAC adresas
  - Priėmimo patvirtinimo kodas
  - Kadro tipas
  - Eilės numeris