

POVEZAVNA PLAST

Tvorjenje okvirjev

Eden od načinov tvorjenja okvirov je zasnovan na **štetju znakov** v okviru. V glavi paketa označimo njegovo dolžino. Sprejemnik lahko s pomočjo štetja sprejetih znakov ugotovi, kdaj je okvira konec. Na prvi pogled je metoda zelo privlačna. Na žalost ima opisani pristop večjo slabost, če pride do napake pri prenosu na mestu, kjer pričakujemo informacijo o dolžini paketa. Mehanizma za reševanje take situacije ni.

Drugi način za določanje meja med okviri je uvedba posebnih znakov, ki označujejo **začetek in konec okvira**. Protokol BSC (Binary Synchronous Control) deluje na sledeč način: začetek paketa označi z znakom DLE (Data Link Escape), ki mu sledi STX (Start of Text); konec paketa pa za DLE in ETX (End of Text). Če se v podatkovnem delu pojavi znak DLE-STX ali DLE-ETX ima oddajnik nalogo da pred ta DLE vrine še en DLE znak. Na ta način sprejemnik ve, da gre za podatek in ne za znak, ki označuje konec ali začetek okvira.

V tem primeru je najmanjši informacijski delček znak. Pravimo, da je okvir znakovno orientiran. Kot informacijska enota v okviru se lahko pojavi tudi bit, tedaj pravimo, da je okvir bitno orientiran.

Odkrivanje napak pri prenosu

Pri prenosu okvira po prenosnem mediju se lahko dogajajo napake: enica med prenosom mutira v ničlo ali obratno. Če pride do take napake, moramo okvir poslati ponovno.

Najpreprostejši način je odkrivanje napak v okviru s pomočjo **paritetnega bita**. Pariteni bit ne odkrije napak če pride do dvojne ali četvorne napake. Tak način zaščite je zato primeren le za zelo zanesljive kanale ali za kratka sporočila.

Za večje pakete se zato uporablja kompleksnejši model zaščitne kode, ki ima podobno vlogo kot paritetni bit, le da namesto enega bita zahteva več bitov, navadno 16, za **ciklično redundančno kodo – polinomski izračun** $g(x) = x^{16} + x^{12} + x^5 + 1$.

Za zagotavljanje ponovnega pošiljanja se na drugi protokolni plasti lahko uporablja kateri koli mehanizem potrjevanja, ki smo jih že obdelali.

Protokoli

Protokole na povezavni plasti delimo po najbolj očitni lastnosti na:

- tiste, ki podpirajo dvotočkovne prenosne kanale
- tiste, ki podpirajo skupinske prenosne kanale

Protokole, ki podpirajo skupinski prenosni medij, dalje delimo v tri skupine:

- kolizijski protokoli:
 - brez prisluškovanja zasedenosti kanala
 - s prisluškovanjem zasedenosti kanala
- protokoli z omejeno kolizijo
- rezervacijski protokoli

Za skupinski medij je značilna možnost trka paketov na prenosnem mediju. To je regularen dogodek, ki ga mora protokol povezavne plasti obvladati.

Dvotočkovni protokoli

Nekateri dvotočkovni protokoli povezovalne plasti so:

- HDLC – High-level Data Link Control: tipičen predstavnik protokola izdelan po ISO/OSI referenčnem modelu. Nastal je na podlagi IBM-ovega protokola SDLC - Synchronous Data Link Control (protokol iz IBM SNA arhitekture).
- SLIP – Serial Line Internet Protocol: znakovno orientirani protokol, ki se največ uporablja za terminalske serijske dostop do Interneta.
- PPP – Point to Point Protocol: dvotočkovni protokol za povezavo na Internet – grafična povezava.
- ATM – Asynchronous Transfer Mode: novejša tehnologija, zasnovana na paketih (fiksne velikosti 53 byte, od tega 48 byte za podatke, 5 za delovanje), ki jim pravimo celice. Velike hitrosti 155 Mbit/s in 622 Mbit/s. Zadoščajo tudi za digitalni TV prenos.

Kolizijski protokoli

Značilnost vseh kolizijskih mehanizmov, ki omogočajo borbo oddajnikov za dostop do skupnega medija, so neprestani trki paketov. Za reševanje nastale situacije poskrbijo protokoli sami.

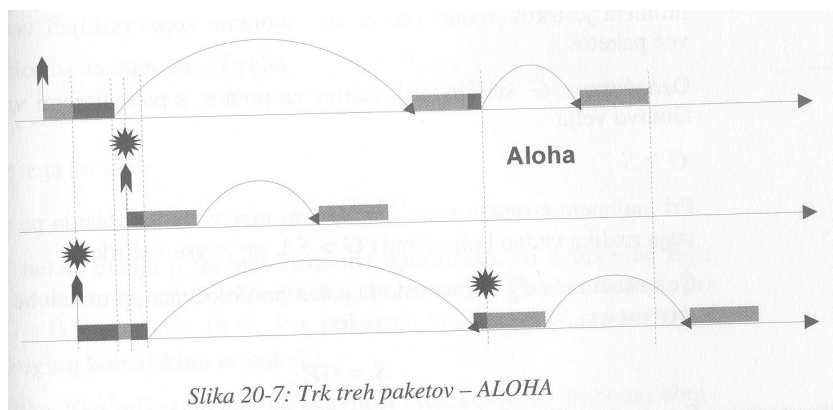
ALOHA

Protokol ALOHA spada že v zgodovino, saj so ga prvič uporabili že leta 1970, ko so na isti radijski frekvenci povezali računalnike na različnih otokih havajskega otočja. Za ALOHA je značilno, da oddajnik ne upošteva morebitne zasedenosti prenosnega kanala. Pogosto začne oddajati paket kljub temu, da se že prenaša nek drug paket. Zaradi trka se seveda uničita oba.

Mehanizem delovanja protokola je naslednji:

- Oddajnik odda paket, kadar se mu zahoče. Hkrati funkcionira tudi kot sprejemnik – sprejema svoj paket.
- Paket je oddan. Oddajnik ugotavlja ali je sprejeti paket enak oddanemu. Če sta enaka, potem ni prišlo do trka in je paket verjetno uspešno prišel na cilj. Če nista enaka je verjetno prišlo do trka, kar pomeni da morajo vsi oddajniki pošiljanje paketa ponoviti.
- V primeru kolizije oddajniki ne začnejo takoj s ponovno oddajo. Vsak od njih sproži naključno časovno kontrolo in šele po njenem izteku ponovi oddajo.

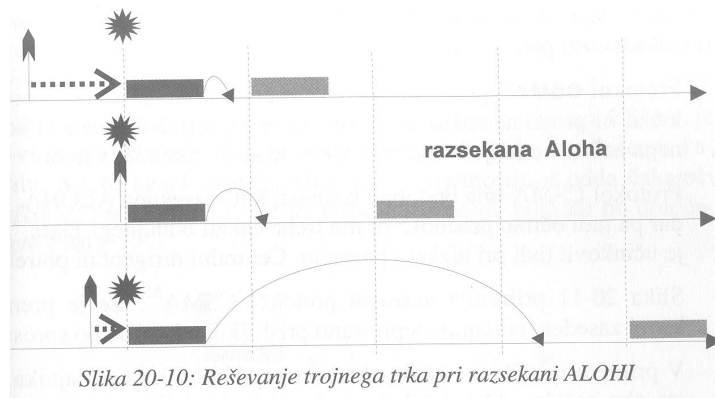
Protokol je preprost in tudi cena njegove izvedbe je nizka, ima pa slabo lastnost, da je izkoriščenost prenosnega kanala le 18%.



RAZSEKANA ALOHA

ALOHA je potrebovala izboljšave. Prva izboljšava je v tem, da smejo oddajniki oddajati paket le v

določenem taktu, ne več ob poljubnem času. Takt je naravnana na največjo dolžino paketa, kar pomeni, da je paket, ki se je srečno začel prenašati, do konca varen pred trkom. Ostale lastnosti so kot pri osnovni ALOHI. Razsekana izvedba ALOHE je dražja, saj potrebuje dirigenta.



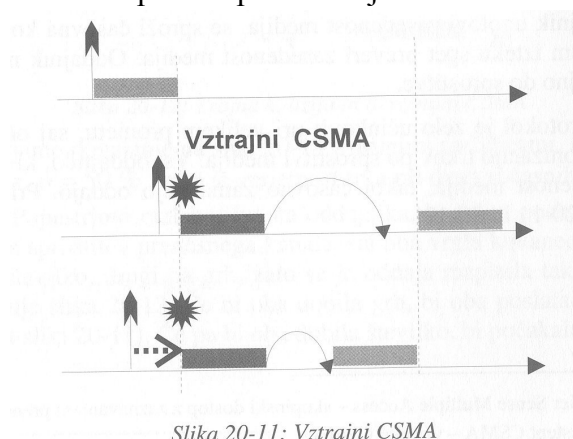
Teoretično je maksimalna propustnost tega protokola 36% kapacitete medija. Razsekani protokol se pri večjem prometu obnaša bolje kot osnovna ALOHA, nekoliko pa izgublja pri nizkem prometu, saj mora tudi osamljen paket čakati na začetek oddajnega intervala.

CSMA (IEEE 802.3)

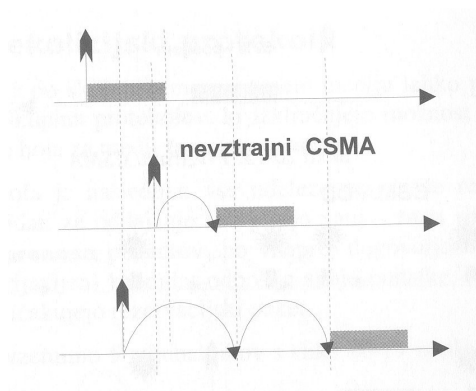
kolizija – trk

CSMA – Carrier Sense Multiple Access: je kvaliteten mehanizem največkrat uporabljen pri topologiji vodila. Ta mehanizem uporablja trk ali kolizijo podatkov na mreži. Je največ časa na tržišču in ima najširšo nameščeno stopnjo. Karakterističen je za topologijo vodila. Protokol pred oddajo paketa preveri, ali je kanal prost. Če kanal ni prost ne začne oddajati. Še vedno obstaja možnost sočasnega začetka oddaje, vendar je paket, ki se že oddaja, varen.

Vztrajni CSMA je različica protokola, pri katerem oddajnik neprestano prisluškuje, kdaj se bo medij sprostil. Izkoriščenost kanala pri tem protokolu je že 52%.

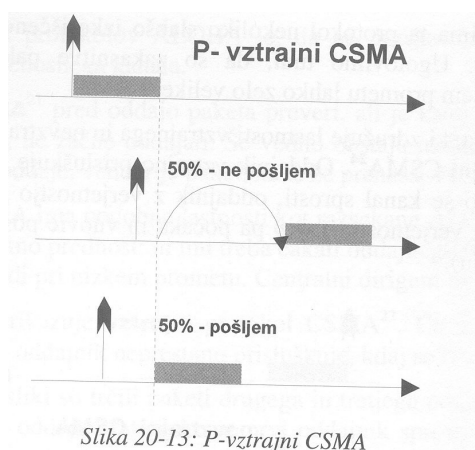


Druge različice CSMA protokola je **nevztrajni CSMA**. Takoj, ko oddajnik ugotovi zasedenost medija, se sproži časovna kontrola. Po njenem izteku spet preveri zasedenost medija. Oddajnik ne posluša vztrajno do sprostitve.



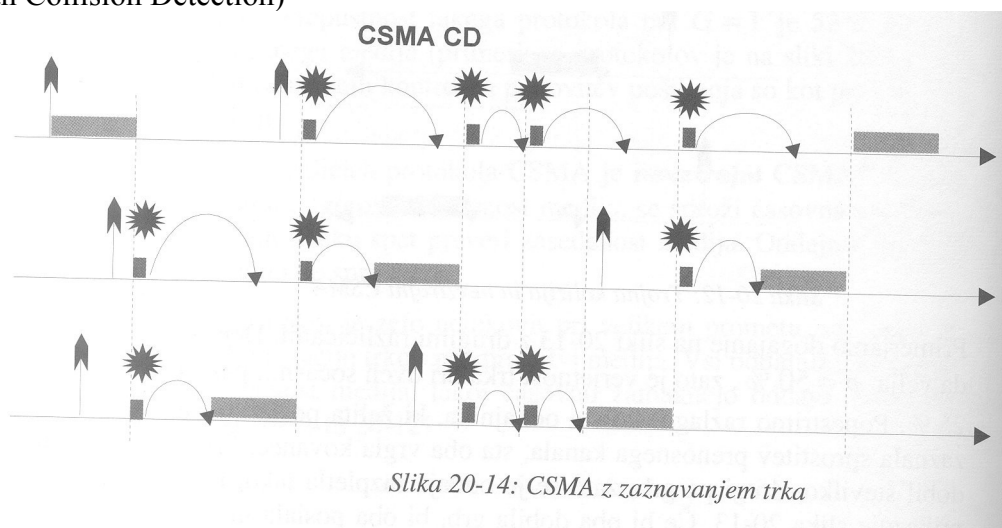
Slika 20-12: Trojna kolizija in nevztrajni CSMA

Različica, ki združuje lastnosti vztrajnega in nevztrajnega CSMA je ***p-vztrajni CSMA***. Oddajnik vztrajno prisluškuje zasedenemu kanalu. Ko se kanal sprosti, oddajnik z p verjetnostjo odda čakajoči paket – z verjetnostjo $1-p$ pa počaka in nato ponovno poskusi po določenem času.



Slika 20-13: P-vztrajni CSMA

Pri vseh dosedanjih različicah se oddajanje paketa nadaljuje tudi po trku. Če oddajniku omogočimo ugotavljanje trka, lahko takoj po trku ustavi oddajo in ne zapravlja že vnaprej izgubljenega časa. Tak protokol imenujemo CSMA/CD – vztrajni CSMA z zaznavanjem trka. (Carrier Sense Multiple Access / with Collision Detection)

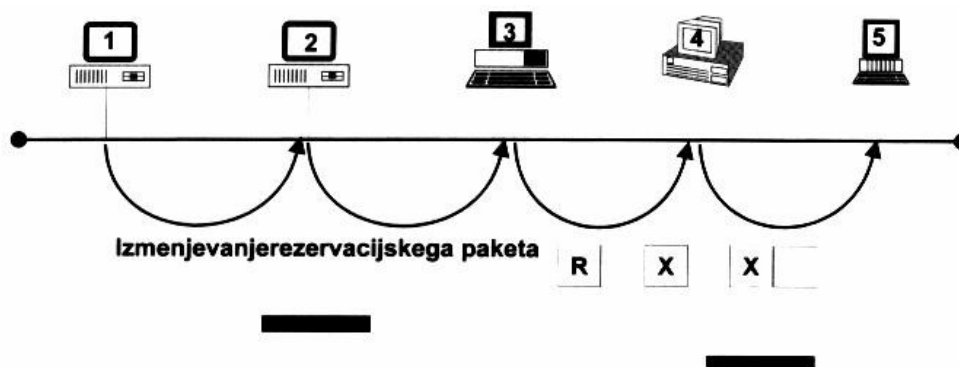


Slika 20-14: CSMA z zaznavanjem trka

Ta različica je standardizirana kot IEEE 802.3, njeno komercialno ime pa je Ethernet. Ta protokol ima dve tipični fazi: fazo prenosa podatkov in fazo borbe za medij, ko prihaja do trkov.

Nekolizijski protokoli

Komunikacija po skupinskem prenosnem mediju se lahko odvija tudi brez trkov. Grupa protokolov, ki izključujejo možnost trkov, ima namesto faze borbe za medij **fazo rezervacije**.



Ideja protokola je naslednja: vse udeležence obišče rezervacijski paket. Kandidati za oddajanje se vpišejo vanj – **faza rezervacije**. Sledi faza prenosa podatkov: po vnaprej dogovorjenem vrstnem redu vsak prijavljeni kandidat odpošlje svoje podatke. Nato udeleženci spet pričakujejo rezervacijski paket.

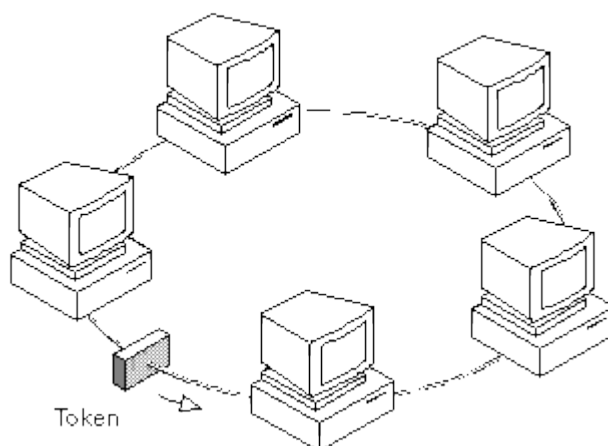
Zanimiva različica rezervacijskega protokola je **protokol z žetonom**. Žeton si lahko predstavljamo kot paket – vagonček, ki potuje od postaje do postaje:

1. začetku je žeton prazen.
2. Postaja, ki želi oddajati, natovori žeton s podatki in ga odpošlje. Ker je žeton poln, naslednje postaje ne morejo oddajati.
3. Ponorna postaja podatke raztovori in odda prazen žeton.
4. Postaja, ki ne želi oddajati, preda naslednji postaji prazen žeton.

Poznamo dve komercialni različici protokola za žetonom: obroč z žetonom in vodilo z žetonom.

TOKEN PASSING RING (IEEE 802.5):

Token Passing Ring: Ta mehanizem je manj svoboden od CSMA, vrstni red komunikacij je določen. Je mehanizem, ki uporablja distribuiran koncept dela, vendar ne s tako svobodo dostopa na medij kot CSMA. Njegova posebnost je žeton, ki neprestano potuje po mreži. Tista delovna postaja, ki žeton pobere iz mreže, lahko odda sporočilo.



Ta mehanizem je značilen za topologijo obroča. Namenjen je izključno komunikaciji točka-točka. Vsaka vmesna postaja žeton sprejme, prebere, očisti, ojača in pošlje naprej.

Sporočilo sestavi in ga posreduje nižjim komunikacijskim nivojem najvišji nivo. Po obdelavi sporočila sprejme povezovalni nivo, vpiše naslov oddajne in sprejemne postaje, doda polje za ugotavljanje napak pri prenosu, označi začetek in konec sporočila, ter ga shrani v pomnilnik (buffer). Potem pa čaka na žeton.

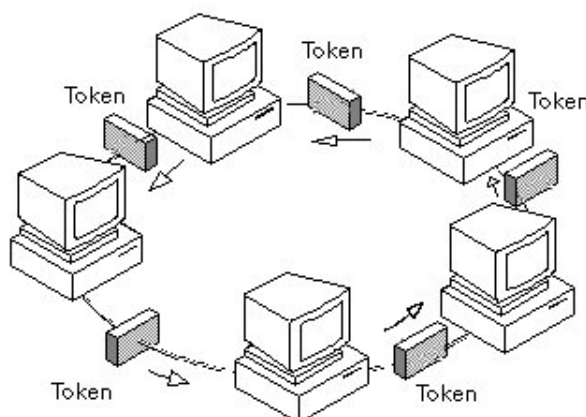
Ko dobi žeton, le tega shrani, na mrežo pa pošlje sporočilo. Preko naslednjih postaj to sporočilo potuje do naslovne postaje, ki sporočilo prebere in sprejme. Ta postaja nato odda potrditev sprejema sporočila. Ko oddajna postaja to sporočilo sprejme vrne žeton v omrežje.

Če zaradi napake oddajna postaja ne dobi potrdila o pravilnem sprejetju sporočila, ne odda žetona v omrežje. V tem primeru mora ena postaja v mreži generirati nov žeton. To lahko naredi vnaprej točno določena postaja (server) ali pa vsaka postaja v omrežju. V tem mehanizmu ni nikakršnega naključnega dogajanja. Takim mehanizmom pravimo determinirani mehanizmi. Glavne lastnosti token passing ring mehanizma so:

1. dostop in zasedba prenosnega medija je dokaj konstantna (ne glede na obremenjenost mreže)
2. zaradi velike količine procesiranja in čakanja žetona je mehanizem v principu počasnejši
3. ugotavljanje in popravljanje napak je preprosto in učinkovito.
4. primeren za procese, ki zahtevajo natančno časovno določljivost

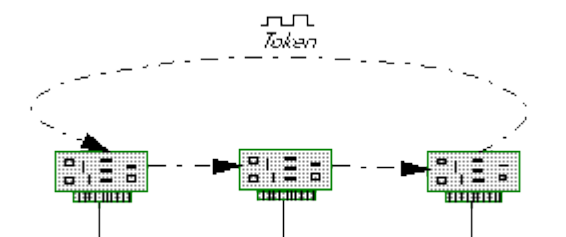
MULTIPLE TOKEN PASSING RING:

Celoten okvir pripotuje na postajo, ki ima ravno tako pripravljeno sporočilo.



Fizični nivo te postaje prekopira okvir v vhodni vmesnik (pomnilnik), pregleduje naslove okvirjev, ter išče žeton. Ko zazna žeton prenese sporočilo na njegovo mesto, ter ga na koncu svojega okvirja doda celotnemu sporočilu. Celoten proces se na vsaki postaji ponovi, na ta način nastane na mreži veriga okvirjev, ki jih naprej poriva žeton.

TOKEN PASSING BUS (IEEE 802.4):



Token Passing Bus: poizkuša prednosti topologije vodila in token passing metode združiti. Za fizično povezavo med delovnimi postajami pa vzpostavi logično topologijo obroča.

Token passing bus mehanizem deluje s pomočjo žetona, ki potuje po dinamičnem naslovnem zaporedju. To zaporedje pomeni, da je naslednje sprejemno vozlišče tisto, katerega naslov se nahaja v krožečem žetonu. Dodajanje in odzemanje delovnih postaj fleksibilno vpliva na vrstni red komunicirajočih postaj. Ob zagonu omrežja je potrebno vzpostaviti logični obroč, ki ga je potrebno tudi stalno vzdrževati. Žeton, ki potuje med postajami ni stalno enak, pač pa se vrednost njegovih polj spreminja v vsaki delovni postaji. Vsaka postaja v žeton vpiše naslov naslednje postaje, ki želi komunikacijo.

1. Inicializacija:

Ta proces se sproži ob začetnem pogonu mreže, ter ob popolnih izpadih.

V stanju pred vzpostavitvijo je mreža prazna. Vsaka postaja, ki želi pošiljati sporočila lahko konkurira za pravico generiranja prvega žetona. Postaja ki v natečaju zmaga lahko pošlje v mrežo prvi žeton.

2. Vzpostavitev logičnega obroča

Prva postaja pošlje na mrežo prijavi okvir v katerem določi naslovno področje.

Postaja, ki se namerava vključiti v logični obroč vključi svoj naslov v naslovno področje. Ko se žeton vrne izvorni postaji je logični obroč vzpostavljen.

3. Vzdrževanje logičnega obroča

Pomeni dodajanje in odzemanje delovnih postaj, brez porušitve mreže.

Protokoli z omejeno kolizijo

Kolizijski protokoli se obnesejo pri šibkem prometu, medtem ko so rezervacijski protokoli dobri za močan promet. Protokol, ki svoje lastnosti prilagaja količini prometa imenujemo **protokol z omejeno kolizijo**. Izvedba te ideje je praktično nemogoča. Vendar dosežemo isti učinek, če ob trkih določenim postajam – oddajnikom omejimo pravico oddajanja.

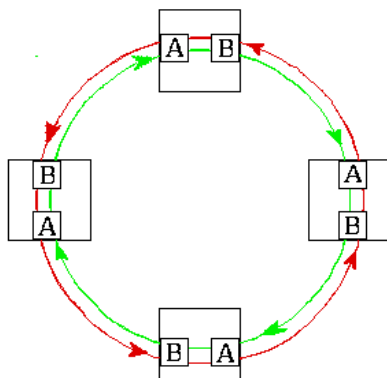
Taki protokoli so zanimivi za zelo specifična omrežja in komercialno niso razširjeni.

Protokoli za hitre komunikacije

Komercialne različice protokolov, ki smo jih omenjali do sedaj, imajo tipično kapaciteto prenosnega kanala 10 Mbit/s. Hitre komunikacije danes pomenijo hitrosti višje od 100 Mbit/s.

Tipičen predstavnik te skupine je FDDI (Fiber Distributed Data Interface), ki omogoča povezave 100 Mbit/s na razdaljah do 200 kilometrov brez ponavljalnikov. FDDI je različica protokola obroča z žetonom. Osnova tega protokola je dvojni optični obroč, ki prenese prekinitev optičnega vlakna na enem mestu.

Med hitre protokole sodi tudi hitri Ethernet, ki prav tako omogoča hitrost 100 Mbit/s in gigabit



Ethernet, ki omogoča hitrost 1000Mbit/s, zasnovana pa sta na standardu IEEE 802.3.

Brezžična in mobilna računalniška omrežja

Brezžično omrežje je tisto, čigar prenosni medij ni fizično oprijemljiv – radijski valovi ali svetloba. **Mobilno omrežje** ni nujno brezžično; bistveno je, da podpira selitve računalnikov.

WI-FI

Definiran je v standardu IEEE 802.11, Wi-Fi pomeni nabor Wireless LAN/WLAN standarda. Terminologija 802.11x je tudi nakaže kateri del standarda je uporabljen. Družina 802.11 trenutno vključuje šest tehnik prenosa podatkov preko radijskih valov. Najpogostejše različice najdemo v praksi v obliki 802.11b, 802.11a in 802.11g.

802.11b in 802.11g standarda uporabljata 2.4 GHz radijski pas, medtem ko 802.11a standard uporablja 5GHz radijski pas. Namreč delovanje na 2.4GHz lahko povzroči motnje med napravami z mikrovalovnimi pečicami, brezžičnimi telefonskimi aparati, bluetooth napravami in drugimi napravami, ki uporabljajo ta radijski pas.

802.11b standard dosega hitrosti do 11Mbit/s in upravlja CSMA/CD način dostopa. Glede na omejitve CSMA/CD načina aplikacije dosegajo hitrosti tja do 6Mbit/s preko TCP protokola in vse tja do 7Mbit/s preko UDP protokola.

Naprave lahko med seboj komunicirajo s pomočjo dostopne točke (access point). Domet dostopne točke do računalnika je znotraj prostorov približno 30metrov, če je pa prostor brez ovir (npr. sten) pa dosegamo tudi dolžine tja do 90metrov. Hitrost prenosa se z oddaljenostjo manjša. Seveda veliko pripomorejo kvalitetne antene nameščene tako na dostopni točki, kot tudi na samih računalnikih.

802.11g standard je nastal junija 2003. Ravno tako kot 802.11b deluje tudi ta standard na 2.4GHz radijskem pasu, ampak njegova maksimalna hitrost je 54Mbit/s. Naprave izdelane v standardu 802.11g naj bi delovale tudi z starejšimi standardi. V primeru napak, se hitrost prenosa zmanjšuje vse dokler ni signal pravilno prenesen med enotama. Možne hitrosti so 54,48,36,24,18,12,9,6 Mbit/s.



Varnost podatkov

Varnost je zagotovljena preko prekrivanja podatkov z raznoraznimi mehanizmi. Eden od teh mehanizmov je WEP (wired equivalent privacy), ki je definiran v 802.11 standardu. Ta način prekrivanja podatkov je sicer zadosten za domača omrežja, ni pa zanesljiv za prenos tajnih podatkov. Namreč z raznoraznimi orodji in različnimi pristopi lahko ugotovimo, kaj se po radijskih valovih prenaša.

Zaradi premajhne varnosti so v IEEE delovni skupini izdelali novi standard z imenom Wi-Fi Protected Access (WPA). Podatki se prekrivajo z RC4 algoritmom in z uporabo 128bitnim ključem in 48bitnim inicializacijskim vektorjem. Ena večja pridobitev WPA v primerjavi z WEP je tako imenovan Temporal Key Integrity Protocol (TKIP), ki dinamično spreminja ključe ko je sistem uporabljen. Priporoča se tudi uporabo WPA.

MAC

Preden si pogledamo IP protokol omenimo najprej **MAC** naslov. Media Access Control address (MAC address) je unikatna številka na vseh napravah priključenih na omrežje.

IEEE 802 MAC naslov ima sedaj standardno ime MAC-48 in prihaja iz specifikacije Ethernet protokola. 48 je število bitov, s katerimi izdelamo MAC naslove. Pomeni pa 2^{48} ali 281.474.976.710.656 možnih MAC naslovov.

MAC je navadno že vtisnjen v napravo ob nakupu, je pa mogoče MAC naslov spremeniti s posebno opremo. Primer MAC-48 naslova „00-0E-35-E1-4E-C8“. MAC naslovi se uporabljajo na povezavni plasti za identifikacijo naprav na omrežju.